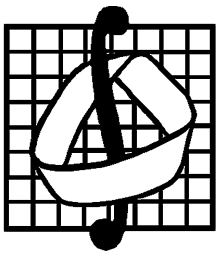
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ

XII Международного семинара

«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»

имени академика О. Б. ЛУПАНОВА

(Москва, 20–25 июня 2016 г.)

Издательство механико-математического факультета МГУ

Москва 2016

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 16–01–20345.

М34 Материалы XII Международного семинара «Дискретная математика и ее приложения» , имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2016. — 417 с.

Сборник содержит материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова, проходившего на механико-математическом факультете МГУ имени М. В. Ломоносова с 20 по 25 июня 2016 г. при поддержке Российского фонда фундаментальных исследований (проект 16–01–20345). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
XII МЕЖДУНАРОДНОГО СЕМИНАРА
«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»
имени академика О. Б. Лупанова
(Москва, МГУ, 20–25 июня 2016 г.)

Под общей редакцией О. М. КАСИМ-ЗАДЕ

Редакционная группа:
О. С. Дудакова, Р. М. Колпаков, Ю. А. Комбаров
В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *Ю. А. Комбаров*

Н/К
ИД № 04059 от 20.02.2001 Подписано к печати 05.08.2016. Формат 60 × 90/16.
Бумага типогр. № 1. Печ. л. 26,5. Тираж 200 экз.
Издательство механико-математического факультета МГУ. 119991, Москва, Ленинские горы, МГУ.
Отпечатано с оригинал-макета в типографии «DIAMOND TEAM», Москва.

ПРЕДИСЛОВИЕ

XII Международный семинар «Дискретная математика и ее приложения» имени О. Б. Лупанова, проходил на механико-математическом факультете МГУ имени М. В. Ломоносова с 20 по 25 июня 2016 г. при поддержке Российского фонда фундаментальных исследований (проект 16–01–20345).

Оргкомитетом семинара до начала его работы были разосланы информационные письма в ведущие научные центры и университеты стран СНГ, отобраны наиболее интересные доклады и сообщения для заслушивания на пленарных и секционных заседаниях.

Семинар собрал более 200 участников (в том числе около 50 докторов наук) из 40 научных центров России, Беларуси, Украины, Молдовы и Узбекистана.

Работа семинара проходила в семи секциях:

— синтез, сложность и надежность управляющих систем,

— теория функциональных систем,

— комбинаторный анализ,

— теория графов,

— математическая теория интеллектуальных систем,

— дискретная геометрия,

— теория кодирования и математические вопросы теории защиты информации.

Всего было заслушано 15 пленарных и 119 секционных докладов; содержание большинства из них отражено в настоящем сборнике.

Тексты публикуются в авторской редакции (исправлены замеченные опечатки).

ПЛЕНАРНЫЕ ДОКЛАДЫ

ОБ ОДНОЙ ЗАДАЧЕ О. Б. ЛУПАНОВА

В. В. Кочергин (Москва)

Отправной точкой для доклада на семинаре и для данного текста стали обнаруженные несколько лет назад три листочка с записями Олега Борисовича Лупанова, датированные, по-видимому, весной 1988 года. В этих листочках О. Б. Лупанов ставил автору, тогда еще студенту-пятикурснику, задачу о сложности вычисления элементов конечных абелевых групп. С тех пор в этом и близких направлениях был получен ряд результатов, постановки задач видоизменялись, расширялись, переосмысливались, так или иначе все дальше удаляясь от исходной. В связи с этим представляется важным вернуться к задаче именно в исходной постановке — решению задач в изначальной постановке О. Б. Лупанов придавал большое значение.

Достаточно серьезное продвижение в решении поставленной задачи было получено в начале 90-х годов в работах [4, 5]. Однако в дальнейшем эти результаты получили развитие в несколько другой плоскости, дистанцировшись от первоначальной задачи. Первой после долгого перерыва попыткой ответить в точности на вопросы из упомянутых листочков стала заметка [10], в которой, в основном, применением ранее установленных для близких задач результатов получены ответы на некоторые вопросы. Для удовлетворительного ответа на все поставленные вопросы потребовалось еще три года...

Постановка задачи

Пусть G — конечная абелева группа (групповую операцию будем называть умножением). Подмножество $B = \{a_1, \ldots, a_q\}$ элементов группы будем называть *базисом* в группе G, если G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B:

$$G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q},$$

где u_i — порядок элемента a_i, $i = 1, \ldots, q$.

Для каждого элемента g группы G определим его *сложность реализации* (*вычисления*) *над базисом* B, обозначаемую через $L(g; B)$ как минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества B, при

этом все уже вычисленные элементы могут быть использованы многократно — в этом принципиальное отличие этой, «схемной», меры сложности от другой, «формульной» (см., например, [2]), меры сложности вычислений элементов в группах. Отметим также, что в алгебре под задачей вычислений в группе понимают, как правило, совсем другую задачу, а именно, задачу распознавания равенства слов в группе — см., например, [17].

Сложность реализации элемента g группы G над базисом B удобно интерпретировать на языке схем из функциональных элементов [15], как это сделано, например, в [5]: на входы схем подаются базисные элементы группы G, сами схемы состоят из двухвходовых элементов, которые по двум представителям группы G, поступающим на входы, реализуют их произведение; под сложностью схемы понимается число функциональных элементов в схеме (т. е. операций умножения), а сложность реализации $L(g;B)$ элемента g группы G над базисом B численно равна минимальной сложности схем, реализующих элемент g над базисом B.

Имеет смысл дать еще одно эквивалентное определение величины $L(g;B)$. *Вычислительной цепочкой* (по аналогии с аддитивной цепочкой [3]) для элемента g конечной абелевой группы G над базисом $B = \{a_1, \ldots, a_q\}$ будем называть всякую последовательность $a_1, \ldots, a_q, h_1, h_2, \ldots, h_r = g$ элементов группы G, удовлетворяющую свойству: для каждого k, $1 \le k \le r$, найдется два не обязательно различных элемента h_{k1} и h_{k2} из множества $\{a_1, \ldots, a_q, h_1, h_2, \ldots, h_{k-1}\}$, т. е. лежащих в этой последовательности левее элемента g_k, таких, что $h_k = h_{k1}h_{k2}$. Число r называется *длиной вычисления* элемента g над базисом B, минимальная длина вычисления элемента g над базисом B совпадает с величиной $L(g;B)$.

Сложность $L(G,B)$ конечной абелевой группы G над базисом B определим так:

$$L(G,B) = \max_{g \in G} L(g;B).$$

Положим

$$LM(G) = \max_{B\colon B-\text{базис } G} L(G,B), \quad Lm(G) = \min_{B\colon B-\text{базис } G} L(G,B).$$

Так как конечная абелева группа G полностью определяется вектором $\mathbf{v} = (v_1, \ldots, v_q)$ порядков примарных циклических компонент, то вместо обозначения $LM(G)$ можно использовать обозначение $M(\mathbf{v})$, а вместо $Lm(G)$ — $m(\mathbf{v})$.

Для абелевой группы, порядки примарных циклических компонент которой задаются вектором $\mathbf{v}$, будем использовать обозначение $G_{\mathbf{v}}$.

Для вектора $\mathbf{v} = (v_1, \ldots, v_q)$ обозначим через $\|\mathbf{v}\|$ величину $v_1 v_2 \ldots v_q$. Положим

$$M(n) = \max_{\mathbf{v}\colon \|\mathbf{v}\| \le n} M(\mathbf{v}), \quad m(n) = \max_{\mathbf{v}\colon \|\mathbf{v}\| \le n} m(\mathbf{v}).$$

Кроме того, введем функции $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, характеризующие средние значения соответствующих мер сложности абелевых групп порядка n, определив их равенствами

$$M_{\text{ср}}(n) = \frac{\sum LM(G)}{A(n)}, \quad m_{\text{ср}}(n) = \frac{\sum Lm(G)}{A(n)},$$

где суммы берутся по всем различным (с точностью до изоморфизма) абелевым группам G порядка n, а $A(n)$ — количество попарно неизоморфных абелевых групп порядка n.

Задача, поставленная О. Б. Лупановым, заключается в том, чтобы, во-первых, как можно более точно оценить величину $L(G, B)$; во-вторых, найти числовые функции $f_1(\mathbf{v})$ и $f_2(\mathbf{v})$, определенные на векторах $\mathbf{v}$, характеризующих порядки примарных циклических групп, с помощью которых выражались бы величины $M(\mathbf{v})$ и $m(\mathbf{v})$ (хотя бы асимптотически или с точностью до порядка при условии, что порядок всей группы стремится к бесконечности); в-третьих, исследовать рост функций $M(n)$ и $m(n)$, а также функций $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, при $n \to \infty$.

Основные результаты

Получение точных формул для введенных мер сложности при больших значениях порядков групп является, по всей видимости, очень трудной задачей, что подтверждается, в частности, NP-полнотой близкой задачи [23], о которой ниже также пойдет речь. Поэтому далее будем говорить только об асимптотических оценках, по возможности асимптотически точных или хотя бы точных по порядку при условии роста к бесконечности порядка группы.

Первые серьезные результаты в решении этих задач были получены в работе [5] (см. также краткий вариант [4]). Помимо двух простых нижних оценок (одна из которых стандартная мощностная), была получена и важная верхняя оценка сложности конечной абелевой группы над заданным базисом. Чтобы сформулировать эти оценки введем следующие обозначения. Пусть $G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q}$.

Тогда для базиса $B = \{a_1, \ldots, a_q\}$ положим $k(B) = \max\limits_{1 \le i \le q} u_i$. Кроме того, для произвольного базиса B конечной абелевой группы положим $q(B) = |B|$. Иногда будем вместо $q(B)$ использовать обозначение q, если при этом не возникает коллизий.

Теорема 1 [5]. *Пусть B — базис конечной абелевой группы G. Тогда*[1]

$$L(G, B) \ge \lfloor \log(k(B) - 1) \rfloor + q(B) - 1.$$

Теорема 2 [5]. *Для произвольного положительного ε найдется такое положительное $m(\varepsilon)$, что для сложности любой конечной абелевой группы G над базисом B при выполнении условия $|G| > m(\varepsilon)$ справедлива оценка*

$$L(G, B) \ge \frac{\log |G|}{\log \log |G|} \left(1 + (1 - \varepsilon) \frac{\log \log \log |G|}{\log \log |G|}\right).$$

В основе доказательства верхней оценки величины $L(G, B)$ из [5] лежит сведéние задачи вычисления элемента группы к задаче реализации булевых матриц специального вида вентильными схемами [14, 26] — ориентированными графами без ориентированных циклов с двумя группами выделенных вершин, называемых, соответственно, входами и выходами схемы, такими что ориентированные пути от входа к входу, от выхода к выходу и от выхода к входу отсутствуют, а число путей от i-го входа к j-му выходу равно элементу матрицы, стоящему на пересечении i-й строки и j-го столбца. Вычисляемому элементу группы сопоставляется булева матрица, столбцами которой являются двоичные записи показателей степеней в представлении элемента через образующие; при этом старшие разряды дополняются нулями для выравнивания высоты. С использованием вентильной конструкции автора из [5], опирающейся в свою очередь на конструкции О. Б. Лупанова [14], Э. И. Нечипорука [16] и Н. Пиппенджера [26] и дающей асимптотически оптимальную оценку через «информационную площадь» матрицы, доказана следующая

Теорема 3 [5]. *Существуют такие положительные константы c_1 и c_2, что для произвольной конечной абелевой группы G и любого базиса B этой группы справедливо неравенство*

$$L(G, B) \le \frac{\log |G|}{\log \log |G|} \left(1 + c_1 \left(\frac{\log \log \log |G|}{\log \log |G|}\right)^{1/2}\right) + \\ + c_2 \max(\log k(B), q(B)).$$

[1] Здесь и далее все логарифмы берутся по основанию 2.

Теоремы 1–3 устанавливают порядок роста величины $L(G, B)$: при условии $|G| \to \infty$ справедливо равенство

$$L(G, B) = \Theta\left(\frac{\log |G|}{\log\log |G|} + \log k(B) + q(B)\right).$$

Кроме того, результаты, установленные в [5], с использованием теоремы Бертрана — Чебышёва о распределении простых чисел (см., например, [20]), в силу которой найдется простое p, удовлетворяющее условиям $\lceil n/2 \rceil < p < 2\lceil n/2 \rceil$, а следовательно, и неравенствам $n/2 < p \leq n$, по-существу позволяют доказать справедливость следующих утверждений.

Теорема 4. *При $n \to \infty$ справедливы равенства*

$$M(n) = \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right);$$

$$m(n) = \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right).$$

Тем самым получено решение еще одной из поставленных О. Б. Лупановым задач — найдена асимптотика роста функций $M(n)$ и $m(n)$ (на самом деле не только асимптотика, но и асимптотика остаточного члена).

Собственно, на этом результаты в данном направлении формально, по-видимому, и исчерпывались. Были еще две работы автора [6, 9], являющиеся в некотором смысле логическим продолжением статьи [5], но они посвящены задачам сложности вычислений (в том же самом смысле) в конечных нильпотентных и разрешимых группах, и в них новых результатов для класса конечных абелеых групп практически не содержится. Однако задачи, поставленные О. Б. Лупановым, имеют тесную связь с задачей Ричарда Беллмана, на которой остановимся несколько подробнее.

В 1963 г. Р. Беллман [22] (для случая $m = 2$), а затем в 1964 г. Е. Страус [28] (для произвольного m) сформулировали задачу о нахождении сложности вычисления одночлена от m переменных. Под *сложностью вычисления одночлена* $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$ (обозначение $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$) понимается минимальное число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \dots, x_m$ одночлена $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$. На аддитивном языке вели-

чина $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$ формально определяется как минимально возможная длина r последовательности m-мерных векторов (наборов)

$$\mathbf{d}_1=(1,0,\dots,0),\mathbf{d}_2=(0,1,\dots,0),\dots,\mathbf{d}_m=(0,0,\dots,1),$$
$$\mathbf{d}_{m+1},\mathbf{d}_{m+2},\dots,\mathbf{d}_{m+r}=(n_1,n_2,\dots,n_m),$$

начинающейся с m единичных векторов и удовлетворяющей условию: для каждого k, $m+1\le k\le m+r$, найдется два натуральных числа (не обязательно различных) i и j, $1\le i\le k-1$, $1\le j\le k-1$, таких, что $\mathbf{d}_k=\mathbf{d}_i+\mathbf{d}_j$ (сложение векторов покомпонентное).

На самом деле задача Беллмана эквивалентна [19, 24, 25] известной задаче Дональда Кнута [3, разд. 4.6.3, упр. 32] о нахождении величины $l(x^{n_1},x^{n_2},\dots,x^{n_m})$ — *сложности вычисления набора степеней* $(x^{n_1},x^{n_2},\dots,x^{n_m})$, т. е. минимального числа умножений, достаточного для вычисления множества степеней $x^{n_1},x^{n_2},\dots,x^{n_m}$ исходной переменной x. Эта эквивалентность, заключающаяся в справедливости равенства

$$l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})+1=l(x^{n_1},x^{n_2},\dots,x^{n_m})+m,$$

позволяет говорить об этих двух задачах как об одной задаче Беллмана — Кнута.

Небольшой обзор результатов по задаче Беллмана — Кнута можно найти в [12].

Очевидно, что для произвольного элемента $a_1^{n_1}a_2^{n_2}\dots a_m^{n_m}$ абелевой группы $\langle a_1\rangle\times\langle a_2\rangle\times\ldots\times\langle a_m\rangle$ справедливо неравенство

$$L\left(a_1^{n_1}a_2^{n_2}\dots a_m^{n_m},\{a_1,a_2,\dots,a_m\}\right)\le l\left(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\right).$$

Поэтому верхние оценки сложности в задаче Беллмана — Кнута автоматически дают верхние оценки в задаче о сложности вычисления элементов конечных абелевых групп. С получением нижних оценок сложности вычисления элементов конечных абелевых групп через нижние оценки для задачи Беллмана — Кнута, конечно, все не так однозначно, что и иллюстрируют следующие два примера.

Пример 1. С одной стороны, справедливо равенство $l(x^{31})=7$ (см., например, [3]), а с другой стороны, в группе $\langle a\rangle_{33}$, очевидно, выполняется соотношение $L(a^{31},\{a\})=6$.

Обобщая, получаем, с одной стороны, неравенство

$$l(x^{2^n-1})\ge n+\log n-2,13,$$

вытекающее из основного результата работы [27], а с другой, для группы $\langle a\rangle_{2^n+1}$ — равенство

$$L\left(a^{2^n-1},\{a\}\right)=n+1.$$

Таким образом,

$$l(x^{2^n-1})-L\left(a^{2^n-1},\{a\}\right)\geq \log n-3,13.$$

Пример 2. Для произвольного m обозначим через $(n_1,n_2,\ldots,n_m)$ набор, удовлетворяющий двум условиям:

1) $n_i\leq 2^m$, $i=1,2,\ldots,m$;

2) $l\left(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}\right)=\max l\left(x_1^{t_1}x_2^{t_2}\ldots x_m^{t_m}\right)$, где максимум берется по всем наборам $(t_1,t_2,\ldots,t_m)$ с целыми неотрицательными компонентами, не превышающими величины 2^m.

Из стандартных мощностных соображений (см., например, [7]) при всех достаточно больших значениях m следует такое неравенство:

$$l\left(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}\right)\geq\frac{m^2}{2\log m}.$$

Теперь положим $n=\max\limits_{j=1,2,\ldots,m}n_j$, $r_i=2n+1-n_i$ $(i=1,2,\ldots,m)$. Отметим, что при всех i, $1\leq i\leq m$, выполняются неравенства $n_i<r_i$. Рассмотрим группу $\langle a_1\rangle_{r_1}\times\langle a_2\rangle_{r_2}\times\ldots\times\langle a_m\rangle_{r_m}$. В этой группе справедлива цепочка равенств

$$(a_1a_2\ldots a_m)^{2n+1}=\prod_{i=1}^{m}a_i^{2n+1-n_i+n_i}=\prod_{i=1}^{m}\left(a_i^{r_i}a_i^{n_i}\right)=a_1^{n_1}a_2^{n_2}\ldots a_m^{n_m}.$$

Поэтому, используя известный факт о том, что для возведения в степень t достаточно $\log t+o(\log t)$ операций умножения [21] (см. также, например, [3]), при $m\to\infty$ получаем следующую оценку[2]:

$$L\left(a_1^{n_1}a_2^{n_2}\ldots a_m^{n_m},\{a_1,a_2,\ldots a_m\}\right)\leq\log n+o(\log n)+m\lesssim 2m.$$

[2]Для функций $f(m)$ и $g(m)$, заданных на множестве натуральных чисел, при $m\to\infty$ запись $f(m)\lesssim g(m)$ означает выполнение условия $\overline{\lim}_{m\to\infty}\frac{f(m)}{g(m)}\leq 1$, запись $f(m)\gtrsim g(m)$ — выполнение условия $\underline{\lim}_{m\to\infty}\frac{f(m)}{g(m)}\geq 1$, и, наконец, запись $f(m)\sim g(m)$ — выполнение условия $\lim_{m\to\infty}\frac{f(m)}{g(m)}=1$.

Следовательно,

$$l\left(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\right) \gtrsim \frac{\left(L\left(a_1^{n_1}a_2^{n_2}\dots a_m^{n_m},\{a_1,a_2,\dots a_m\}\right)\right)^2}{8\log L\left(a_1^{n_1}a_2^{n_2}\dots a_m^{n_m},\{a_1,a_2,\dots a_m\}\right)},$$

т. е. отличие в порядках роста сложности с увеличением параметра m для двух задач почти квадратичное.

Таким образом, сами нижние оценки, полученные при исследовании задачи Беллмана — Кнута, не могут быть напрямую применены для получения нижних оценок сложности вычислений элементов конечных абелевых групп. Однако основные методы получения нижних оценок с различной степенью эффективности работают и в этой задаче.

Возвращаясь к верхним оценкам в задаче Беллмана — Кнута, отметим, что наиболее сильная из них получена в работе [12] на основе оценок из [1], которые, в свою очередь, существенно опираются на результаты из [5]. Нам достаточно будет следующей упрощенной формулировки (в работе [12] это следствие к теореме 1).

Утверждение 1 [12]. *Для любой последовательности наборов натуральных чисел* $\tilde{n}(s) = \big(n_1(s), n_2(s), \dots, n_{m(s)}(s)\big)$, $s = 1, 2, \dots$, *удовлетворяющей условию*

$$\sum_{i=1}^{m(s)} n_i(s) \to \infty,$$

при $s \to \infty$ *выполняется неравенство*

$$l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}) \lesssim \log\left(\max_{1\le i\le m} n_i(s)\right) + \frac{\log N(s)}{\log\log N(s)} + m(s),$$

где $N(s) = n_1(s)n_2(s)\dots n_m(s)$.

С использованием утверждения 1 один из результатов работы [5] можно значительно усилить следующим образом.

Теорема 5. *Пусть* $G = \langle a_1\rangle_{u_1} \times \dots \times \langle a_q\rangle_{u_q}$, $B = \{a_1, \dots, a_q\}$. *Тогда при* $|G| \to \infty$ *справедливы соотношения*

$$\max\left(\frac{\log|G|}{\log\log|G|},\ \log k(B) + q\right) \lesssim L(G,B) \lesssim \frac{\log|G|}{\log\log|G|} + \log k(B) + q.$$

Теперь, возвращаясь к нижним оценкам, сформулируем в упрощенном виде, удобном для наших целей, основной результат работы [8].

Утверждение 2 [8]. *Пусть последовательность наборов*

$$\tilde{n}(s) = \big(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\big), \quad s = 1, 2, \ldots,$$

натуральных чисел при $s \to \infty$ удовлетворяет условию

$$m(s) = o\left(\log\left(\max_i n_i(s)\right) + \frac{\log N(s)}{\log\log N(s)}\right),$$

где $N(s) = \prod_{i=1}^{m(s)} n_i(s)$. Тогда при $s \to \infty$ справедливо соотношение

$$\max l\left(x_1^{t_1} x_2^{t_2} \ldots x_{m(s)}^{t_{m(s)}}\right) \gtrsim \log\left(\max_i n_i(s)\right) + \frac{\log N(s)}{\log\log N(s)},$$

где максимум берется по всем наборам $(t_1, t_2, \ldots, t_{m(s)})$ целых чисел, удовлетворяющих условиям $0 \le t_i \le n_i(s)$, $i = 1, 2, \ldots, m(s)$.

Как уже отмечалось выше, из нижней оценки для задачи Беллмана напрямую не следует аналогичная нижняя оценка сложности конечных абелевых групп. Тем не менее, повторяя с соответствующими изменениями рассуждения из работы [8], можно установить следующий факт.

Теорема 6. *Пусть B — базис конечной абелевой группы G. При $|G| \to \infty$ если выполняется условие*

$$q(B) = o\left(\frac{\log|G|}{\log\log|G|} + \log k(B)\right),$$

то справедлива асимптотическая оценка

$$L(G, B) \gtrsim \frac{\log|G|}{\log\log|G|} + \log k(B).$$

Теперь перейдем к исследованию асимптотики роста величин $M(\mathbf{v})$ и $m(\mathbf{v})$.

Функцию $h(n)$ натурального аргумента будем называть *допустимой*, если выполняется следующее свойство — для любых двух последовательностей натуральных чисел $\{d_n^{(1)}\}$ и $\{d_n^{(2)}\}$, удовлетворяющих условиям:

1) $d_n^{(1)} \to \infty$;

2) $d_n^{(2)}/2 \le d_n^{(1)} \le 2d_n^{(2)}$ для всех достаточно больших значениях n,

при $n \to \infty$ справедливо асимптотическое равенство $h(d_n^{(1)}) \sim h(d_n^{(2)})$.

Заметим, что допустимую функцию можно определить как функцию натурального аргумента, допускающую доопределение до медленно меняющейся на бесконечности функции (см., например, [18]).

Теорема 7 [13]. *При $\|\mathbf{v}\| \to \infty$ выполняются соотношения*

$$\frac{\log \|\mathbf{v}\|}{\log\log \|\mathbf{v}\|} \lesssim m(\mathbf{v}) \le M(\mathbf{v}) \lesssim \log \|\mathbf{v}\|,$$

причем для любых допустимых функций $h_1(n)$ и $h_2(n)$, удовлетворяющих при $n \to \infty$ условиям

$$\frac{\log n}{\log\log n} \lesssim h_1(n) \lesssim h_2(n) \lesssim \log n,$$

найдется последовательность векторов $\mathbf{v}_s$, удовлетворяющая условию $\|\mathbf{v}_s\| \to \infty$, для которой справедливы соотношения

$$m(\mathbf{v}_s) \sim h_1(\|\mathbf{v}_s\|), \qquad M(\mathbf{v}_s) \sim h_2(\|\mathbf{v}_s\|).$$

Перейдем к исследованию величины $M(\mathbf{v})$. Пусть группа G представлена как прямое произведение своих примарных циклических компонент:

$$G = \langle a_1 \rangle_{v_1} \times \ldots \times \langle a_q \rangle_{v_q}.$$

Обозначим через $q(\mathbf{v})$ размерность (число координат) вектора $\mathbf{v}$. Далее для каждого простого делителя p_i величины $\|\mathbf{v}\|$ обозначим через $P_i(\mathbf{v})$ максимальный из порядков примарных циклических подгрупп, являющихся степенями числа p_i. Теперь положим $P(\mathbf{v}) = \prod P_i(\mathbf{v})$, где произведение берется по всем простым делителям числа $\|\mathbf{v}\|$. Легко заметить, что величина $P(\mathbf{v})$ численно равна максимальному значению порядка среди всех элементов группы G. Кроме того, всегда найдется базис B_1 группы G, для которого справедливо равенство $k(B_1) = P(\mathbf{v})$.

Очевидно, что справедливы оценки $M(\mathbf{v}) \ge q(\mathbf{v}) - 1$ и $M(\mathbf{v}) \ge \log(P(\mathbf{v}) - 1)$, но «объединение» их путем сложения оценок в одно неравенство подобно теореме 1 не является, вообще говоря, верным соотношением — например, для вектора $\mathbf{v} = (2, 3)$ имеем: $M(\mathbf{v}) = 3$, $q(\mathbf{v}) = 2$, $\log(P(\mathbf{v}) - 1) \approx 2,32$.

А вот соответствующая асимптотическая оценка справедлива.

Теорема 8 [13]. *При* $\|\mathbf{v}\| \to \infty$ *выполняется асимптотическое неравенство*

$$M(\mathbf{v}) \gtrsim q(\mathbf{v}) + \log P(\mathbf{v}).$$

Следующая теорема дает ответ еще на одну часть исходной задачи.

Теорема 9 [13]. *При* $\|\mathbf{v}\| \to \infty$ *выполняются соотношения*

$$\max\left(\frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|}, q(\mathbf{v})+\log P(\mathbf{v})\right) \lesssim M(\mathbf{v}) \lesssim \frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|} + q(\mathbf{v}) + \log P(\mathbf{v}).$$

Теорема 9 уставливает порядок роста величины $M(\mathbf{v})$, причем верхняя оценка может превышать нижнюю асимптотически не более чем в два раза. Кроме того, в случае, когда одна из величин $\frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|}$ или $q(\mathbf{v})+\log P(\mathbf{v})$ растет существенно быстрее другой, т. е. выполняется условие

$$\frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|(\log P(\mathbf{v}) + q(\mathbf{v}))} + \frac{\log\log\|\mathbf{v}\|(\log P(\mathbf{v}) + q(\mathbf{v}))}{\log\|\mathbf{v}\|} \to \infty,$$

теорема 9 устанавливает следующую асимптотику роста функционала сложности $M(\mathbf{v})$:

$$M(\mathbf{v}) \sim \frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|} + \log P(\mathbf{v}) + q(\mathbf{v}).$$

Для формулировки оценок асимптотического роста величины $m(\mathbf{v})$ введем обозначения. Пусть B — базис конечной абелевой группы G. Положим

$$r(B) = \lfloor \log(k(B)-1) \rfloor + q(B), \quad r(\mathbf{v}) = \min_{B:\ B-\text{базис } G_{\mathbf{v}}} r(B).$$

Теорема 10 [13]. *С одной стороны при* $\|\mathbf{v}\| \to \infty$ *выполняется верхняя оценка*

$$m(\mathbf{v}) \lesssim \frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|} + r(\mathbf{v});$$

с другой стороны, при всех достаточно больших значениях $\|\mathbf{v}\|$ *справедлива нижняя оценка*

$$m(\mathbf{v}) \geq \max\left(\frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|},\ r(\mathbf{v}) - 1\right).$$

Эта теорема уставливает порядок роста величины $m(\mathbf{v})$, причем опять верхняя оценка может превышать нижнюю асимптотически не более чем в два раза. В случае, когда одна из величин $\frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|}$ или $r(\mathbf{v})$ растет существенно быстрее другой, т. е. выполняется условие

$$\frac{\log\|\mathbf{v}\|}{(\log\log\|\mathbf{v}\|)r(\mathbf{v})} + \frac{(\log\log\|\mathbf{v}\|)r(\mathbf{v})}{\log\|\mathbf{v}\|} \to \infty,$$

теорема устанавливает следующую асимптотику роста функционала сложности $m(\mathbf{v})$:

$$m(\mathbf{v}) \sim \frac{\log\|\mathbf{v}\|}{\log\log\|\mathbf{v}\|} + r(\mathbf{v}).$$

В заключение сформулируем наиболее трудный из результатов в этом направлении за последнее время — теорему об асимптотическом поведении функций $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, характеризующих средние значения соответствующих мер сложности абелевых групп порядка n.

Теорема 11 [13]. *При $n \to \infty$ выполняются соотношения*

$$\frac{\log n}{\log\log n} \lesssim m_{ср}(n) \leq M_{ср}(n) \lesssim \log n,$$

причем для любых допустимых функций $h_1(n)$ и $h_2(n)$, удовлетворяющих при $n \to \infty$ условиям

$$\frac{\log n}{\log\log n} \lesssim h_1(n) \lesssim h_2(n) \lesssim \log n,$$

найдется такая последовательность $\{n_s\}$, что $n_s \to \infty$ при $s \to \infty$, для которой справедливы соотношения

$$m_{\text{ср}}(n_s) \sim h_1(n_s); \quad M_{\text{ср}}(n_s) \sim h_2(n_s).$$

Работа выполнена при финансовой поддержке РФФИ, проект № 14–01–00598.

Список литературы

1. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. — Новосибирск, 1992. — Вып. 52. — С. 22–40.

2. Глухов М. М., Зубов А. Ю. О длинах симметрических и знакопеременных групп подстановок в различных системах образующих // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 5–32.

3. Кнут Д. Е. Искусство программирования для ЭВМ, т. 2. 1-е издание. — М.: Мир, 1977.

4. Кочергин В. В. О сложности вычислений в конечных абелевых группах // Доклады АН СССР — 1991. — Т. 317, № 2. — С. 291–294.

5. Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики, вып. 4. — М.: Наука, 1992. — С. 178–217.

6. Кочергин В. В. О сложности вычислений в конечных абелевых, нильпотентных и разрешимых группах // Дискретная математика. — Т. 5, вып. 1. — 1993. — С. 91–111.

7. Кочергин В. В. О вычислении наборов степеней // Дискретная математика. — Т. 6, вып. 2. — 1994. — С. 129–137.

8. Кочергин В. В. О сложности вычислений одночленов и наборов степеней // Дискретный анализ. — Новосибирск: Издательство Института математики СО РАН, 1994. — (Тр./РАН. Сиб. отделение. Ин-т математики; Т. 27) — С. 94–107.

9. Кочергин В. В. О сложности вычислений в конечных нильпотентных группах // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 1. — С. 43–51.

10. Кочергин В. В. Некоторые задачи сложности вычисления элементов конечных абелевых групп // Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2012 г.) — М.: Издательство механико-математического факультета МГУ, 2012. — С. 135–138.

11. Кочергин В. В. Об одной нижней оценке сложности вычисления элементов конечных абелевых групп // Проблемы теоретической кибернетики. Материалы XVII международ. конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 155–158.

12. Кочергин В. В. Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута // Дискретный анализ и исследование операций. — 2014. — Т. 21, № 6. — С. 51–72.

13. Кочергин В. В. О некоторых мерах сложности конечных абелевых групп // Дискретная математика. — 2015. — Т. 27, вып. 3. — С. 25–43.

14. Лупанов О. Б. О вентильных и контактно-вентильных схемах // Доклады АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.

15. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики, вып. 10. — М.: Физматгиз, 1963. — С 63–97.

16. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики, вып. 21. — М.: Наука, 1969. — С. 5–102.

17. Ольшанский А. Ю. О сложности вычислений в группах // Соросовский образоват. журнал. — 2000. — Т. 6, № 3. — С. 118–123.

18. Сенета Е. Правильно меняющиеся функции. — М.: Наука, 1985. — 144 с.

19. Сидоренко А. Ф. Сложность аддитивных вычислений семейств целочисленных линейных форм // Записки научных семинаров ЛОМИ. — Л.: Наука, 1981. — Т. 105. — С. 53–61.

20. Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974.

21. Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — V. 45. — P. 736–739.

22. Bellman R. E. Addition chains of vectors (Advanced problem 5125) // Amer. Math. Monthly. — 1963. — V. 70. — P. 765.

23. Downey P., Leong B., Sethi R. Computing sequences with addition chains // SIAM Journal on Computing. — V. 10. — 1981. — P. 638–646.

24. Knuth D. E., Papadimitriou C. H. Duality in addition chains // Bulletin of the European association for Theoretical Computer Science. — 1981. — V. 13. — P. 2–4.

25. Olivos J. On vectorial addition chains // J. Algorithms. — 1981. — V. 2, N 1. — P. 13–21.

26. Pippenger N. The mimimum number of edges in graphs with prescribed paths // Math. Systems Theory. — 1979. — V. 12, № 4. — P. 325–346.

27. Schönhage A. A lower bound for the lenght of addition chains // Theoretical Computer Science. — 1975. — V. 1. — P. 1–12.

28. Straus E. G. Addition chains of vectors // Amer. Math. Monthly. — 1964. — V. 71. — P. 806–808.

КРИПТОГРАФИЯ И p-АДИЧЕСКИЙ АНАЛИЗ

М. П. Минеев, В. Н. Чубариков (Москва)

Настоящая статья представляет собой изложение нашего сообщения на Международном семинаре имени академика О. Б. Лупанова. На наш взгляд следующие слова Б. Паскаля в определенном смысле отражают жизненные принципы О. Б. Лупанова: “Весь блеск почестей и величия не имеет цены в глазах людей, посвятивших себя исследованиям в умственной области.”

Введение

Арифметика занимается изучением свойств целых чисел. Величина числа связана с аддитивной структурой чисел, последнее определяет абелеву группу с образующей, равной 1. Другая характеристика целых чисел связана с их делимостью и тесно связана с мультипликативной структурой целых чисел. По умножению целые числа образуют полугруппу, количество образующих которой бесконечно. Это простые числа. Данное обстоятельство вносит элемент неиссякаемого научного интереса к теории целых чисел и ее приложениям. В частности, к применению ее в криптографии. Большую пользу при изучении мультипликативной теории чисел дает теория сравнений. Первые вопросы здесь возникают в связи со свойствами различных арифметических объектов в полной и приведенной системах вычетов по некоторым определенным модулям. Подобным моментам теории чисел посвящено настоящее сообщение.

§1. Китайская теорема об остатках

Пусть $m > 1$ — натуральное число, $m = m_1 m_2, (m_1, m_2) = 1$. Тогда найдутся числа m_1' и m_2' такие, что

$$m_1 m_1' \equiv 1 \pmod{m_2}, \quad m_2 m_2' \equiv 1 \pmod{m_1}.$$

Рассмотрим систему сравнений

$$\begin{cases} x \equiv x_1 \pmod{m_1}, \\ x \equiv x_2 \pmod{m_2}, \end{cases}$$

с неизвестным x по модулю m. Единственное решение этой системы имеет вид

$$x \equiv m_2 m_2' x_1 + m_1 m_1' x_2 \pmod{m}.$$

Другими словами, если переменная x_1 пробегает полную систему вычетов по модулю m_1, а x_2 — полную систему вычетов по модулю m_2,

то x пробегает полную систему вычетов по модулю m. Это утверждение и есть *китайская теорема об остатках* (см., например, [1, гл. IV, §3, с. 57]).

1.1. *Применение китайской теоремы об остатках к шифру Виженера.*

Возвращаемся к "сложным" шифрам, для которых китайская теорема об остатках дает возможность изменить частоту появления знаков в них.

Рассмотрим известный многоалфавитный шифр Виженера. Он является обобщением одноалфавитного шифра простой замены и представляет собой шифр гаммирования с периодической гаммой (см., например, [9, с. 151–152; 8, с. 11]).

Пусть количество символов алфавита равно составному числу n. Каждому символу $\alpha_r (r = 1, \ldots, n)$ алфавита присваивается некоторый вычет a_r по модулю n, причем различным символам отвечают различные вычеты. Можно предложить следующий способ шифрования.

1.2. *Предварительные преобразования.* Пусть число n представимо в виде $n = dq, (d, q) = 1, d > 1, q > 1$. Представим каждое число $1 \leq a \leq n$ в виде

$$a \equiv qb + dc \pmod{n}, \tag{2.1.1}$$

где $1 \leq b \leq d, 1 \leq c \leq q$. Тогда по китайской теореме об остатках вычет a по модулю n однозначно определяет вычеты b по модулю d и c по модулю q и наоборот.

Составим две таблицы Виженера, отвечающие вычетам b и c. Пусть $b_1, \ldots, b_d$ — полная система вычетов по модулю d, например, $1, 2, \ldots, d$, и $c_1, \ldots, c_q$ — полная система вычетов по модулю q.

Тогда таблицы Виженера будут иметь вид

$$\begin{array}{ll}
\underline{b_1, b_2, \ldots, b_{d-1}, b_d,} & \underline{c_1, c_2, \ldots, c_{q-1}, c_q,} \\
b_2, b_3, \ldots, b_d, \quad b_1, & c_2, c_3, \ldots, c_q, \quad c_1, \\
\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\
b_d, b_1, \ldots, b_{d-2}, b_{d-1}, & c_q, c_1, \ldots, c_{q-2}, c_{q-1}.
\end{array}$$

Для каждой из приведенных выше таблиц Виженера при некоторых натуральных числах s, t с условиями $1 \leq s \leq d, 1 \leq t \leq q$ возьмем свой ключ $k = (b_{k_1}, b_{k_2}, \ldots, b_{k_s})$ для первой таблицы и соответственно $p = (c_{p_1}, c_{p_2}, \ldots, c_{p_t})$ для второй таблицы. Над каждым вычетом первой строки первой таблицы выписываем в строку символы ключа k следующим образом

$$b_{k_1}, b_{k_2}, \ldots b_{k_s}, b_{k_1}, b_{k_2}, \ldots.$$

Аналогично выписываем ключ p над второй таблицей.

1.3. *Процедура шифрования открытого текста.*

Пусть задан открытый текст $a_{h_1}a_{h_2}\dots a_{h_u}$. По формуле (2.1.1) преобразуем его в два текста. Имеем

$$b_{h_1}b_{h_2}\dots b_{h_u};\quad c_{h_1}c_{h_2}\dots c_{h_u}.$$

На пересечении h_1-го столбца и k_1-й строки в первой таблице находим символ x_1, а на пересечении h_1-го столбца и p_1-й строки второй таблицы находим символ y_1. Повторим эту процедуру для следующего символа a_{h_2} и т.д. Получим шифрованный текст

$$x_1y_1x_2y_2\dots x_uy_u$$

или два шифрованных текста $x_1x_2\dots x_u$ и $y_1y_2\dots y_u$, или $z_1z_2\dots z_u$, где $z_t = qx_t + dy_t, 1 \le t \le u$.

1.4. *Процедура расшифрования.*

По ключам k и p в первой и второй таблицах Виженера находим строки с номерами k_1 и p_1 соответственно. На этих строках находим элементы x_1 в первой таблице и y_1 во второй таблице, а затем по этим элементам находим, отвечающие им столбцы, и получаем элементы b_{h_1} и c_{h_1}. По тому же правилу восстанавливаются элементы b_{h_2} и c_{h_2} и т. д.

Далее, используя формулу (2.1.1), по паре символов (b_{q_t}, c_{q_t}) находим символ a_{q_t}, $t = 1,\dots,u$. Процедура расшифрования завершена.

§2. p-адическая метрика поля рациональных чисел Q

Пусть k — поле. Тогда отображение $\phi : k \to \mathbf{R}_+$ называется *метрикой,* если

1) $\forall\alpha \in k \quad \phi(\alpha) > 0, \phi(0) = 0$;

2) $\forall\alpha,\beta \in k \quad \phi(\alpha+\beta) \le \phi(\alpha) + \phi(\beta)$;

3) $\forall\alpha,\beta \in k \quad \phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$.

Пара (k,ϕ) называется *метризованным полем.* Последовательность α_n из k называется сходящейся к элементу α, если $\phi(\alpha_n - \alpha) \to 0$ при $n \to \infty$. Говорят, что α_n *фундаментальная последовательность,* если она удовлетворяет условию Коши: для всякого $\varepsilon > 0$ найдется номер n_0 такой, что для всех $n, m > n_0$ имеем $\phi(\alpha_n - \alpha_m) < \varepsilon$. Метризованное поле (k,ϕ) называется *полным,* если любая фундаментальная последовательность сходится к элементу поля k. Для любого метризованного поля k существует полное метризованное поле $\bar{k}$, содержащее k в качестве всюду плотного подполя. Поле $\bar{k}$ определяется однозначно с точностью до топологического изоморфизма, оставляющего элементы поля k на месте.

Поле p-адических чисел $\mathbf{Q_p}$ — это пополнение поля рациональных $\mathbf{Q}$ по p-адической метрике $\phi_p(x) = \rho^{\nu_p(x)}$, где ρ — любое фиксированное число с условием $0 < \rho < 1$, а символ $\nu_p(x)$ означает содержание простого числа p в рациональном числе x.

Согласно известной теореме А. Островского все нетривиальные метрики поля рациональных чисел исчерпываются вещественной метрикой и p-адическими метриками для всех простых чисел p.

Из всякой ограниченной последовательности p-адических чисел $\mathbf{Q_p}$ можно выделить сходящуюся подпоследовательность.

Любое $\xi \in \mathbf{Q_p}$ является пределом последовательности рациональных чисел по p-адической метрике.

В поле $\mathbf{Q_p}$ справедлив критерий Коши.

Ряд $\Sigma\xi_n$, $\xi_n \in \mathbf{Q_p}$, сходится тогда и только тогда, когда $\lim\limits_{n\to\infty} \phi_p(\xi_n) = 0$.

Любая перестановка членов сходящегося ряда из $\mathbf{Q_p}$ не нарушает сходимости и при перестановке его сумма не изменяется.

Если два ряда сходятся, то при любой перестановке попарных произведений их членов ряд, являющийся произведением этих рядов сходится к произведению их сумм.

Каждое $\xi \in \mathbf{Q_p} \setminus \{0\}$ однозначно представляется в виде $\xi = p^m\varepsilon$, где $m = \nu_p(\xi)$, а

$$\varepsilon = \sum_{n=0}^{\infty} a_n p^n, \quad 1 \le a_0 < p, \quad 0 \le a_n < p \forall n > 0.$$

Арифметические операции (четыре арифметических действия) над сходящимися рядами дают сходящиеся ряды. Суперпозиция сходящихся рядов приводит к сходящемуся ряду.

2.1. *p-адическое обобщение малой теоремы Ферма. Теорема А. Г. Постникова.*

Пусть p — простое число, $\{a_n\}$ — последовательность p-адических чисел из $\mathbf{Q_p}$. Тогда последовательность

$$a'_n = \Delta a_n = \frac{a_{n+1} - a_n}{p^n}$$

называется *производной последовательностью* по Шуру. Далее определим индуктивно высшую производную

$$a_n^{(\nu)} = \Delta^\nu a_n = \Delta(a_n^{\nu-1}) = \Delta(\Delta^{\nu-1} a_n).$$

Малая теорема Ферма имеет вид.

Теорема 2.1. *Пусть a — целое p-адическое число. Тогда последовательность*

$$\Delta a^{p^n} = \frac{a^{p^{n+1}} - a^{p^n}}{p^{n+1}}$$

будет состоять из целых p-адических чисел.

И. Шур в подтверждение такой трактовки малой теоремы Ферма доказал интересное ее обобщение.

Теорема 2.2. *Пусть a — целое p-адическое число и $p \not| a$. Тогда следующие производные последовательности*

$$\Delta a^{p^n}, \Delta^2 a^{p^n}, \ldots, \Delta^{p-1} a^{p^n},$$

состоят из целых p-адических чисел.

Более того, если

$$\frac{a^{p-1} - 1}{p} \equiv 0 \pmod{p},$$

то $\Delta^r a^{p^n}, r = 1, \ldots, p-1$, состоят из целых p-адических чисел. Если же

$$\frac{a^{p-1} - 1}{p} \not\equiv 0 \pmod{p},$$

то для любого n число p в точности делит знаменатель $\Delta^p a^{p^n}$.

Важное приложение p-адических рядов к теории L-рядов Дирихле в 1955 г. дал А. Г. Постников [4].

Теорема 2.3. *Пусть g — первообразный корень по модулю p^n, p — простое и n — натуральное,* $\mathrm{ind}_g(k)$ *— индекс натурального числа k по модулю p^n относительно первообразного корня g. Тогда справедлива формула*

$$\frac{\mathrm{ind}_g(1 + pu)}{p - 1} \equiv \Lambda f(u) \pmod{p^{n-1}},$$

где $f(u)$ — многочлен степени $n-1, \Lambda$ — некоторая целочисленная постоянная.

Это утверждение является p-адическим аналогом классического разложения при $|x| < 1$ для логарифма

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots.$$

§3. Об одной цифровой подписи и блочном шифре

3.1. *О цифровой подписи.*

Дадим обобщение цифровой подписи М. О. Рабина [11] (см. также [10]). Оно связано с рассмотрением чисел по модулю, равному степени простого числа.

Пусть абонент $\mathcal{A}$ создает цифровую подпись и передает ее по открытому каналу связи абоненту $\mathcal{B}$. В качестве секретного ключа абонент $\mathcal{A}$ выбирает большие нечетные простые числа p и q, сравнимые с 3 по модулю 4 и два натуральных числа a и b. Открытый ключ состоит из двух чисел $n = p^a$ и $r = p^b$. Секретный ключ известен только абоненту $\mathcal{A}$.

Далее абоненту $\mathcal{A}$ присваивается некоторая метка Q — натуральное число.

Затем выбирается часть L передаваемого сообщения m. Числа L и Q обязаны удовлетворять следующим условиям

$$(L,p)=1, 0<L<n, \left(\frac{L}{p}\right)=1, (Q,q)=1, 0<Q<r, \left(\frac{Q}{q}\right)=1.$$

Если для чисел L или Q не выполняется хотя бы одно из этих условий, то абонент $\mathcal{A}$ заменяет в случае необходимости число L на $L \pm 1$ и метку Q на $Q \pm 1$. Он повторяет эту процедуру до тех пор, пока не найдет числа L и Q, удовлетворяющие приведенным выше условиям.

Абонент $\mathcal{A}$ образует новое сообщение C_1, C_2, где $0 < C_1 < n, 0 < C_2 < r$, вида

$$L \equiv C_1^2 \pmod{n}, Q \equiv C_2^2 \pmod{r},$$

и передает числа C_1, C_2 и L, Q, а также те величины, на которые изменились числа L и Q, по открытому каналу связи абоненту $\mathcal{B}$. Эти четыре числа C_1, C_2, L, Q и образуют цифровую подпись.

Решения C_1, C_2 строятся абонентом $\mathcal{A}$, обладающим секретными ключами p, q и a, b. Сравнения $L \equiv C_1^2 \pmod{n}$ и $Q \equiv C_2^2 \pmod{r}$ решаются единым алгоритмом. Поэтому рассмотрим сравнение $H \equiv x^2 \pmod{p^s}$, где заданы натуральные числа H, s, простое число p, и величина x является неизвестной. Представим переменную x в виде $x \equiv u_\nu \pmod{p^{\nu+1}}$, где $u_\nu = u_{\nu-1} + x_\nu p^\nu, \nu \geq 1, u_0 = x_0$, и координаты $x_0, x_1, \ldots, x_{s-1}$ изменяются в пределах от 0 до $p-1$. Решим сначала сравнение

$$H \equiv x_0^2 \pmod{p}.$$

Все его решения суть: $x_0 \equiv \pm H^{(p+1)/4} \pmod{p}$. Из двух найденных значений величины x_0 возьмем то, которое является квадратичным вычетом по модулю p, и обозначим его y_0, причем $0 < y_0 < p$.

Далее, предположим, что найдено $u_{\nu-1}$ при $\nu \geq 1$, причем $u_0 = y_0$. Найдем значение u_ν при $\nu \geq 1$. Имеем цепочку сравнений

$$H \equiv (u_{\nu-1} + p^\nu x_\nu)^2 \pmod{p^{\nu+1}},$$

$$H \equiv u_{\nu-1}^2 + 2p^\nu u_{\nu-1} x_\nu \pmod{p^{\nu+1}},$$

$$x_\nu \equiv (H - u_{\nu-1}^2)(2u_{\nu-1})^{-1} \pmod{p},$$

поскольку $H \equiv x_0^2 \pmod{p}$, $H \equiv u_{\nu-1}^2 \pmod{p^\nu}$ и $2u_{\nu-1} \equiv 2x_0 \pmod{p}$, $2x_0 \not\equiv 0 \pmod{p}$.

Абонент $\mathcal{B}$ и представитель третьей стороны могут проверить подлинность подписи с помощью открытого ключа n. Для этого вычисляются значения $L' \equiv C_1^2 \pmod{n}$ и $Q' \equiv C_2^2 \pmod{r}$. Достаточно установить, что $L' = L, Q' = Q$.

3.2. *О блочном шифре.*

Пусть задан открытый текст, представленный в цифровом виде числом m, имеющим в двоичной записи k цифр. Возьмем любое натуральное число r, удовлетворяющее условиям $1 \leq r \leq k/2$. Разобьем число m на блоки, представив его в виде

$$m = m_1 + m_2 2^r + \cdots + m_n 2^{(n-1)r},$$

где $0 \leq m_1, \ldots, m_n < 2^r$ и $(n-1)r \leq k < nr$.

Расположим числа $m_1, \ldots, m_n$ в порядке возрастания, при этом отметим места, где встречаются равные числа m_s и числа m_s, равные нулю. Далее, выбросим все m_s, равные нулю и оставим по одному экземпляру из ненулевых равных чисел. Получим $0 < \tilde{m}_1 < \cdots < \tilde{m}_d < 2^r$.

Затем найдем сумму $\tilde{m}_1 + \cdots + \tilde{m}_d = N_1$. Очевидно, имеем $d(d+1)/2 \leq N_1 < d2^r$. Выберем простое число p, находящееся в промежутке $N_1 \leq p < 2N_1$. Предположим, что $\tilde{m}_s \not\equiv \tilde{m}_t \pmod{p}$ для всех $s \neq t, 1 \leq s, t \leq d$. Наконец, найдем суммы вторых,..., d-х степеней чисел $\tilde{m}_1, \ldots, \tilde{m}_d$. Получим

$$\begin{cases} \tilde{m}_1 + \cdots + \tilde{m}_d = N_1, \\ \tilde{m}_1^2 + \cdots + \tilde{m}_d^2 = N_2, \\ \cdots \quad \cdots \quad \cdots \\ \tilde{m}_1^d + \cdots + \tilde{m}_d^d = N_d. \end{cases} \tag{5.2.1}$$

Заметим, что $p \geq N_1 \geq \tilde{m}_d > \cdots > \tilde{m}_1$.

Числа $N_1, \ldots, N_d$ составят часть шифртекста.

Покажем, как по этим числам можно восстановить числа $\tilde{m}_1, \ldots, \tilde{m}_d$. Рассмотрим систему сравнений

$$\begin{cases} x_1 + \cdots + x_d \equiv N_1 \pmod{p}, \\ x_1^2 + \cdots + x_d^2 \equiv N_2 \pmod{p}, \\ \ldots \quad \ldots \quad \ldots \\ x_1^d + \cdots + x_d^d \equiv N_d \pmod{p}. \end{cases} \tag{5.2.2}$$

Эта система сравнений имеет единственное решение $0 < \nu_{1,0} < \cdots < \nu_{d,0} \leq p$, причем $\nu_{1,0} \equiv \tilde{m}_1 \pmod{p}, \ldots, \nu_{d,0} \equiv \tilde{m}_d \pmod{p}$.

Действительно, пусть при $1 \leq s \leq d$ символ $\sigma_s = \sigma_s(x_1, \ldots, x_d)$ обозначает s-ю элементарную симметрическую функцию. Тогда при $p > d$ из формул Ньютона—Варинга (см., например, [3, с. 60–61])

$$N_s - N_{s-1}\sigma_1 + \cdots + (-1)^s s\sigma_s \equiv 0 \pmod{p}$$

функции $\sigma_1, \ldots, \sigma_d$ однозначно выражаются через суммы степеней $N_1, \ldots, N_d$. С другой стороны, в поле из p элементов многочлен $f(z) = z^d - \sigma_1 z^{d-1} + \cdots + (-1)d\sigma_d$ однозначно разлагается на линейные множители $f(z) = (z - x_1) \ldots (z - x_d)$. Тем самым, с точностью до перестановки находятся корни $\nu_{1,0}, \ldots, \nu_{d,0}$ предыдущей системы сравнений.

Пусть при $1 \leq s \leq d$ найдены решения $u_{1,s-1}, \ldots, u_{d,s-1}$ системы сравнений

$$\begin{cases} u_{1,s-1} + \cdots + u_{d,s-1} \equiv N_1 \pmod{p^{s-1}}, \\ u_{1,s-1}^2 + \cdots + u_{d,s-1}^2 \equiv N_2 \pmod{p^{s-1}}, \\ \ldots \quad \ldots \quad \ldots \\ u_{1,s-1}^d + \cdots + u_{d,s-1}^d \equiv N_d \pmod{p^{s-1}}. \end{cases}$$

Далее будем искать решение $u_{1,s}, \ldots, u_{d,s}$ системы сравнений по модулю p^s. При $1 \leq t, s \leq d$ положим $u_{t,s} = u_{t,s-1} + p^{s-1}x_{t,s}$. Имеем систему сравнений

$$\begin{cases} u_{1,s} + \cdots + u_{d,s} \equiv N_1 \pmod{p^s}, \\ u_{1,s}^2 + \cdots + u_{d,s}^2 \equiv N_2 \pmod{p^s}, \\ \ldots \quad \ldots \quad \ldots \\ u_{1,s}^d + \cdots + u_{d,s}^d \equiv N_d \pmod{p^s}. \end{cases} \tag{5.2.3}$$

Эта система сравнений эквивалентна следующей линейной относительно неизвестных $x_{1,s}, \ldots, x_{d,s}$ системе сравнений вида

$$\begin{cases} x_{1,s} + \cdots + x_{d,s} \equiv N_1^{'} \pmod{p}, \\ u_{1,s-1}x_{1,s} + \cdots + u_{d,s-1}x_{d,s} \equiv N_2^{'} \pmod{p}, \\ \ldots \quad \ldots \quad \ldots \\ u_{1,s-1}^{d-1}x_{1,s} + \cdots + u_{d,s-1}^{d-1}x_{d,s} \equiv N_d^{'} \pmod{p}, \end{cases} \tag{5.2.4}$$

где $p^{s-1}N_l^{'} \equiv N_l - u_{1,s-1}^l - \cdots - u_{d,s-1}^l \pmod{p^s}$ при $1 \le l \le d$.

Поскольку для всех $t = 1, \ldots, d$ имеем $u_{t,s-1} \equiv \nu_{t,0} \pmod{p}$, определитель системы сравнений является определителем Вандермонда с элементами $\nu_{1,0}, \ldots, \nu_{d,0}$, не сравнимыми между собой по модулю p, т. е. этот определитель отличен нуля. Следовательно, предыдущая система сравнений имеет единственное решение $x_{1,s} \equiv \nu_{1,s} \pmod{p}, \ldots, x_{d,s} \equiv \nu_{d,s} \pmod{p}$.

Таким образом, при $s = d$ из предыдущей системы сравнений получим ее единственное решение вида

$$u_{t,d} = \nu_{t,0} + p\nu_{t,1} + \cdots + p^{d-1}\nu_{t,d} \equiv \tilde{m}_t \pmod{p^d},\ 1 \le t \le d.$$

Кроме того, так как $0 \le u_{t,d} < p^d$ и $0 < \tilde{m}_t < N_1 \le p^d$, то $u_{t,d} = \tilde{m}_t$ при всех $t = 1, \ldots, d$.

Тем самым, доказано, что по числам $N_1, \ldots, N_d$ однозначно восстанавливаются числа $\tilde{m}_1, \ldots, \tilde{m}_d$.

Таким образом, весь шифрованный текст будет состоять из натуральных чисел $N_1, \ldots, N_d$, указания мест расположения нулевых чисел m_s, т. е. указания индексов s для нулевых m_s, далее указания индексов индексов чисел m_t в порядке возрастания $\tilde{m}_s, 1 \le s \le d$ и простого числа p.

Восстановление открытого текста по приведенному шифртексту проведем по следующим шагам.

1. Вычислим $\sigma_d = \sigma_d(N_1, \ldots, N_d)$, где $\sigma_d = \tilde{m}_1 \ldots \tilde{m}_d$.

2. Найдем $\tilde{\sigma}_d \equiv \sigma_d \pmod{p}$. Поскольку при всех $t = 1, \ldots, d$ справедливы сравнения $\tilde{m}_t \equiv \nu_{t,0} \pmod{p}$, имеем $\tilde{\sigma}_d \equiv \tilde{m}_1 \ldots \tilde{m}_d \pmod{p}$. Последнее обстоятельство упрощает перебор наборов при поиске решения системы сравнений (5.2.2) по модулю p.

3. При $s = 1, \ldots, d$ находим решение $u_{1,s}, \ldots, u_{d,s}$ системы сравнений (5.2.3), решая линейную систему сравнений (5.2.4). Тем самым будут найдены $\tilde{m}_1, \ldots, \tilde{m}_d$.

4. Так как имеется взаимно однозначное соответствие между набором $\tilde{m}_1, \ldots, \tilde{m}_d$ и набором $m_1, \ldots, m_n$, то открытый текст будет восстановлен.

Заметим, что избавиться от условия, что числа $\tilde{m}_t, 1 \leq t \leq d$, не сравнимы между собой по модулю p, можно добавлением к каждому из этих чисел натуральных слагаемых, не превосходящих d.

§4. Полные арифметические суммы значений многочленов Бернулли от произвольного рационального многочлена

Нам представляется полезным в качестве приложения рассмотреть следующую сумму с многочленом Бернулли $B_s(x)$. Заметим,что для этих сумм удается построить теорию, аналогичную анализу Фурье для тригонометрических функций.

Полная рациональная арифметическая сумма от функции $\rho_s(x) = B_s(\{x\})$ имеет вид

$$S = S\left(\frac{f(x)}{q}\right) = \sum_{x=1}^{q} \rho_s\left(\frac{f(x)}{q}\right),$$

где $q > 1$ — натуральное число, $f(x) = a_n x^n + \cdots + a_1 x + a_0$ — многочлен степени $n \geq 1$, причем $(a_n, \ldots, a_1, q) = 1$.

4.1. *Гауссова теорема умножения для многочленов Бернулли.*

Нам необходима следующая известная формула Гаусса умножения для многочленов Бернулли.

Лемма 4.1.1. *Пусть n — натуральное число, $(a, n) = 1$. Тогда для любого вещественного числа x имеем*

$$n^{1-s} B_s(nx) = B_s(x) + B_s\left(x + \frac{a}{n}\right) + \cdots + B_s\left(x + \frac{a(n-1)}{n}\right).$$

Из леммы 4.1.1 выведем следующее утверждение.

Лемма 4.1.2. *Пусть n — натуральное число, $(a, n) = 1$. Тогда для любого вещественного числа x имеем*

$$n^{1-s} B_s(\{nx\}) = B_s(\{x\}) + B_s\left(\left\{x + \frac{a}{n}\right\}\right) + \cdots + B_s\left(\left\{x + \frac{a(n-1)}{n}\right\}\right).$$

Доказательство. Левая и правая части равенства имеют период, равный $1/n$. Действительно,

$$B_s\left(n\left\{x + \frac{1}{n}\right\}\right) = B_s(\{nx + 1\}) = B_s(\{nx\});$$

$$\sum_{m=0}^{n-1} B_s\left(\left\{x+\frac{am}{n}\right\}\right)=\sum_{m=0}^{n-1} B_s\left(\left\{x+\frac{m}{n}\right\}\right),$$

поскольку am пробегает полную систему вычетов по модулю n при $(a,n)=1$, если m пробегает полную систему вычетов по модулю n; далее

$$\sum_{m=0}^{n-1} B_s\left(\left\{x+\frac{1}{n}+\frac{m}{n}\right\}\right)=\sum_{m=0}^{n-1} B_s\left(\left\{x+\frac{m+1}{n}\right\}\right)=$$

$$=\sum_{m=1}^{n} B_s\left(\left\{x+\frac{m}{n}\right\}\right)=\sum_{m=0}^{n-1} B_s\left(\left\{x+\frac{m}{n}\right\}\right).$$

Поэтому достаточно доказать равенство при $0\le x<1/n$. Для целых $0\le m\le n-1$ имеем

$$\{nx\}=nx,\left\{x+\frac{m}{n}\right\}=x+\frac{m}{n},$$

$$\sum_{m=0}^{n-1} B_s\left(\left\{x+\frac{m}{n}\right\}\right)=\sum_{m=0}^{n-1} B_s\left(x+\frac{m}{n}\right),$$

$$B_s(\{nx\}))=B_s(nx).$$

Следовательно, по теореме умножения (лемма 4.1.1) получаем искомую формулу. Лемма доказана.

Утверждение леммы 4.1.2 можно записать в виде.

$$n^{1-s}\rho_s(nx)=\rho_s(x)+\rho_s\left(x+\frac{a}{n}\right)+\cdots+\rho_s\left(x+\frac{a(n-1)}{n}\right).$$

4.2. *Редукция полных рациональных арифметических сумм по произвольному модулю к суммам по модулям, равным степеням простых чисел.*

Лемма 4.2.1. *Пусть* $(q_1,q_2)=1, f(x)=a_nx^n+\dots a_1x+a_0=g(x)+a_0$ *— многочлены с целыми коэффициентами. Тогда справедливо равенство*

$$S\left(\frac{f(x)}{q_1q_2}\right)=S\left(\frac{q_2^{-1}g(q_2x_1)}{q_1}+\frac{q_1^{-1}g(q_1x_2)}{q_2}+\frac{a_0}{q_1q_2}\right), \qquad \text{(I.2.1)}$$

где x, x_1, x_2 пробегают соответственно полные системы вычетов по модулям q_1q_2, q_1, q_2.

Доказательство. Пусть x_1 и x_2 пробегают независимо соответственно полные системы вычетов по модулям q_1 и q_2. Тогда x вида

$$x \equiv q_2x_1 + q_1x_2 \pmod{q_1q_2}$$

пробегает полную систему вычетов по модулю q_1q_2 и наоборот.

Отсюда находим

$$g(x) \equiv g(q_2x_1) + g(q_1x_2) \pmod{q_1q_2},$$

что немедленно приводит к искомому равенству.

4.3. *"Подъем" решений полиномиального сравнения по модулю, равному степени простого числа.*

Лемма 4.3.1. *Пусть p — простое число, $g(x)$ — многочлен с целыми коэффициентами, a — корень кратности m сравнения $g(x) \equiv 0 \pmod p$, и пусть u — наибольшая степень числа p, делящая все коэффициенты многочлена $h(x) = g(px + a)$. Тогда число корней сравнения*

$$p^{-u}h(x) \equiv 0 \pmod p$$

с учетом их кратностей не превосходит m.

Доказательство см., например, в [14, с. 55, лемма 2].

Лемма 4.3.2. *Пусть p — простое число, $f(x) = a_nx^n + \cdots + a_1x + a_0$ — многочлен с целыми коэффициентами, $(a_n, \ldots, a_1, p) = 1$, и пусть u — наивысшая степень числа p, делящая все коэффициенты многочлена $g(x) = f(\lambda + px) - f(\lambda)$. Тогда имеем $1 \le u \le n$.*

Доказательство см., например, [14, с.56, лемма 3].

4.4. *Редукция к линейным сравнениям.*

Пусть p — простое число, $l \ge 2$ — натуральное число, $f(x) = \sum\limits_{k=0}^{n} a_kx^k$, $(a_n, \ldots, a_1, p) = 1$. Рассмотрим сначала случай, когда p превосходит степень многочлена f, т. е. $p > n$. Представим сумму $S\left(\frac{f(x)}{p^l}\right)$ в виде

$$S\left(\frac{f(x)}{p^l}\right) = \sum_{\xi=1}^{p} S_\xi, \quad S_\xi = \sum_{\substack{x=1 \\ x \equiv \xi \pmod p}}^{p^l} \rho_s\left(\frac{f(x)}{p^l}\right). \tag{I.4.1}$$

Имеем следующее утверждение.

Лемма 4.4.1. *Пусть* $f'(\xi) \not\equiv 0 \pmod p$. *Тогда* $S_\xi = p^{(1-s)(l-1)}\rho_s\left(\frac{f(\xi)}{p}\right)$.

Доказательство. Имеем

$$S_\xi = \sum_{\substack{y=1 \\ y\equiv\xi \pmod p}}^{p^{l-1}} \sum_{z=0}^{p-1} \rho_s\left(\frac{f(y+p^{l-1}z)}{p^l}\right) =$$

$$= \sum_{\substack{y=1 \\ y\equiv\xi \pmod p}}^{p^{l-1}} \sum_{z=0}^{p-1} \rho_s\left(\frac{f(y)}{p^l} + \frac{f'(y)z}{p}\right). \qquad \text{(I.4.2)}$$

Воспользуемся леммой 4.1.2. Найдем

$$S_\xi = p^{1-s} \sum_{\substack{y=1 \\ y\equiv\xi \pmod p}}^{p^{l-1}} \rho_s\left(\frac{f(y)}{p^{l-1}}\right).$$

Повторяя эту процедуру $l-2$ раза, получим утверждение леммы.

Лемма 4.4.2. *Пусть* $f'(\xi) \equiv 0 \pmod p$. *Тогда*

$$S_\xi = \sum_{\substack{y=1 \\ y\equiv\xi \pmod p}}^{p^{l-1}} \rho_s\left(\frac{f(y)}{p^l}\right) p = p\sum_{y=1}^{p^{l-2}} \rho_s\left(\frac{f(\xi+py)}{p^l}\right).$$

Доказательство. Из равенства (I.4.2) получим утверждение леммы 4.4.2.

4.5. *Цепочка показателей и оценка полной рациональной арифметической суммы.*

Теорема 4.5.1. *Пусть* $n \geq 2$ *— целое число,* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *— многочлен с целыми коэффициентами,* $(a_n, \ldots, a_1, p) = 1, p > n$ *— простое число и* l *— натуральное число, и пусть* j *— наименьшая длина цепочки показателей* $(u_1, u_2, \ldots)$. *Тогда, если* $u_1 + \cdots + u_j \geq l, u_1 + \cdots + u_j + u_{j-1} = l - 1$, *то имеем оценку*

$$\left|S\left(\frac{f(x)}{p^l}\right)\right| \leq n^2 p^{l-j-1/2};$$

если же $u_1 + \cdots + u_j \geq l, u_1 + \cdots + u_j + u_{j-1} < l - 1$, *то имеем*

$$\left| S\left(\frac{f(x)}{p^l}\right)\right| \leq np^{l-j}.$$

Приведем только схему вывода оценки суммы из утверждения теоремы.

Пусть кратность корня ξ сравнения $f'(x) \equiv 0 \pmod p$ равна $n > m \geq 1$ и u_1 — наивысшая степень числа p, делящая все коэффициенты многочлена

$$f(\xi + py) - f(\xi) = p^{u_1} f_1(y) = \sum_{k=1}^{n} \frac{f^{(k)}(\xi)}{k!}(py)^k.$$

Из леммы I.3.2 следует, что $2 \leq u_1 \leq n$.

При $l \leq u_1$ по лемме 4.4.2 получим

$$S_\xi = p^{l-1}\rho_s\left(\frac{f(\xi)}{p^l}\right). \tag{I.5.1}$$

Далее, при $l > u_1$ находим

$$S_\xi = p\sum_{y=1}^{p^{l-2}} \rho_s\left(\frac{f(\xi)}{p^l} + \frac{f_1(y)}{p^{l-u_1}}\right).$$

Представим y в виде $y = z + p^{l-u_1}t$, где $1 \leq z \leq p^{l-u_1}, 0 \leq t \leq p^{u_1-2} - 1$. Тогда сумма S_ξ примет вид

$$S_\xi = p^{u_1-1}\sum_{z=1}^{p^{l-u_1}} \rho_s\left(\frac{f(\xi)}{p^l} + \frac{f_1(z)}{p^{l-u_1}}\right).$$

При $l > u_1$ преобразуем сумму S_ξ, если $f'(\xi) \equiv 0 \pmod p$. Имеем

$$S_\xi = p^{u_1-1}\sum_{\xi_1=1}^{p} S_{\xi,\xi_1}, \quad S_{\xi,\xi_1} = \sum_{\substack{z=1 \\ z\equiv\xi_1 \pmod p}}^{p^{l-u_1}} \rho_s\left(\frac{f(\xi)}{p^l} + \frac{f_1(z)}{p^{l-u_1}}\right).$$

Пусть сначала $f_1'(\xi_1) \not\equiv 0 \pmod p$. Тогда аналогично предыдущему получим

$$S_{\xi,\xi_1} = p^{(1-s)(l-1)}\rho_s\left(\frac{f(\xi)}{p^{u_1-1}} + \frac{f_1(\xi_1)}{p}\right).$$

Пусть теперь $f_1'(\xi_1) \equiv 0 \pmod p$, кратность корня ξ_1 равна m_1 и p^{u_2} — наивысшая степень числа p, делящая все коэффициенты многочлена

$$f_1(pt + \xi_1) - f_1(\xi_1) = p^{u_2} f_2(t).$$

Из лемм 4.4.1 и 4.4.2 имеем $2 \le u_2 \le u_1 \le n, m_2 \le m_1$.

При $l \le u_1 + u_2$ найдем

$$S_{\xi,\xi_1} = p^{u_1-1} \sum_{t=1}^{p^{l-u_1-1}} \rho_s \left(\frac{f(\xi)}{p^l} \right) = p^{l-2} \rho_s \left(\frac{f(\xi)}{p^l} \right).$$

При $l > u_1 + u_2$ получим

$$S_{\xi,\xi_1} = \sum_{\substack{z=1 \\ z \equiv \xi_1 \pmod p}}^{p^{l-u_1}} \rho_s \left(\frac{f(\xi)}{p^l} + \frac{f_1(z)}{p^{l-u_1}} \right) =$$

$$= p \sum_{t=1}^{p^{l-u_1-2}} \rho_s \left(\frac{f(\xi)}{p^l} + \frac{f_1(\xi_1)}{p^{l-u_1}} + \frac{f_2(t)}{p^{l-u_1-u_2}} \right) =$$

$$= p^{u_2-1} \sum_{t=1}^{p^{l-u_1-u_2}} \rho_s \left(\frac{f(\xi)}{p^l} + \frac{f_1(\xi_1)}{p^{l-u_1}} + \frac{f_2(t)}{p^{l-u_1-u_2}} \right).$$

Продолжая предыдущие рассмотрения, получим наборы корней сравнений $(\xi, \xi_1, \dots)$ и отвечающий каждому из этих наборов единственный набор показателей $(u_1, u_2, \dots, u_t)$, где величина $t = t(\xi, \xi_1, \dots)$ определяется с помощью соотношений

$$u_1 + \dots + u_t \ge l > u_1 + \dots + u_{t-1},$$

причем из леммы 4.3.1 имеем, что количество наборов показателей $(u_1, \dots, u_t)$ не превосходит степени n многочлена $f(x)$ и справедливы неравенства $n \ge u_1 \ge u_2 \ge \dots \ge u_t \ge 2$. Отсюда получаем искомую оценку.

4.6. *Средние значения полных рациональных арифметических сумм.*

Пусть $n \ge 2, f(x) = a_n x^n + \dots + a_1 x + a_0$ — многочлен с целыми коэффициентами, p — простое число и $(a_n, \dots, a_1, p) = 1$. Назовем

средним значением $\sigma_p = \sigma_p(k;\rho_s)$ *полной рациональной арифметической суммы*

$$S\left(\frac{f(x)}{p^s}\right) = \sum_{x=1}^{p^s} \rho_s\left(\frac{f(x)}{p^s}\right)$$

выражение вида

$$\sigma_p = 1 + \sum_{t=1}^{+\infty} A(p^t), \quad A(p^t) = \sum_{\substack{a_n=0 \\ (a_n,\ldots,a_1,p)=1}}^{p^t-1} \cdots \sum_{a_1=0}^{p^t-1} \sum_{a_0=0}^{p^t-1} \left| p^{-t} S\left(\frac{f(x)}{p^t}\right)\right|^{2k}.$$

Теорема 4.6.1. *Ряд* σ_p *сходится при* $2k > (n^2+n)/2+1$ *и расходится при* $2k \le (n^2+n)/2+1$.

Пусть $f_g(x) = a_n x^n + a_m x^m + \cdots + a_r x^r + a_0$ — "выщербленный" многочлен с целыми коэффициентами, $1 \le r < \cdots < m < n, r + \cdots + m + n < (n^2+n)/2$, и пусть $\varsigma = \varsigma(k;\rho_s;f_g)$ — среднее значение полной рациональной арифметической суммы от ρ_s-функции с "выщербленным" многочленом $f_g(x)$ в аргументе, т. е.

$$\varsigma_p = 1 + \sum_{t=1}^{+\infty} \mathcal{A}(p^t), \quad \mathcal{A}(p^t) = \sum_{\substack{a_n=0 \\ (a_n,a_m,\ldots,a_r,p)=1}}^{p^t-1} \sum_{a_m=0}^{p^t-1} \cdots \sum_{a_r=0}^{p^t-1} \sum_{a_0=0}^{p^t-1} \left| p^{-t} S\left(\frac{f_g(x)}{p^t}\right)\right|^{2k}.$$

Теорема 4.6.2. *Ряд* ς_p *сходится при* $2k > n+m+\cdots+r$ *и расходится при* $2k \le n+m+\cdots+r$. Теоремы 4.6.1 и 4.6.2 стандартным образом выводятся из теоремы 4.5.1.

4.7. *Кратные полные рациональные арифметические суммы.*

Приведем оценку модуля полной рациональной кратной арифметической суммы с ρ-функцией, аргумент которой является многочленом от нескольких переменных.

Теорема 4.7.1. *Пусть* $n, \alpha \ge 2$ *— натуральные числа,* p *— простое число,*

$$F(x_1,\ldots,x_r) = \sum_{t_1=0}^{n} \cdots \sum_{t_r=0}^{n} a(t_1,\ldots,t_r) x_1^{t_1} \ldots x_r^{t_r}$$

многочлен с целыми коэффициентами, взаимно простыми в совокупности с p*, исключая свободный член* $a(0,\ldots,0)$*, и пусть*

$$S\left(\frac{F(x_1,\ldots,x_r)}{p^\alpha}\right) = \sum_{x_1=1}^{p^\alpha} \cdots \sum_{x_r=1}^{p^\alpha} \rho_s\left(\frac{F(x_1,\ldots,x_r)}{p^\alpha}\right).$$

Тогда имеем оценку

$$\left|S\left(\frac{F(x_1,\ldots,x_r)}{p^\alpha}\right)\right| \ll_{n,r,s} (\alpha+1)^{r-1}p^{\alpha(r-1/n)}.$$

Далее, пусть $\sigma_p^{(r)} = \sigma(k;\rho_s)$ — среднее значение полной рациональной арифметической суммы от ρ_s-функции

$$\sigma_p^{(r)} = 1 + \sum_{q=1}^{+\infty} A_r(p^q),$$

$$A_r(p^q) = \sum_{\substack{a_{n,\ldots,n}=0 \\ (a_{n,\ldots,n},\ldots,a_{1,0,\ldots,0},p)=1}}^{p^q-1} \cdots \sum_{a_{1,0,\ldots,0}=0}^{p^q-1} \sum_{a_{0,\ldots,0}=0}^{p^q-1} \left|p^{-qr}S\left(\frac{F(x_1,\ldots,x_r)}{p^q}\right)\right|^{2k}.$$

Тогда ряд $\sigma_p^{(r)}$ сходится при $2k > n(n+1)^r$ и расходится при $2k < \sum_{l=1}^{n} l^t \sim \frac{(n+1)^{r+1}}{r+1}$.

Работа выполнена при финансовой поддержке РФФИ, грант № 16-01-00-071.

Список литературы

1. Виноградов И. М. Основы теории чисел. — Москва—Ижевск: НИЦ «Регулярная и хаотическая динамика», 2005. — 176 с.

2. Виноградов И. М. Особые варианты метода тригонометрических сумм. — М.: Наука, 1976. — 120 с.

3. Виноградов И. М. Метод тригонометрических сумм в теории чисел. — М.: Наука, 1980. — 144 с.

4. Постников А. Г. Избранные труды. — М.: ФИЗМАТЛИТ, 2005. — 512 с.

5. Минеев М. П., Чубариков В. Н. Задача об искажении частоты появления знаков в шифре простой замены // Математические вопросы кибернетики. Вып. 16. — 2007. — С. 242–245.

6. Минеев М. П., Чубариков В. Н. Об одном методе искажения частоты появления знаков в шифре простой замены // Докл. РАН. — 2008. — Т. 420, №6. — С. 736–738.

7. Минеев М. П., Чубариков В. Н. К вопросу об искажении частот появления знаков в шифре простой замены // Докл. РАН. — 2009. — Т. 426, №1. — С. 6–8.

8. Баричев С. Криптография без секретов (`www.artelecom.ru/library/books/swos/index/html`)

9. Бабаш А. В., Шанкин Г. П. Криптография. — М.: СОЛОН-ПРЕСС, 2007. — 511 с.

10. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. — СПб.: БХВ-Петербург,2005.

11. Rabin M. O. Digitalized signatures and public key functions as intractable as factorization // Technical report MIT/LCS/TR-212.MIT Laboratory for Computer Science. — 1979.

12. Чубариков В. Н. О кратных рациональных тригонометрических суммах и кратных интегралах // Мат. заметки. — 1976. — Т. 20, № 1. — С. 61-68.

13. Архипов Г. И. Избранные труды. — Орел: Изд–во Орловского гос. ун-та, 2013.

14. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Теория кратных тригонометрических сумм. — М.: Наука, 1987. — 368 с.

15. Архипов Г. И., Садовничий В. А., Чубариков В. Н. Лекции по математическому анализу. — М.: Дрофа, 2006. — 640 с.

16. Романов Н. П. Теория чисел и функциональный анализ: сборник трудов / Под общ. ред. В. Н. Чубарикова. — Томск: Изд-во Том. ун-та, 2013. — 478 с.

17. Arkhipov G. I., Karatsuba A. A., Chubarikov V. N. Trigonometric integrals. Izv. Akad. Nauk SSSR. Ser. Mat. — 1979. — 43 (5). — P. 971–1003.

18. Hua L.-K. On the number of solutions of Tarry's problem // Acta Sci. Sinica. — 1953. — 1. — P. 1–76.

ДВЕ ПОСТАНОВКИ ЗАДАЧИ КОДИРОВАНИЯ НЕДООПРЕДЕЛЕННЫХ ДАННЫХ

Л. А. Шоломов (Москва)

Рассматриваются последовательности недоопределенных символов. Каждому такому символу соответствует некоторое множество основных (полностью определенных) символов, одним из которых

он может быть замещен (доопределен). Имеются две естественные постановки задачи кодирования недоопределенных данных.

В первой постановке кодирование должно обеспечить восстановление какого-либо доопределения исходных данных (но не их самих). Она соответствует случаю, когда в равной мере устраивает любое доопределение данных. При второй постановке от кодирования требуется, чтобы оно позволяло полностью восстановить исходные недоопределенные данные. К такой постановке приводит задача их хранения. С первой постановкой будем связывать термин «сжатие», со второй — термин «архивация». Отметим, что для полностью определенных данных эти термины понимаются одинаково.

Результаты, относящиеся к задаче сжатия, были представлены в докладе на X семинаре "Дискретная математика и ее приложения" [1]. Данный доклад в большей степени посвящен задаче архивации.

Введем ряд понятий. Задан алфавит $A_0 = \{a_0, a_1, \ldots, a_{m-1}\}$ *основных символов*. Обозначив $M = \{0, 1, \ldots, m-1\}$, сопоставим каждому непустому $T \subseteq M$ символ a_T. Он называется *недоопределенным* и его *доопределением* считается всякий основной символ a_i, $i \in T$. Символ a_M, доопределимый любым основным символом, называется *неопределенным* и обозначается $*$. Считаем, что выделена система $\mathcal{T}$ некоторых непустых подмножеств T множества M и с ней связан *недоопределенный алфавит* $A = A_{\mathcal{T}} = \{a_T \mid T \in \mathcal{T}\}$.

Приведем некоторые **результаты, относящиеся к задаче сжатия**. Их развернутое изложение имеется в [2–4] (см. также [1]).

Задача сжатия допускает вероятностную и детерминированную постановки. При вероятностной постановке считаем, что имеется источник S, порождающий символы $a_T \in A$ независимо с вероятностями p_T. *Энтропией источника* S назовем величину

$$\mathcal{H}(S) = \min_{Q} \Big\{ - \sum_{T \in \mathcal{T}} p_T \log \sum_{i \in T} q_i \Big\},$$

где $\log x = \log_2 x$, минимум берется по наборам $Q = (q_i,\ i \in M)$, $q_i \geq 0$, $\sum_{i \in M} q_i = 1$. Наряду с $\mathcal{H}(S)$ будем использовать обозначение $\mathcal{H}(P)$, где $P = (p_T,\, T \in \mathcal{T})$.

Свойства энтропии $\mathcal{H}(S)$ во многом обобщают свойства энтропии Шеннона [3], а в случае всюду определенных данных $\mathcal{H}(S)$ совпадает с энтропией Шеннона.

В задаче сжатия недоопределенных данных требуется осуществить кодирования источника, позволяющее по коду порождаемой им последовательности восстановить какое-либо ее доопределение.

Качество кодирования характеризуется *средней длиной кода* $\bar{l}$ на символ последовательности. Теорема кодирования полностью определенных источников обобщается на недоопределенный случай в следующем виде.

Теорема 1 [2]. *При любом способе блокового кодирования недоопределенного источника S выполнено $\bar{l} \geq \mathcal{H}(S)$ и существует блоковое кодирование, для которого $\bar{l} \leq \mathcal{H}(S) + o(\log n/n)$*, где n — длина блока.

При детерминированной постановке задачи сжатия недоопределенных данных рассматривается класс $\mathcal{K}_n(\mathbf{r})$, $\mathbf{r} = (r_T, T \in \mathcal{T})$, всех слов длины n, $n = \sum_{T\in\mathcal{T}} r_T$, в алфавите A, в которых символ $a_T \in A$ встречается r_T раз. Обозначим через $N_n(\mathbf{r})$ минимальную мощность множества слов в алфавите A_0, содержащего доопределение каждого слова из $\mathcal{K}_n(\mathbf{r})$. Величина $h_n(\mathbf{r}) = \log N_n(\mathbf{r})$ называется *комбинаторной энтропией* класса $\mathcal{K}_n(\mathbf{r})$.

Теорема 2 [2]. *Справедливы оценки комбинаторной энтропии*

$$n\mathcal{H}(\mathbf{r}/n) - c\log n \leq h_n(\mathbf{r}) \leq n\mathcal{H}(\mathbf{r}/n) + c\log n,$$

где $c = c(m)$ — некоторая константа.

Эта теорема дает границы минимальной длины кодовых слов при кодировании класса $\mathcal{K}_n(\mathbf{r})$.

Приведем некоторые результаты, не имеющие аналогов в классической теории информации, поскольку связаны с наличием неопределенных символов.

Э. И. Нечипорук установил [5], что слова длины n в алфавите $\{0, 1, *\}$ и двоичные слова, образованные из них удалением символов $*$, представимы кодами одинаковой с точностью до $O(\log n)$ длины. Этот факт в расширенной интерпретации (для других классов слов и требований к кодированию) будем называть эффектом Нечипорука.

Применительно к недоопределенным данным общего вида он имеет следующую формулировку.

Теорема 3 [4]. *Если класс $\mathcal{K}_{n'}(\mathbf{r}')$, $n' = n - r_*$, образован из класса $\mathcal{K}_n(\mathbf{r})$ удалением в его словах символов $*$, то*

$$h_n(\mathbf{r}) = h_{n'}(\mathbf{r}') + O(\log n).$$

Эффект Нечипорука распространяется и на кодирование с заданным критерием верности. Пусть слова в алфавите A недоопределенных символов должны быть представлены словами (той же длины n) в алфавите A_0 при выполненении некоторых условий верности воспроизведения. Будем считать, что эти условия задаются отношением

$v\,\omega\,w$ допустимости воспроизведения слова $w \in A_0^n$ вместо $v \in A^n$. Будем полагать, что отношение ω не зависит от нумерации разрядов слов и обладает тем свойством, что для любых слов v, w и $\hat{w}$ таких, что $\hat{w}$ и w отличаются лишь в разрядах, где v содержит символ $*$, выполнено $v\omega w \Leftrightarrow v\omega\hat{w}$.

Пусть $N_{n,\omega}(\mathbf{r})$ — минимальное число слов в алфавите A_0, содержащих для каждого слова из $\mathcal{K}_n(\mathbf{r})$ ω-допустимое слово. Величину $h_{n,\omega}(\mathbf{r}) = \log N_{n,\omega}(\mathbf{r})$ назовем *комбинаторной ω-энтропией* класса $\mathcal{K}_n(\mathbf{r})$. Применительно к ω-энтропии эффект Нечипорука формулируется в следующем виде.

Теорема 4 [4]. *Если класс $\mathcal{K}_{n'}(\mathbf{r}')$, $n' = n - r_*$, образован из $\mathcal{K}_n(\mathbf{r})$ удалением в его словах символов $*$ и отношение допустимости ω' для $\mathcal{K}_{n'}(\mathbf{r}')$ индуцировано отношением ω для $\mathcal{K}_n(\mathbf{r})$, то*

$$h_{n,\omega}(\mathbf{r}) = h_{n',\omega'}(\mathbf{r}') + O(\log n).$$

Оставшаяся часть доклада посвящена **результатам, относящимся к задаче архивации недоопределенных данных**. Результаты, авторство которых не указано, взяты из [6].

Для архивации будем использовать представления алфавитов A_0 и A в виде двоичной и недоопределенной двоичной матриц с некоторым числом s строк. Для этого каждому $a_i \in A_0$ сопоставим код $\lambda_i = (\lambda_i(1), \ldots, \lambda_i(s)) \in \{0,1\}^s$, а каждому $a_T \in A$ — представление $\lambda_T = (\lambda_T(1), \ldots, \lambda_T(s)) \in \{0,1,*\}^s$. Образуем матрицу Λ со столбцами λ_i, $i \in M$, и матрицу $\hat{\Lambda}$ со столбцами λ_T, $T \in \mathcal{T}$. Будем говорить, что пара $(\Lambda, \hat{\Lambda})$ задает *двоичное представление* алфавита A, если

$$\lambda_i \textit{ доопределяет } \lambda_T \Leftrightarrow i \in T.$$

Таким образом, отношение доопределимости между основными и недоопределенными символами переносится на представляющие их наборы, что позволяет решать задачи, связанные со сжатием и доопределением данных, работая непосредственно с представлениями. В случае, когда $\hat{\Lambda}$ — матрица в двоичном алфавите $\{0,*\}$, представление будем называть *строго двоичным*.

Утверждение 1. *Для любого алфавита A существует двоичное и строго двоичное представление.*

Будем рассматривать побуквенное представление недоопределенных слов, при котором слову $a_{T_1}a_{T_2}\ldots a_{T_N}$ соответствует представление $\lambda_{T_1}\lambda_{T_2}\ldots\lambda_{T_N}$. Его построение и восстановление по нему исходного слова использует матрицу $\tilde{\Lambda}$, число столбцов которой может

достигать $2^m - 1$. Это делает процедуру неэффективной (неполиномиальной). Покажем, как эту задачу можно эффективно решать пользуясь лишь матрицей Λ, имеющей m столбцов.

Матрица Λ называется *$\mathcal{T}$-допустимой* (*строго $\mathcal{T}$-допустимой*), если существует двоичное (строго двоичное) представление $(\Lambda, \hat{\Lambda})$ алфавита $A_{\mathcal{T}}$, использующее матрицу кодирования Λ. Дадим описание $\mathcal{T}$-допустимых и строго $\mathcal{T}$-допустимых матриц.

Под *дизъюнкцией $\lambda \vee \lambda'$ двоичных слов* $\lambda = (\lambda(1) \dots \lambda(s))$ и $\lambda' = (\lambda'(1) \dots \lambda'(s))$ в алфавите $\{0, 1\}$ понимается слово с разрядами $\lambda(i) \vee \lambda'(i)$, $i = 1, \dots, s$. Считается, что слово λ' *покрывает* λ, если $\lambda \vee \lambda' = \lambda'$, и что некоторое множество слов покрывает λ, если λ покрывается их дизъюнкцией.

Скажем, что множество столбцов T матрицы Λ (1) *покрывает*, (2) *инверсно покрывает*, (3) *дважды покрывает* столбец λ_j, если (1) дизъюнкция столбцов из T покрывает λ_j, (2) дизъюнкция инверсий столбцов из T покрывает инверсию столбца λ_j, (3) множество столбцов T покрывает и инверсно покрывает λ_j.

Матрица Λ называется *свободной от $\mathcal{T}$-покрытий* (*двойных $\mathcal{T}$-покрытий*), если для любого $T \in \mathcal{T}$ множество столбцов T не покрывает (не покрывает дважды) ни одного столбца вне T.

Теорема 5. *Матрица Λ $\mathcal{T}$-допустима* (*строго $\mathcal{T}$-допустима*) *тогда и только тогда, когда она свободна от двойных $\mathcal{T}$-покрытий* (*от $\mathcal{T}$-покрытий*).

Следующая теорема дает способ построения матрицы $\hat{\Lambda}$ соответствующей допустимой матрице кодирования Λ.

Теорема 6. 1) *Если матрица кодирования Λ $\mathcal{T}$-допустима, то для двоичного представления $(\Lambda, \hat{\Lambda})$ алфавита $A = A_{\mathcal{T}}$ может быть взята матрица $\hat{\Lambda}$ со столбцами $\lambda_T = \nabla_{i \in T} \lambda_i$, где операция $v \nabla w$ над троичными словами $v, w \in \{0, 1, *\}^s$ дает троичное слово, разряд $v(i) \nabla w(i)$ которого равен 0 при $v(i) = w(i) = 0$, равен 1 при $v(i) = w(i) = 1$ и равен $*$ в остальных случаях.*

2) *Если матрица кодирования Λ строго $\mathcal{T}$-допустима, то для строго двоичного представления $(\Lambda, \hat{\Lambda})$ алфавита $A = A_{\mathcal{T}}$ может быть взята матрица $\hat{\Lambda}$ со столбцами $\lambda_T = \vee^*_{i \in T} \lambda_i$, где операция $v \vee^* w$ над троичными словами $v, w \in \{0, 1, *\}^s$ дает троичное слово, разряд $v(i) \vee^* w(i)$ которого равен 0 при $v(i) = w(i) = 0$ и равен $*$ в остальных случаях.*

В соответствии с этой теоремой, (строгое) представление λ_T сим-

вола a_T находится по матрице Λ с полиномиальной сложностью. И обратно, по (строгому) представлению λ_T и матрице Λ с полиномиальной сложностью определяется символ a_T — множество T образовано всеми i, при которых столбец λ_i доопределяет λ_T.

Приведем еще одну полезную характеризацию допустимых матриц. Скажем, что система $\mathcal{Z}$ подмножеств множества M образует *конъюнктивный базис* системы $\mathcal{T}$, если каждое множество $T \in \mathcal{T}$ может быть получено как пересечение некоторых множеств из $\mathcal{Z}$, и образует *обобщенный конъюнктивный базис*, если каждое $T \in \mathcal{T}$ может быть получено как пересечение каких-либо множеств из $\mathcal{Z}$ либо их дополнений (до M).

Посредством $\lambda(v)$, $v = 1, \ldots, s$, будем обозначать строки матрицы Λ. Строке $\lambda(v)$ сопоставим множество $Z_v \subseteq M$, $Z_v = \{i \mid \lambda_i(v) = 1\}$, характеристическим набором которого строка является. Положим $\mathcal{Z}(\Lambda) = \{Z_1, \ldots, Z_s\}$, $\mathcal{Z}'(\Lambda) = \{\bar{Z}_1, \ldots, \bar{Z}_s\}$, где $\bar{Z}_v = M \setminus Z_v$.

Теорема 7. *Матрица кодирования* Λ

1) $\mathcal{T}$*-допустима тогда и только тогда, когда система множеств* $\mathcal{Z}(\Lambda)$ *образует обобщенный конъюнктивный базис системы* $\mathcal{T}$,

2) строго $\mathcal{T}$*-допустима тогда и только тогда, когда система множеств* $\mathcal{Z}'(\Lambda)$ *образует конъюнктивный базис системы* $\mathcal{T}$.

Двоичное представление алфавита $A_{\mathcal{T}}$ допускает интерпретацию в терминах вложения системы $\mathcal{T}$ подмножеств множества M в булев куб $\{0,1\}^s$ (подходящей размерности s). При вложении каждому $i \in M$ сопоставляется некоторая точка λ_i куба, каждому $T \in \mathcal{T}$ — некоторый подкуб λ_T, и этот подкуб содержит те и только те точки λ_i, которые соответствуют значениям $i \in T$. Параметр s будем называть *размерностью представления* (вложения). Наименьшее s, при котором для алфавита A имеется двоичное представление размерности s, обозначим $s(A)$ и назовем *размерностью алфавита* A. Аналогично вводится размерность $s_0(A)$ при строго двоичном представлении.

Задача о размерности алфавита состоит в том, чтобы по алфавиту A и числу s узнать, существует ли для A двоичное представление размерности s. Аналогично формулируется задача о размерности алфавита при строго двоичном представлении.

Теорема 8. *Задачи о размерности алфавита и о размерности при строго двоичном представлении NP-полны.*

В связи с трудностью нахождения значений $s(A)$ и $s_0(A)$ представляют интерес оценки этих величин. Обозначим через $s(m,n)$ и $s_0(m,n)$ максимальные значения $s(A)$ и $s_0(A)$ по всем алфавитам A

с $|A_0| = m$, $|A| = n$, где $|\cdot|$ означает мощность множества.

Утверждение 2. *Имеют место равенства*

$$s(m,n) = s_0(m,n) = \min\{m,n\}.$$

В качестве основного будем рассматривать случай $m \le n$. При этом условии утверждение 2 приобретает вид $s(m,n) = s_0(m,n) = m$.

В случае, когда множество $\mathcal{T}$ образовано всеми t-элементными подмножествами множества M, матрицы, свободные от $\mathcal{T}$-покрытий (двойных $\mathcal{T}$-покрытий), будем называть свободными от t-покрытий [7] (двойных t-покрытий). Матрицы, свободные от t-покрытий, называются также *t-дизъюнктивными*. Они возникли в работе [8] как средство описания введенных в ней дизъюнктивных (superimposed) кодов. Последние широко применяются в задачах прикладной математики и информатики — см., например, [8–12] и цитированные там источники.

Обозначим через $s_0(m;t)$ (через $s(m;t)$) минимальное число строк матрицы с m столбцами, свободной от t-покрытий (двойных t-покрытий). В работе [13] установлено, что при $t \to \infty$ (и, как следствие, $m \to \infty$) имеет место асимптотическое равенство $s_0(m;t) \sim s(m;t)$, поэтому дальше будем вести речь об оценках величины $s_0(m;t)$.

Тривиальные мощностные нижние оценки величины $s_0(m;t)$ имеют порядок $t \log m$. Впервые немощностная (и к данному моменту наилучшая) нижняя оценка для $s_0(m;t)$ установлена Дьячковым и Рыковым [9].

Теорема 9 [9]. *При $t \to \infty$ справедлива оценка*

$$s_0(m;t) \gtrsim \frac{t^2}{2\log t} \log m.$$

Этот факт доказывается достаточно сложно индукцией по t. Позднее в работе [14] было найдено чисто комбинаторное доказательство в 4 раза более слабой оценки. Затем в заметке [15] было представлено очень простое комбинаторное доказательство оценки, которая хуже оценки теоремы 8 в 2 раза. Она вытекает из установленного в [15] соотношения

$$m \le t + \binom{s}{\left\lceil \frac{2(s-t)}{t(t+1)} \right\rceil},$$

связывающего параметры t-дизъюнктивной матрицы — число m столбцов и число s строк.

Приведем верхнюю оценку величины $s_0(m;t)$, полученную многими авторами различными вариантами метода случайного кодирования [7–9, 11, 16] или жадного алгоритма (напр., в [17, 18]).

Теорема 10. *При $t \to \infty$ справедлива оценка*

$$s_0(m;t) \lesssim \frac{et^2}{\log e} \log m.$$

Верхняя и нижняя оценки теорем 10 и 9 различаются по порядку в $\log t$ раз. Этот разрыв по порядку ликвидирован в [19], где также использован метод случайного кодирования.

Теорема 11 [19]. *При $t \to \infty$ имеет место оценка*

$$s_0(m;t) \lesssim \frac{e^2t^2}{4 \log t} \log m.$$

Оценки теорем 9 и 11 различаются асимптотически в $2e^{-2} = 0.271\ldots$ раз.

Метод случайного кодирования не дает конструкции t-дизъюнктивной матрицы, а трудоемкость жадного алгоритма экспоненциальна. Возникает задача нахождения эффективных и конструктивных алгоритмов, обеспечивающих «достаточно хорошие» верхние оценки величины $s_0(m;t)$. Детерминированный алгоритм считается эффективным, если его трудоемкость ограничена полиномом от размера исходных данных, и считается конструктивным, если из него извлекается явное описание объекта.

В работе [8] представлены некоторые конструкции дизъюнктивных кодов. Один из предложенных там подходов основан на использовании q-ичных кодов с большим кодовым расстоянием. Реализация этого подхода с применением кодов Рида—Соломона позволила для дизъюнктивных матриц получить достаточно хорошую эффективную оценку величины m при заданных t и s [8]. Применительно к задаче двоичного представления недоопределенных данных из нее вытекает следующий результат.

Утверждение 3. *Существует эффективный и конструктивный метод, обеспечивающий при $t \to \infty$ оценку*

$$s_0(m;t) \lesssim \left(\frac{2t \log m}{\log(t \log m)} \right)^2.$$

В работе [11] приведена эффективная конструкция, позволившая при малых t улучшить эту оценку. Она использует некоторое семейство алгебро-геометрических кодов Гоппы. Из полученной в [11] оценки m в функции от t и s вытекает следующий результат для двоичных представлений.

Утверждение 4. *Существует эффективный и конструктивный метод, обеспечивающий оценку*

$$s_0(m;t) = O\left(\frac{t^3 \log m}{\log t}\right).$$

Разрыв между детерминированными эффективными оценками и оценкой теоремы 10, полученной методом случайного кодирования, устранен в работе [12]. Из нее вытекает следующий факт.

Утверждение 5. *Существует эффективный метод, обеспечивающий оценку*

$$s_0(m;t) = O\left(t^2 \log m\right).$$

Однако, этот результат нельзя считать вполне удовлетворительным, поскольку метод работы [12] эффективен (полиномиален), но не конструктивен — использует дерандомизацию метода случайного кодирования.

Рассмотрим теперь более общий случай системы множеств $\mathcal{T}$. Недоопределенные данные, с которыми имеют дело в приложениях, обычно помимо неопределенного символа $*$ используют лишь символы, имеющие небольшое число доопределений.

Обозначим через $s(m,n;t)$ (через $s_0(m,n;t)$) максимумальную из размерностей $s(A)$ (соответственно, $s_0(A)$) алфавитов A, для которых $|A_0| = m$, $|A| = n$ и каждый символ $a_T \in A$ имеет не более t доопределений либо является неопределенным.

Приведем верхние и нижние оценки этих величин.

Теорема 12. *Справедливы оценки*

$$s_0(m,n;t) \le s(m,n;t) \le e(t+1)\ln(mn) + 1.$$

Теорема 13. *При выполнении условия*

$$t = o\left(\frac{\log n}{\log\log n}\right)$$

справедливы оценки

$$\begin{aligned} s_0(m,n;t) &\gtrsim \frac{(t+1)\log n}{2(2\log t + c)}, \\ s(m,n;t) &\gtrsim \frac{(t-1)\log n}{2(2\log(t-1)+c)}, \end{aligned}$$

где $c = \log\dfrac{3e}{4} < 1.027$.

Верхняя оценка получена методом случайного кодирования с использованием теоремы 7, сводящей оценку числа строк $\mathcal{T}$-допустимой матрицы к оценке мощности обобщенного конъюнктивного базиса системы $\mathcal{T}$. При доказательстве нижней оценки основную роль играет неравенство Фареди, приведенное в тексте после теоремы 9.

При растущем t разрыв между верхними и нижними оценками теорем 12 и 13 в основном случае $m \le n$ имеет порядок $\log t$.

Список литературы

1. Шоломов Л. А. Элементы теории недоопределенной информации // Материалы X Международного семинара "Дискретная математика и ее приложения" (1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 52–58.

2. Шоломов Л. А. Сжатие частично определенной информации // Нелинейная динамика и управление. — Вып. 4. — М.: Физматлит, 2004. — С. 385–399.

3. Шоломов Л. А. Информационные свойства недоопределенных данных // Дискретная математика и ее приложения: Сборн. лекций молодежных научных школ. — Вып. IV. — М.: Изд-во ИПМ РАН, 2007. — С. 26–50.

4. Шоломов Л. А. О кодировании недоопределенных последовательностей с заданной точностью воспроизведения // Доклады Академии наук. — 2009. — Т. 429, № 5. — С. 605–609.

5. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. — 1965. — Т. 163, № 1. — С. 40–42.

6. Шоломов Л. А. Двоичные представления недоопределенных данных и дизъюнктивные коды // Прикладная дискретная математика. — 2013. — № 1 (19). — С. 17–33.

7. Erdos P., Frankl P., Furedi Z. Families of finite sets in which no set is covered by the union of r others // Israel Journal of Mathematics. — 1985. — Vol. 51, № 1–2. — P. 79–89.

8. Kautz W. H., Singleton R. C. Nonrandom binary superimposed codes // IEEE Transactions on Information Theory. — 1964. — Vol. 10, № 4. — P. 363–377.

9. Дьячков А. Г., Рыков В. В. Границы длины дизъюнктивных кодов // Проблемы передачи информации. — 1982. — Т. 18, вып. 3. — С. 7–13.

10. D'yachkov A. G. Lectures on designing screening experiments. Lecture Note Series 10. — Korea: Combinatorial and computation mathematics center, Pohan University of science and technology, 2003.

11. Kumar R., Rajagopalan S., Sahai A. Coding construction for blacklisting problems without computational assumptions // CRYPTO-99. Lecture Notes in Computer Science, vol. 1666. — Berlin, Heidelberg: Springer-Verlag, 1999. — P. 609–623.

12. Porat E., Rotshchild A. Explicit non-adaptive combinatorial group testing schemes // Automata, Languages and Programming. Lecture Notes in Computer Science, vol. 5125. — Springer, 2008. — P. 748–759.

13. D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Symmetric disjunctive list-decoding codes // Proceedings of the IEEE International symposium on information theory (Hong Kong, 14–19 June, 2015). — IEEE, 2015. — P. 2236–2240.

14. Ruszinko M. On the upper bound of the size of the r-cover-free families // Journal of Combinatorial Theory. Ser. A. — 1994. — Vol. 66. — P. 302–310.

15. Furedi Z. On r-cover-free families // Journal of Combinatorial Theory. Ser. ,A. — 1996. — Vol. 73. — P. 172–173.

16. Cheng V., Du D.-Z., Lin G. On the upper bounds of the minimum number of rows of disjunct matrices // Optimization Letters. — 2009. – Vol. 3, iss 2. — P. 297–302.

17. Hwang F. K., Sos V. T. Non-adaptive hypergeometric group testing // Studia Scientiarum Mathecarum Hungarica. — 1987. — Vol. 22. — P. 257–263.

18. Шоломов Л. А. Двоичное представление недоопределенных данных // Доклады Академии наук. — 2013. — Т. 448, № 3. — С. 275–278.

19. Дьячков А. Г., Воробьев И. В., Полянский В. А., Щукин В. Ю. Границы скорости дизъюнктивных кодов // Проблемы передачи информации. — 2014. — Т. 50, вып. 1. — С. 31–63.

О СИНТЕЗЕ СХЕМ И ФОРМУЛ ИЗ ЭЛЕМЕНТОВ С ПРЯМЫМИ И ИТЕРАТИВНЫМИ ВХОДАМИ

В. А. Коноводов, С. А. Ложкин (Москва)

В работе [1] был определен класс функционально-проводящих схем, который обобщает многие известные классы дискретных управляющих систем [2–4], реализующих функции алгебры логики (ФАЛ). Там же, а так же в [5], были введены некоторые специальные подклассы указанного класса схем, связанные, в частности, с разделением управляющих входов каждого базисного функционального-проводящего элемента (ФПЭ) на т. н. прямые и итеративные входы.

Рассмотрим сначала классы контактных схем (КС) и итеративно-контактных схем (ИКС) над заданным базисом ФПЭ, частными случаями которых являются известные классы схем «проводящего» типа — классы «обычных» КС и ИКС [4].

Рассматриваемые схемы строятся из ФПЭ базиса $\mathcal{A} = \{\mathcal{E}_1, \ldots, \mathcal{E}_b\}$, каждый элемент $\mathcal{E}_i$, $i = 1, \ldots, b$, которого представляет собой тройку $\langle \varphi_i, L_i, \tau_i \rangle$, где φ_i — ФАЛ, существенно зависящая от булевых переменных (БП) $x_1, \ldots, x_{k_i}$, L_i — положительное действительное число, а τ_i — булевская константа. Предполагается, что число L_i характеризует сложность («вес») ФПЭ $\mathcal{E}_i$, который состоит из ориентированного в случае $\tau_i = 0$ и неориентированного в случае $\tau_i = 1$ контакта K_i, проводящего на наборе α значений БП $x_1, \ldots, x_{k_i}$ тогда и только тогда, когда $\varphi_i(\alpha) = 1$, причем указанная проводимость в случае $\tau_i = 0$ имеет место только в направлении ориентации K_i.

Таким образом, с формальной точки зрения ФПЭ $\mathcal{E}_i$ представляет собой контакт (ребро) K_i с пометкой φ_i. При этом из содержательных соображений можно считать, что ФПЭ $\mathcal{E}_i$ состоит из контакта K_i и функционального элемента E_i, реализующего ФАЛ φ_i, выход которого «управляет» проводимостью K_i.

Следуя [1, 4], определим (одновходовую) КС $\Sigma = \Sigma(x_1, \ldots, x_n; z_1, \ldots, z_m)$ над базисом $\mathcal{A}$ как частично ориентированный граф с единственным (проводящим) входом, помеченным символом 1, и m (проводящими) выходами, помеченными выходными БП $z_1, \ldots, z_m$, каждое ориентированное (соответственно, неориентированное) ребро которого помечено одной из базисных ФАЛ φ_i, где $\tau_i = 0$ (соответственно, $\tau_i = 1$), зависящей от k_i переменных из множества входных (управляющих) БП $X(n) = \{x_1, \ldots, x_n\}$. Для любой упорядоченной пары (u, v) вершин данной КС стандартным образом вводится ФАЛ проводимости от u к v, зависящая от БП $X(n)$. Будем, как обычно, считать, что в каждой вершине рассматриваемой КС Σ реализуется

ФАЛ проводимости от входа 1 к этой вершине, и что сама КС Σ реализует систему ФАЛ $F_\Sigma = (f_1, \ldots, f_m)$, где f_j — ФАЛ, реализуемая в вершине Σ с пометкой z_j, $j = 1, \ldots, m$.

Пусть $\mathcal{U}_\mathcal{A}^K$ — класс КС над базисом $\mathcal{A}$, входные и выходные БП которых берутся из счетных упорядоченных непересекающихся алфавитов $\mathcal{X} = \{x_1, x_2, \ldots, x_n, \ldots\}$ и $\mathcal{Z} = \{z_1, z_2, \ldots, z_m, \ldots\}$ соответственно. Предполагается, что базис $\mathcal{A}$ является полным, то есть любая ФАЛ от БП из $\mathcal{X}$ может быть реализована схемой из $\mathcal{U}_\mathcal{A}^K$. Заметим, что любой базис, содержащий «обычные» неориентированные замыкающий и размыкающий контакты, т. е. контакты с базисной ФАЛ x_i и $\bar{x}_i$ соответственно, является полным. Базис $\mathcal{A}_0$, состоящий из замыкающего и размыкающего контактов веса 1, будем считать *стандартным*.

Под сложностью схемы $L(\Sigma)$ КС Σ, $\Sigma \in \mathcal{U}_\mathcal{A}^K$, понимается, как обычно, сумма весов всех её ФПЭ, а под сложностью $L_\mathcal{A}^K(F)$ системы ФАЛ $F = (f_1, \ldots, f_m)$ от БП из $\mathcal{X}$ — минимальная из сложностей схем класса $\mathcal{U}_\mathcal{A}^K$, её реализующих. Для указанного функционала сложности обычным образом вводится соответствующая функция Шеннона

$$L_\mathcal{A}^K(n) = \max_{f \in P_2(n)} L_\mathcal{A}^K(f), \tag{1}$$

где $P_2(n)$ — множество всех ФАЛ от БП $X(n)$, $n = 1, 2, \ldots$

Положим

$$\pi_\mathcal{A} = \min_{1 \leqslant i \leqslant b} L_i, \quad \theta_\mathcal{A} = \min_{L_i = \pi_\mathcal{A}} (3 - k_i), \tag{2}$$

и будем считать базис $\mathcal{A}$ *ориентированным*, если оба минимума в (2) достигаются на «ориентированном» ФПЭ $\mathcal{E}_j$, для которого $\tau_j = 0$. Заметим, что для произвольного базиса $\mathcal{A}$ из результатов [1] вытекают неравенства[3]

$$\pi_\mathcal{A} \frac{2^n}{n} \left(1 + \frac{\theta_\mathcal{A} \log n - O(1)}{n}\right) \leqslant L_\mathcal{A}^K(n) \leqslant \pi_\mathcal{A} \frac{2^n}{n} \left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right), \tag{3}$$

а в случае ориентированного базиса $\mathcal{A}$ — соотношение

$$L_\mathcal{A}^K(n) = \pi_\mathcal{A} \frac{2^n}{n} \left(1 + \frac{\theta_\mathcal{A} \log n \pm O(1)}{n}\right), \tag{4}$$

[3] в настоящей работе все логарифмы рассматриваются по основанию 2

которое описывает поведение функции Шеннона $L^K_{\mathcal{A}}(n)$ на уровне асимптотических оценок высокой степени точности (АОВСТ).

Исходя из содержательных соображений в классе $\mathcal{U}^K_{\mathcal{A}}$ так же, как и в классе «обычных» КС $\mathcal{U}^K_{\mathcal{A}_0}$, можно выделять некоторые (полные) подклассы и изучать поведение связанных с ними функций Шеннона, определяемых аналогично (1).

Так, в работе [6] для базиса $\overrightarrow{\mathcal{A}_0}$, состоящего из ориентированных замыкающего и размыкающего контактов веса 1, и произвольного фиксированного натурального λ, $\lambda \geqslant 2$, рассматривался класс $\mathcal{U}^K_{\overrightarrow{\mathcal{A}_0},\lambda}$ — класс КС над $\overrightarrow{\mathcal{A}_0}$ с полустепенью исхода вершин, не превосходящей λ. При этом поведение соответствующей функции Шеннона $L^K_{\overrightarrow{\mathcal{A}_0},\lambda}(n)$ было установлено на уровне близких к АОВСТ оценок вида

$$L^K_{\overrightarrow{\mathcal{A}_0},\lambda}(n) = \frac{\lambda}{\lambda-1}\frac{2^n}{n}\left(1 + \frac{-\frac{1}{\lambda-1}\log n \pm O(\log\log n)}{n}\right).$$

Оценки аналогичного уровня точности были получены в [7] для класса двоичных решающих диаграмм (BDD), являющегося подклассом класса $\mathcal{U}^K_{\overrightarrow{\mathcal{A}_0}}$.

Определим далее класс $\mathcal{U}^{\text{ИКС}}_{\mathcal{A}}$ — класс *итеративно-контактных схем над базисом* $\mathcal{A}$, который обобщает класс $\mathcal{U}^K_{\mathcal{A}}$ аналогично тому как класс «обычных» ИКС [4] обобщает класс обычных КС $\mathcal{U}^K_{\mathcal{A}_0}$.

Для этого рассмотрим счетный упорядоченный алфавит итеративных БП $\mathcal{Y} = \{y_1, y_2, \ldots, y_p, \ldots\}$, где $\mathcal{Y} \cap \mathcal{X} = \mathcal{Y} \cap \mathcal{Z} = \varnothing$, и индукцией по t, $t = 0, 1, \ldots$, введём класс $\mathcal{U}^{\text{ИКС}}_{\mathcal{A},t}$ — класс ИКС *итеративного ранга* t над базисом $\mathcal{A}$. Базис указанной индукции составляет класс $\mathcal{U}^{\text{ИКС}}_{\mathcal{A},0}$ — класс ИКС итеративного ранга 0, который совпадает с классом $\mathcal{U}^K_{\mathcal{A}}$.

Индуктивный переход, позволяющий от ИКС $\Sigma = \Sigma(x_1, \ldots, x_n; z_1, \ldots, z_m)$ из класса $\mathcal{U}^{\text{ИКС}}_{\mathcal{A},t}$, реализующей систему ФАЛ $(f_1, \ldots, f_m)$ от БП $x = (x_1, \ldots, x_n)$, переходить к реализующей систему ФАЛ $(f'_1, \ldots, f'_{j-1}, f'_{j+1}, \ldots, f'_m)$ от БП $x' = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ ИКС $\Sigma' = \Sigma'(x', z_1, \ldots, z_{j-1}, z_{j+1}, \ldots, z_m)$ из класса $\mathcal{U}^{\text{ИКС}}_{\mathcal{A},t+1}$, связан с применением операции присоединения выхода z_j ИКС Σ к её входу x_i. Эта операция применима, если ФАЛ f_j не зависит существенно от x_i и состоит в замене пометки z_j выходной вершины v ИКС Σ, а также

всех пометок БП x_i на контактах Σ пометками БП y_{t+1}. При этом предполагается, что ФАЛ $f'_s(x')$, где $s \neq j$, получается из ФАЛ $f_s(x)$ подстановкой ФАЛ $f_j(x')$ вместо БП x_j.

Будем считать, что для описанных выше схем ИКС Σ является *базовой ИКС ранга* t для ИКС Σ' и что переходя от ИКС Σ к её базовой ИКС ранга $(t-1)$ и т. д. мы придем к базовой для ИКС Σ' КС $\hat{\Sigma}$. Заметим, что сложности всех построенных ИКС одинаковы и равны $L(\hat{\Sigma})$. Определим, наконец, класс $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$ как объединение классов $\mathcal{U}_{\mathcal{A},i}^{\text{ИКС}}$ по всем i, $i = 0, 1, \ldots$.

Рассмотрим теперь подклассы класса $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$, связанные с теми ограничениями, которые накладывает на применение операции присоединения выходов ИКС к её входам наличие у ФПЭ базиса $\mathcal{A}$ прямых и итеративных входов. Будем считать, что каждому ФПЭ $\mathcal{E}_i$, $i = 1, \ldots, b$, базиса $\mathcal{A}$ сопоставлено число k'_i, $0 \leqslant k'_i \leqslant k_i$, и что первые k'_i входов являются *прямыми*, а остальные — *итеративными* входами данного ФПЭ. Будем говорить, что ИКС Σ является *итеративно-правильной*, если прямые входы всех её ФПЭ являются входами Σ, то есть, если при построении ИКС Σ в операциях присоединения выходов ИКС к их входам участвовали только итеративные входы ФПЭ. При этом множество $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$ будем трактовать как множество всех итеративно-правильных ИКС над базисом $\mathcal{A}$. Заметим, что $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}} = \mathcal{U}_{\mathcal{A}}^{\text{КС}}$, если $k'_i = k_i$ при всех i, $i = 1, \ldots, b$, т. е. если у ФПЭ базиса $\mathcal{A}$ нет итеративных входов.

Для базиса $\mathcal{A}$, в котором есть ФПЭ с итеративными входами, вводятся параметры

$$\pi_i = \frac{L_i}{k_i - k'_i + 1}, \quad \theta_i = \frac{2k_i - 3k'_i + 3}{k_i - k'_i + 1},$$

где $i = 1, \ldots, b$, а затем определяются величины (ср. с (2))

$$\pi_{\mathcal{A}} = \min_{1 \leqslant i \leqslant b} \pi_i, \quad \theta_{\mathcal{A}} = \min_{\pi_i = \pi_{\mathcal{A}}} \theta_i. \tag{5}$$

Для полного класса $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$ и произвольной системы ФАЛ $F = (f_1, \ldots, f_m)$ обычным образом определяется сложность $L_{\mathcal{A}}^{\text{ИКС}}(F)$ — сложность реализации системы F в классе $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$, а затем аналогично (1) вводится соответствующая функция Шеннона $L_{\mathcal{A}}^{\text{ИКС}}(n)$.

В [1] приведены результаты, согласно которым функция Шеннона $L_{\mathcal{A}}^{\text{ИКС}}(n)$ удовлетворяет оценкам (3) для произвольного (полного)

базиса $\mathcal{A}$ и оценкам (4) если оба минимума в (5) достигаются на ФПЭ $\mathcal{E}_j$ таком, что либо сама ФАЛ $\tau_j\varphi_j$, либо ФАЛ, получающаяся из неё заменой одной из итеративных БП ФАЛ φ_j константой, тождественно равна 0. В работе [5] для одного специального базиса $\mathcal{A}$ поведение функции Шеннона, характеризующей сложность реализации схемами из $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$ класса таких ФАЛ, столбцы значений которых принадлежат экспоненциальному языку, порожденному заданной грамматикой с конечным числом состояний, установлено с порядком относительной погрешности таким же, как у АОВСТ вида (4).

Рассмотрим теперь более детально результаты последних лет, связанные с изучением сложности ФАЛ и поведения соответствующих функций Шеннона для классов формул и схем, построенных из функциональных элементов с прямыми и итеративными входами.

Заметим, что класс $\mathcal{U}_A^C$ — класс схем из функциональных элементов (СФЭ) над базисом $A = \{E_1, \ldots, E_b\}$, где $E_i = \langle \varphi_i(x_1, \ldots, x_{k_i}), L_i \rangle$ для всех i, $i = 1, \ldots, b$, — можно считать подклассом класса $\mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$, где $\mathcal{A} = \{\mathcal{E}_1, \ldots, \mathcal{E}_b\}$ и $\mathcal{E}_j = \langle \varphi_i, L_i, 0 \rangle$ для всех j, $j = 1, \ldots, b$. Действительно, указанный подкласс состоит из тех ИКС Σ, $\Sigma \in \mathcal{U}_{\mathcal{A}}^{\text{ИКС}}$, в которых начальная вершина контакта любого ФПЭ совпадает с входом 1, а также отсутствуют циклы по операции присоединения выходов схемы к её итеративным входам.

Для произвольного множества БП $W \subseteq \mathcal{X} \cup \mathcal{Y}$ будем обозначать через $P_2(W)$ множество всех ФАЛ, зависящих от БП из W. ФАЛ, не имеющие общих существенных [8] БП, будем называть *независимыми*.

На множестве $P_2(\mathcal{X} \cup \mathcal{Y})$, согласно [9], введём следующие операции суперпозиции:

1) переименование (с отождествлением) прямых БП, т. е. БП из $\mathcal{X}$;

2) подстановка констант 0, 1 вместо БП;

3) переименование (с отождествлением) итеративных БП, т. е. БП из $\mathcal{Y}$;

4) подстановка одной из двух независимых ФАЛ вместо итеративной БП другой ФАЛ;

5) замена итеративных БП прямыми.

Пусть $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$ — некоторое конечное множество базисных ФАЛ. Будем рассматривать одновыходные СФЭ из функциональных элементов [4] над базисом A с ограничениями на соединения

элементов между собой, соответствующими введённым операциям суперпозиции. Вход базисного функционального элемента будем называть *константным*, если вместо него в этот элемент подставлена константа 0 или 1. Правила соединения элементов в СФЭ ограничиваются следующим образом:

1) прямые входы любого элемента либо присоединяются к входам СФЭ, либо являются константными входами;

2) итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам СФЭ, либо являются константными входами;

3) неконстантным входам СФЭ сопоставлены некоторые БП из множества $\mathcal{X}$.

Под формулами будем понимать те одновыходные СФЭ, которые не содержат ветвлений выходов элементов. С точки зрения рекурсивного определения формулы как символьной записи [8] указанные выше операции дают возможность проводить суперпозицию только по итеративным БП базисных ФАЛ.

Систему ФАЛ A, $A \subseteq \mathcal{X} \cup \mathcal{Y}$, будем называть *полной*, если для любой ФАЛ f, $f \in P_2(\mathcal{X})$, существует формула, построенная в соответствии с введёнными выше ограничениями, реализующая ФАЛ f.

Пусть A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$. Множество тех ФАЛ, которые можно получить из функций системы A в результате применения указанных выше операций суперпозиции, обозначим $[A]$. Множество ФАЛ Q, такое, что $Q \supseteq \{0, 1, x_1\}$, и $[Q] = Q$, называется *замкнутым классом*.

Множество $\delta(A) = [A] \cap P_2(\mathcal{Y})$ называется *итеративным замыканием* [9, 10] базиса A, и определяет все те ФАЛ от итеративных БП, которые можно получить из базисных ФАЛ рассматриваемыми операциями суперпозиции. Заметим, что $\delta(A)$ является «обычным» замкнутым классом [8] в $P_2(\mathcal{Y})$, содержащим все константы, и поэтому совпадает с одним из классов системы

$$\Delta = \{B, I, O, D, K, L, M, P_2(\mathcal{Y})\},$$

где $B = \{0, 1\}$, $I = \mathcal{Y} \cup B$, $O = I \cup \{\bar{y} : y \in \mathcal{Y}\}$, класс D (класс K) содержит константы и дизъюнкции (соответственно, конъюнкции) БП $\mathcal{Y}$, а классы L и M состоят из линейных и монотонных ФАЛ от БП $\mathcal{Y}$ соответственно. Таким образом, введение оператора δ позволяет классифицировать все системы ФАЛ от прямых и итеративных БП по их итеративным замыканиям. Эта классификация имеет прямое

отношение к полноте базисов и исследованию сложности формул в них.

Для каждого $\tilde{\delta}$, $\tilde{\delta} \in \Delta$, через $Z(\tilde{\delta})$ обозначим множество всех замкнутых классов Q, для которых $\delta(Q) = \tilde{\delta}$. Максимальным по включению классом системы $Z(\tilde{\delta})$ является класс $R(\tilde{\delta})$ тех ФАЛ f, $f \in P_2(\mathcal{X} \cup \mathcal{Y})$, для которых все ФАЛ из $P_2(\mathcal{Y})$, получаемые при подстановке констант вместо БП в f, лежат в $\tilde{\delta}$.

Замкнутый класс Q называется *предполным классом системы* $Z(\tilde{\delta})$, $\tilde{\delta} \in \Delta \setminus \{B\}$, если $\delta(Q) = \tilde{\delta}$, и $R(\tilde{\delta}) \subset Q$, но $R(\tilde{\delta}) = [Q \cup \{\varphi\}]$ для любой ФАЛ $\varphi \in R(\tilde{\delta}) \setminus Q$. Для каждого $\tilde{\delta} \in \Delta$ существует конечное число предполных классов $Z(\tilde{\delta})$, все они построены в [9]. Там же описаны структурные и мощностные особенности замкнутых классов в $P_2(\mathcal{X} \cup \mathcal{Y})$ и получен следующий критерий полноты конечных множеств ФАЛ относительно $P_2(\mathcal{X})$.

Теорема 1 [9]. *Конечное множество ФАЛ A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$, является полным тогда и только тогда, когда $\delta(A) \neq B$ и либо $\delta(A) = P_2(\mathcal{Y})$, либо A не содержится целиком ни в одном из предполных классов системы $Z(\delta(A))$.*

Далее будут рассматриваться только полные системы ФАЛ A.

Будем считать, что подстановка константы вместо входа любого элемента не меняет его сложности. *Функцией Шеннона* $L_A^C(n)$ для сложности СФЭ из класса $\mathcal{U}_A^C$, как обычно, будем называть максимальное значение $L_A^C(f)$ среди всех ФАЛ f, $f \in P_2(n)$, где $L_A^C(f)$ — минимальная сложность СФЭ из рассматриваемого класса, реализующей ФАЛ f от прямых БП. Аналогично можно определить функцию Шеннона $L_A^\Phi(n)$ для сложности реализации ФАЛ от прямых БП в классе формул над базисом A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$.

Приведенным весом элемента E_i, $i = 1, \ldots, b$, такого, что $k_i > 1$, будем называть величину

$$\rho_i = \frac{L_i}{k_i - 1}.$$

Назовем *макроблоком* в базисе A СФЭ в этом базисе, состоящую из одного элемента E_j, такого, что $k_j'' > 1$, и m, $0 \leqslant m \leqslant k_j'' - 1$, элементов $E_{i_1}, \ldots, E_{i_m}$, не имеющих итеративных входов, выходы которых подаются на итеративные входы элемента E_j. Отметим, что число макроблоков в конечном базисе конечно.

Прямыми входами макроблока будем считать входы элементов $E_{i_1}, \ldots, E_{i_m}$, а также все свободные (т. е. те, на которые не подают-

ся выходы других элементов макроблока) входы элемента E_j, кроме одного из итеративных, который будем считать единственным итеративным входом макроблока.

Таким образом, макроблок M имеет сложность $\mathcal{L}_M = L_j + L_{i_1} + \ldots + L_{i_m}$, а число его входов равно $k_M = k'_j + k_{i_1} + \ldots + k_{i_m} + k''_j - m = k_{i_1} + \ldots + k_{i_m} + k_j - m$. *Приведенным весом* макроблока M назовем величину $\rho_M = \frac{\mathcal{L}_M}{k_M - 1}$, и обозначим за ρ_A минимальный приведенный вес среди всех элементов, имеющих хотя бы один итеративный вход, и всех макроблоков в этом базисе.

Для базиса A указанного выше вида введем при j, $j = 1, \ldots, b$, таких что $k''_j \geqslant 2$, следующие величины:

$$\hat{\rho}_j = \frac{L_j}{k''_j - 1}, \quad \theta_j = \frac{k'_j}{k''_j - 1}.$$

Пусть, далее,

$$\hat{\rho}_A = \min_{k''_j \geqslant 2} \hat{\rho}_j, \quad \theta_A = \max_{\hat{\rho}_j = \hat{\rho}_A} \theta_j.$$

Теорема 2 [11]. *Для любой системы ФАЛ A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$, при $n \to \infty$ справедливо соотношение*

$$L_A^C(n) = \hat{\rho}_A \frac{2^n}{n} \left(1 + \frac{(1 - \theta_A \pm o(1)) \log n}{n}\right).$$

Эта теорема устанавливает поведение функции Шеннона для сложности СФЭ с прямыми и итеративными входами в произвольном полном базисе, которая имеет «стандартный» порядок роста $2^n/n$.

Задача синтеза формул в базисах с прямыми и итеративными входами оказывается существенно сложнее. Как будет показано, в этом случае соответствующая функция Шеннона не всегда имеет «стандартный» для формул порядок роста $2^n / \log n$.

Следующая теорема устанавливает асимптотику функции Шеннона для сложности формул в базисах, итеративное замыкание которых содержит класс монотонных ФАЛ.

Теорема 3 [12]. *Для любой системы ФАЛ A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$, такой, что $\delta(A) \in \{M, P_2(\mathcal{Y})\}$, при $n \to \infty$ справедливо соотношение*

$$L_A^{\Phi}(n) \sim \rho_A \cdot \frac{2^n}{\log n}.$$

Для таких базисов функция $L_A^{\Phi}(n)$ имеет «стандартный» для формул порядок роста $2^n/\log n$, при этом константа в асимптотике отличается от константы для случая СФЭ. В остальных семействах базисов в классификации по их итеративным замыканиям существуют примеры, для которых эта функция имеет «граничный» порядок роста 2^n:

Теорема 4 [10]. *Для каждого δ, $\delta \in \{I, O, D, K, L\}$, существует базис A такой, что $\delta(A) = \delta$ и при этом*

$$L_A^{\Phi}(n) = \Theta\left(2^n\right).$$

При этом оказалось, что при переходе от базиса к базису сложность индивидуальной ФАЛ может кардинально меняться в рамках одного и того же семейства. Пусть $l_n = x_1 \oplus \ldots \oplus x_n$ — линейная ФАЛ n, $n \geqslant 1$, БП.

Теорема 5 [10]. *Пусть*

$$\begin{aligned}
A_1 &= \{x_1 y_1 \vee \bar{x_1} y_2\},\\
A_2 &= \{(x_1 \oplus x_2) y_1, (x_1 \oplus x_2 \oplus 1) y_1, y_1 \vee y_2\},\\
A_3 &= \{(x_1 \oplus x_2) y_1, y_1 \vee y_2\},\\
A_4 &= \{(x_1 \oplus x_2 \oplus 1) y_1, y_1 \vee y_2\}.
\end{aligned}$$

Тогда справедливы соотношения:

$$L_{A_1}^{\Phi}(l_n) = \Theta(2^n),$$

$$L_{A_2}^{\Phi}(l_n) = \Theta(2^{n/2}),$$

$$c_1 \cdot 2^{n/2} \leqslant L_{A_i}^{\Phi}(l_n) \leqslant c_2 \cdot 3^{n/2}, \quad i = 3, 4,$$

где c_1, c_2 — некоторые положительные константы.

Итеративное замыкание каждого из указанных в теореме базисов образует класс D. Следует отметить, что сложность $L_{A_1}^{\Phi}(f)$ для почти всех ФАЛ $f \in P_2(\mathcal{X})$ равна [11] $o(2^n)$.

В работе [13] рассматривались так называемые обобщённые ДНФ, а из полученных в ней результатов следует, в частности, что

$$L_{A_3}^{\Phi}(n) = \Omega\left(\frac{2^n}{n^{1/4}}\right).$$

В теореме 4 получена асимптотика функции Шеннона для случая тех базисов A, для которых $\delta(A) \supseteq M$. Для некоторых классов таких базисов в следующих теоремах установлены асимптотические оценки высокой степени точности. Для формул в базисе A, все элементы которого имеют только итеративные входы, оценка высокой степени точности для соответствующей функции Шеннона получена в [1] и имеет вид:

$$\rho_A \frac{2^n}{\log n}\left(1 + \frac{\varkappa_A \log\log n \pm O(1)}{\log n}\right),$$

где ρ_A — минимальный приведенный вес элементов из A, а константа $\varkappa_A \in \{0, 1\}$ и зависит только от ФАЛ, реализуемых элементами с минимальным приведенным весом.

Для каждого базиса A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$, обозначим через $\hat{A}$ множество тех элементов базиса A с итеративными входами, которые либо имеют приведенный вес, равный ρ_A, либо входят в макроблоки этого базиса с приведенным весом ρ_A.

Теорема 6 [14]. *Пусть A, $A \subseteq P_2(\mathcal{X} \cup \mathcal{Y})$, — конечный полный базис, такой, что $\delta(A) \supseteq M$. Пусть, далее, справедливо хотя бы одно из следующих утверждений:*

1) $\delta(\hat{A}) \supseteq M$;

2) *базис $\hat{A}$ является полным базисом;*

3) $\delta(\hat{A}) \in \{L, D, K\}$, *множество $\hat{A}$ содержит ФАЛ f вида*

$$f = (\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0,$$

где $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(\mathcal{X})$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, для которой найдутся такие индексы $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, и наборы α, β значений прямых БП, что

$$\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0.$$

Тогда при растущем значении натурального аргумента n, $n \geqslant 2$, справедливо соотношение

$$L_A^{\Phi}(n) = \rho_A \cdot \frac{2^n}{\log n}\left(1 \pm \frac{O(1)}{\log n}\right).$$

Другое поведение остаточного члена в оценках высокой степени точности для функции Шеннона сложности формул рассматриваемого класса демонстрирует следующая теорема.

Теорема 7 [15]. *Пусть*

$$A_1 = \{y_1 \cdot \ldots \cdot y_{k_1}, x_1 \vee \ldots \vee x_{k_2}, \bar{y}_1\};$$
$$A_2 = \{y_1 \vee \ldots \vee y_{k_1}, x_1 \cdot \ldots \cdot x_{k_2}, \bar{y}_1\};$$

где $k_1, k_2 \geqslant 2$. *Тогда для* $i = 1, 2$ *имеют место следующие неравенства:*

$$\rho_{A_i} \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{k_2} \log\log n \pm O(1)}{\log n}\right) \leqslant L^{\Phi}_{A_i}(n) \leqslant$$
$$\leqslant \rho_{A_i} \frac{2^n}{\log n} \left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Если при этом минимальный приведенный вес ρ_{A_i} *базиса* A_i, $i \in \{1, 2\}$, *достигается на макроблоке, отличном от элемента базиса, то справедливо соотношение:*

$$L^{\Phi}_{A_i}(n) = \rho_{A_i} \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{k_2} \log\log n \pm O(1)}{\log n}\right).$$

Итеративное замыкание приведённых в теореме базисов равно $P_2(\mathcal{Y})$.

Работа выполнена при финансовой поддержке гранта РФФИ 15-01-07474.

Список литературы

1. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.

2. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

3. Лупанов О. Б. О сложности реализации функций алгебры логики релейно-контактными схемами // Проблемы кибернетики. Вып. 11. — 1964. — С. 25–48.

4. Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М.: Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с

5. Кондратов А. В. Асимптотические оценки высокой степени точности для сложности реализации функций, связанных с автоматными языками, в некоторых классах схем // Математические вопросы кибернетики. Вып. 13. — М.: Наука, 2004. — С. 279–288.

6. Шиганов А. Е. О сложности ориентированных контактных схем с ограниченной полустепенью исхода // Учёные записки Казанского университета. Серия Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 164–172.

7. Lozhkin S. A., Shiganov A. E. High Accuracy Asymptotic Bounds on the BDD Size and Weight of the Hardest Functions // Fundamenta Informaticae. — V. 104, N. 3. — 2010. — P. 239–253.

8. Яблонский. С. В. Введение в дискретную математику. — М.: Наука, 1986. — 384 с.

9. Ложкин С. А. О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 1999. — № 3. — С. 35–41.

10. Коноводов В. А. Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными входами // Учёные записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, № 3. — С. 76–83.

11. Ложкин С. А. О сложности реализации функций алгебры логики схемами и формулами, построенными из функциональных элементов с прямыми и итеративными переменными // Тр. III Международной конференции «Дискретные модели в теории управляющих систем». — М.: Диалог-МГУ, 1998. — С. 72–73.

12. Ложкин С. А., Коноводов В. А. О сложности формул алгебры логики в некоторых полных базисах, состоящих из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 1. — С. 55–68.

13. Ложкин С. А. Реализация функций алгебры логики схемами из функциональных элементов с задержками // Диссертация на соискание ученой степени кандидата физико-математических наук. — МГУ им. М. В. Ломоносова, 1979.

14. Ложкин С. А., Коноводов В. А. Оценки высокой степени точности для сложности булевых формул в некоторых базисах из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 2. — С. 16–30.

15. Коноводов В. А. Асимптотические оценки высокой степени точности для сложности булевых формул в некоторых базисах, состоящих из элементов с прямыми и итеративными входами // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г. — М.: МАКС Пресс, 2015. — С. 110–113.

КВАНТОВОЕ КРИПТОГРАФИЧЕСКОЕ ХЕШИРОВАНИЕ

Ф. М. Аблаев, М. Ф. Аблаев (Казань)

Криптографическое хеширование предъявляет ряд специальных требований на хеш-функции, обусловленные требованиями противостояния атакам на передаваемую и хранимую информацию [3]. Одним из центральных понятий, определяющих понятие криптографической хеш-функций, является свойство однонаправленности (односторонности, one-way property) функции. Формализация понятия "однонаправленная функция" следующая.

Рассмотрим функцию $f : \Sigma^* \to \Sigma^*$. Определим следующий эксперимент $Invert_{A,f}$ обращения функции f на основе полиномиального по времени алгоритма A и числа $n \in \mathbf{N}$:

Процедура обращения функции f. Процедура обращения

$$Invert_{A,f} : \mathbf{N} \to \{\mathbf{0}, \mathbf{1}\} :$$

- Выбирается произвольный элемент $x \in \Sigma^n$. Вычисляется значение $y = f(x)$.
- Вероятностный (обращающий) алгоритм A для данных входов 1^n и y выдает результат x'.
- Результат процедуры $Invert_{A,f}$ полагается равным 1, если $f(x') = y$ и полагается равным 0, если $f(x') \neq y$.

На основе процедуры $Invert$ формулируется понятие однонаправленной функции. Функцию $f : \Sigma^* \to \Sigma^*$ называют однонаправленной, если выполняются следующие два условия:

1. Функция легко вычислима: существует полиномиальный (от длины аргумента) по времени алгоритм $\mathcal{M}_f$ вычисляющий f; т. е., $\mathcal{M}_f(x) = f(x)$ для всех $x \in \Sigma^*$.
2. Вероятность быстрого обращения функции незначительна: для произвольного полиномиального по времени вероятностного алгоритма A, обращающего функцию f, для произвольного полинома $p(n) \in POLY$ выполняется

$$Pr[Invert_{A,f}(n) = 1] \leq 1/p(n).$$

Известно, что в терминах приведенной выше формализации существование однонаправленной функции влечет $NP \neq P$. Таким

образом все используемые на сегодняшний день однонаправленные функции — функции, для которых не известны быстрые алгоритмы их обращения — являются “условно однонаправленными” (“условно односторонними”).

Классическое хеширование. Требования. Криптографическая хеш-функция h, “сжимающая” слова в алфавите Σ

$$h : \Sigma^* \to \Sigma^*, \qquad h : \Sigma^k \to \Sigma^m, \quad k > m$$

должна удовлетворять (как минимум) следующим требованиям.

1. Функция h должна быть однонаправленной (точнее “условно однонаправленной” на сегодняшний день).
2. Функция h должна быть стойкой к коллизиям первого рода: для заданного сообщения w должно быть “вычислительно сложно” подобрать другое сообщение v, для которого $h(w) = h(v)$.
3. Функция h должна быть стойкой к коллизиям второго рода: должно быть “вычислительно сложно” подобрать пару сообщений (w, v) такую, что $h(w) = h(v)$.
4. Функция h должна удовлетворять свойству лавинного эффекта (Avalanche effect): изменение одного символа аргумента должно вызывать изменение в среднем половины выходных символов (лавинное изменение).

Квантовое хеширование. Пусть $\mathbf{X}$ — конечное множество, $K = |\mathbf{X}|$. Например, $\mathbf{X} = \Sigma^k$ — множество слов длины k в алфавите Σ или $\mathbf{X} = \{0, 1, \ldots, q-1\}$ — конечное множество чисел.

Мы используем систему понятий и обозначений работ [1–4]. Предлагается следующая формализация понятия односторонней квантовой функции (quantum one-way function).

1. Пусть $\psi : \mathbf{X} \to (\mathbf{H}^2)^{\otimes s}$ квантовая функция.
2. Пусть дана функция $D : (\mathbf{H}^2)^{\otimes s} \to \mathbf{X}$. Будем называть D — “декодированием квантовой s-кубитной системы” (кратко — “декодированием”). Содержательно декодирование D — это извлечение информации из квантового системы, состоящее из процесса измерения квантового состояния $|\psi\rangle \in (\mathbf{H}^2)^{\otimes s}$ и алгоритма преобразования результата измерения в элемент w множества X.

Определение. Пусть $\psi : X \to (\mathbf{H}^2)^{\otimes s}$ квантовая функция. Пусть X случайная величина, равномерно распределенная над множеством $\mathbf{X}$, $\{Pr[X = w] = 1/|\mathbf{X}| : \mathbf{w} \in \mathbf{X}\}$. Пусть случайная величина $Y = \mathbf{D}(|\psi(X)\rangle)$ над X, получена применением декодирования D к значению $|\psi(X)\rangle$ функции ψ случайной величины X. Пусть $\epsilon > 0$.

Будем называть функцию ψ односторонней ϵ-устойчивой (a one-way ϵ-resistant), если для произвольного декодирования $\mathbf{D}$ вероятность $Pr[Y = X]$ события, "декодирование D верно определяет значение X из значения $|\psi(X)\rangle$" ограничена величиной ϵ

$$Pr[Y = X] \leq \epsilon.$$

Содержательно квантовое s кубитное состояние $|\psi\rangle$ может "содержать огромный объем информации", при этом один из фундаментальных законов квантовой информатики, известный как Теорема Холево, утверждает, что при извлечении информации из состояния $|\psi\rangle$ можно получить не более s бит информации о $|\psi\rangle$. Для наших целей достаточен следующий специальный вариант формализации [5] Теоремы Холево.

Свойство. *Пусть случайная величина X равномерно распределена на множестве $\{0,1\}^k$. Пусть случайная величина Y на $\{0,1\}^k$ задается квантовой функцией $\psi : \{0,1\}^k \to (\mathbf{H}^2)^{\otimes s}$ и декодированием $D : (\mathbf{H}^2)^{\otimes s} \to \{0,1\}^k$ по правилу $Y = D(|\psi(X)\rangle)$.*

Тогда вероятность $Pr[Y = X]$ правильного извлечения значения случайной величины X декодированием D из значения $|\psi(X)\rangle$ оценивается сверху следующим образом

$$Pr[Y = X] \leq \frac{2^s}{2^k}.$$

Определение. *Функция $\psi : \mathbf{X} \to (\mathbf{H^2})^{\otimes \mathbf{s}}$ называется коллизия δ-устойчивой (resistant), если для каждой пары w, w' различных элементов из $\mathbf{X}$ выполняется*

$$|\langle\psi(w)|\psi(w')\rangle| \leq \delta.$$

Понятие коллизия δ-устойчивости обеспечивает выполнение требований 2–4 для классической хеш-функции [3, 4].

Предлагается следующее определение квантовой хеш-функции.

Определение. Пусть $K = |\mathbf{X}|$, $s \geq 1$. Квантовую ϵ-одностороннюю и δ-устойчивую функцию $\psi : \mathbf{X} \to (\mathbf{H}^2)^{\otimes s}$ будем называть (ϵ, δ)-устойчивой квантовой хеш-функцией.

Два примера хеш-функций.

Следующие два простых примера показывают особенности (ϵ, δ)-устойчивой квантовой хеш-функций.

Пример 1. *Пусть число* $v \in \{0, \ldots, 2^k - 1\}$ *отображается в кубит по правилу:*

$$\psi : v \mapsto \cos\left(\frac{2\pi v}{2^k}\right)|0\rangle + \sin\left(\frac{2\pi v}{2^k}\right)|1\rangle.$$

Извлечение информации из кубита $|\psi\rangle$ путем его измерения относительно базиса $\{|0\rangle, |1\rangle\}$ дает нам следующее. Функция ψ односторонняя $1/2^k$-устойчивая и коллизия δ-устойчива для $\delta = \cos\left(\pi/2^{k-1}\right)$. Таким образом функция ψ обладает хорошим свойством одосторонности, но плохим свойством устойчивости к коллизиям для больших k.

Пример 2. *Здесь мы считаем число* $v \in \{0, \ldots, 2^k - 1\}$ *двоичным словом* $v \in \{0, 1\}^k$. *Пусть* $v = \sigma_1 \ldots \sigma_k$. *Мы представляем слово* v *в виде системы из* k *кубит:*

$$\psi : v \mapsto |v\rangle = |\sigma_1\rangle \cdots |\sigma_k\rangle.$$

В этом случае извлечение информации из $|\psi\rangle = |v\rangle$ путем измерения $|\psi\rangle$ относительно базиса $\{|0 \ldots 0\rangle, \ldots, |1 \ldots 1\rangle\}$ дает нам следующее. Различные слова отображаются в ортогональные состояния поэтому ψ абсолютно устойчива к колизиям, но потеряно свойство одонаправленности — функцию ψ легко обратить. Таким образом в отличии от примера 1 квантовая функция ψ из примера 2 — односторонне 1-устойчива и коллизия 0-устойчива.

"Сбалансированная" квантовая хеш-функция. Рассмотренные выше примеры показывают, что устойчивость однонаправленная и устойчивость к коллизиям конфликтные свойства: чем более квантовая функция однонаправленно устойчива тем менее она устойчива к коллизиям и наоборот. Поэтому естественно ввести понятие "сбалансированной" квантовой хеш-функции.

В [2] приведено свойство, которое дает нижнюю оценку на требуемое число кубит квантовой системы для требуемой коллизии δ-устойчивости.

Свойство. *Если функция* $\psi : \mathbf{X} \to (\mathbf{H^2})^{\otimes \mathbf{s}}$ *коллизия* δ*-устойчива. то*

$$s \geq \log\log|\mathbf{X}| - \log\log\left(1+\sqrt{2/(1-\delta)}\right) - 1.$$

Приведенные выше свойства определяют рамки конструкции "сбалансированной" квантовой (ϵ,δ)-устойчивой хеш-функции [4]. Пусть требуется построить квантовую "максимально одностороннюю" функцию, коллизия δ-устойчиво, хеширующую элементы множества X мощности K. Тогда, в случае построения квантовой $(K;s)$ функции коллизия δ-устойчивой с $s \approx \log\log K - c(\delta)$ кубитами, мы получаем квантовую хеш-функцию, которая будет квантовой (ϵ,δ)-устойчивой хеш-функцией для $\epsilon \approx \log K/K$. Такую функцию естественно считать сбалансированной квантовой хеш-функцией.

Конструкция сбалансированной квантовой хеш-функции. Пример сбалансированной квантовой хеш-функции приведен в работе [3]. Здесь излагаются конструкция построения такой квантовых хеш-функций, в терминах изменяющих комплексную "фазу" квантовой системы [1]. Это позволяет не только упростить математические выкладки, но и представить конструкции квантовых хеш-функций в терминах квантово-оптических технологий. Пусть q — простое число, $\mathbf{F}_q$ — поле, а $B \subset \mathbf{F}_q$. Квантовая функция

$$\psi_{q,B} : \{0,1\}^{\log q} \to (\mathbf{H}^2)^{\otimes \log|B|} \tag{1}$$

имеет вид

$$|\psi_{q,B}(a)\rangle = \frac{1}{\sqrt{|B|}} \sum_{j=1}^{|B|} e^{i\frac{2\pi a b_j}{q}} |j\rangle.$$

Справедлив следующий результат.

Теорема. *Для числа* $\delta(q) = 1/(\log q)^{O(1)}$ *существует множество ("хорошее множество")* $B \subset \mathbf{F}_q$ *мощности* $|B_{\delta,q}| = (\log q)^{O(1)}$ *такое, что для* $s = \log(\log q)^{O(1)}$ *квантовая хеш-функция*

$$\psi_{q,B} : \{0,1\}^{\log q} \to (\mathbf{H}^2)^{\otimes s}$$

является (ϵ,δ)*-устойчивой квантовой хеш-функцией, где*

$$\epsilon \leq \frac{(\log q)^{O(1)}}{q}.$$

Приведенная выше общая нижняя оценка на число s используемых в конструкции квантовой хеш функции дает следующую конкретную нижнюю оценку на число s используемых в конструкции $\psi_{q,B}$ кубит:

$$s \geq \log\log q.$$

Работа выполнена в рамках Российской государственной программе повышения конкурентоспособности Казанского федерального университета и при поддержке грантов РФФИ 14-07-00878, 14-07-00557, 15-37-21160.

Список литературы

1. Аблаев М. Ф. О конструкции квантовых хеш-функций // Материалы IX Международной конференции "Дискретные модели в теории управляющих систем". — М.: Изд-во механико-математического ф-та МГУ, 2015. — С. 8–9.

2. Ablayev F.M., Ablayev M.F. Quantum hashing via classical e-universal hashing constructions // arXiv:1404.1503v2 [quant-ph].

3. Ablayev F.M., Vasiliev A.V. Cryptographic quantum hashing // Laser Phys. Lett. — 2015. — 11 025202.

4. Ablayev F.M., Ablayev M.F., Vasiliev A.V. On the balanced quantum hashing // Journal of Physics: Conference Series. —V. 681, No. 1. 2015 — P. 012019.

5. Nayak A. Optimal lower bounds for quantum automata, random access codes // arXiv:quant-ph/9904093v, 1999.

СЛОЖНОСТЬ ПОЛИНОМИАЛЬНЫХ ПРЕДСТАВЛЕНИЙ ФУНКЦИЙ k-ЗНАЧНЫХ ЛОГИК

С. Н. Селезнева (Москва)

В докладе предлагается обзор сложности представлений и приближений функций k-значной логики полиномиальными формами. Пусть $E_k = \{0, 1, \ldots, k-1\}$, где $k \geq 2$ — натуральное число, $P_k = \{f^{(n)} : E_k^n \to E_k \mid n = 0, 1, 2, \ldots\}$ — множество всех функций k-значной логики.

Первые две части доклада посвящены представлениям функций k-значных логик полиномиальными формами. Полиномиальной

формой (ПФ) называется сумма по модулю k произведений каких-то базисных функций одной переменной, длиной $l(P)$ ПФ P называется число ее попарно различных слагаемых. Классы ПФ различаются видом базисных функций. Длиной $l^K(f)$ функции k-значной логики f в классе K назовем наименьшую длину среди всех ПФ из класса K, представляющих эту функцию. Рассматривается наибольшая длина $L_k^K(n)$ в классе K среди всех функций k-значной логики, зависящих от n переменных. В этих частях мы также коснемся вопросов сложности представления систем функций k-значной логики полиномиальными формами. Сложностью системы ПФ из класса K называется число попарно различных слагаемых во всех ПФ этой системы. Сложностью $l^{\mathrm{K}}(F)$ системы F функций k-значной логики в классе K называется наименьшая сложность среди всех систем ПФ в классе K, представляющих все функции этой системы. Рассматривается наибольшая сложность $L_k^{\mathrm{K}}(m,n)$ в классе K среди всех систем с m функциями, зависящими от одних и тех же n переменных.

В первой части доклада расматриваются ПФ для функций алгебры логики ($k=2$).

Поляризованной полиномиальной формой (ППФ) по вектору поляризации $\delta=(d_1,\ldots,d_n)\in E_2^n$ называется сумма по модулю два произведений поляризованных переменных $x_i\oplus d_i$. Каждая функция алгебры логики $f(x_1,\ldots,x_n)$ представима однозначной ППФ $P^\delta(f)$ по каждому вектору $\delta\in E_2^n$, при нулевом векторе поляризации получаем полином Жегалкина $P(f)$ [1]. В [2, 3] найдены некоторые оценки $L_2^{\text{ППФ}}(n)$, в [4] доказано $L_2^{\text{ППФ}}(n)=\lfloor\frac{2}{3}\cdot 2^n\rfloor$. Нижняя оценка в [4] получена предъявлением последовательностей симметрических функций алгебры логики $f_n(x_1,\ldots,x_n)$, для которых $l^{\text{ППФ}}(f_n)\geq\lfloor\frac{2}{3}\cdot 2^n\rfloor$. В [5] найдено $L_2^{\text{ППФ}}(m,n)=L_{S_2}^{\text{ППФ}}(m,n)=2^n$ при $m\geq 2$, $n\geq 1$, где S_2 — множество всех симметрических функций алгебры логики. Нижняя оценка получена предъявлением систем симметрических функций алгебры логики с указанной сложностью, функции из [2].

Полиномиальной нормальной формой (ПНФ) называется сумма по модулю два произведений переменных или их отрицаний. В [6] получено $L_2^{\text{ПНФ}}(n)\geq\frac{2^n}{n\log_2 3}$. В [7] найдено $L_2^{\text{ПНФ}}(n)\leq\frac{2^{n+1}}{n}(\log_2 n+1)$, но с учетом оценки из [8] по теореме из [7] получается $L_2^{\text{ПНФ}}(n)=\Theta\left(\frac{2^n}{n}\right)$. Отсюда с учетом нижней мощностной оценки следует, что для сложности систем с m функциями в классе ПНФ справедливо

$L_2^{\text{ПНФ}}(m,n) = \Theta\left(m \cdot \frac{2^n}{n}\right)$ при $m = o(n)$ и $L_2^{\text{ПНФ}}(m,n) = \Theta\left(2^n\right)$ при $n = O(m)$.

Во второй части доклада расматриваются ПФ для функций многозначных логик ($k \geq 3$). Каждая функция k-значной логики представима полиномом по модулю k тогда и только тогда, когда k — простое число. Если в полиномах степени переменных не превосходят $k-1$, то представление однозначно [1]. Далее считаем, что k — простое число, и степени переменных в полиномах не выше $k-1$. Можно рассматривать полиномы относительно операций поля $(E_k; +, \cdot)$ (если такое поле существует) [1].

Поляризованной полиномиальной формой (ППФ) по вектору поляризации $\delta = (d_1, \ldots, d_n) \in E_k^n$ называется сумма по модулю k произведений поляризованных переменных $x_i + d_i$. Каждая функция k-значной логики $f(x_1, \ldots, x_n)$ представима однозначной ППФ $P^\delta(f)$ по каждому вектору $\delta \in E_k^n$ [9], при нулевом векторе поляризации получаем полином $P(f)$. Найдены следующие оценки в классе ППФ: $L_k^{\text{ППФ}}(n) \leq \frac{k(k-1)}{k(k-1)+1} \cdot k^n$ [9], $L_k^{\text{ППФ}}(n) \leq \frac{k(k-1)-1}{k(k-1)} \cdot k^n$ $(k \geq 3)$ [10], $\frac{k-1}{k} \cdot k^n \lesssim L_k^{\text{ППФ}}(n)$ [11], $L_k^{\text{ППФ}}(1) = k-1$ [12]. В [13, 5] доказано $L_3^{\text{ППФ}}(n) \geq \lfloor \frac{3}{4} \cdot 3^n \rfloor$. Оценки из [13, 5] получены предъявлением последовательностей функций трехзначной логики $f_n(x_1, \ldots, x_n)$, для которых $l^{\text{ППФ}}(f_n) \geq \lfloor \frac{3}{4} \cdot 3^n \rfloor$, в [5] функции — симметрические. В [5] также найдено $L_3^{\text{ППФ}}(m,n) = L_{S_3}^{\text{ППФ}}(m,n) = 3^n$ при $m \geq 2$, $n \geq 1$, где S_3 — множество всех симметрических функций трехзначной логики логики. Нижняя оценка получена предъявлением систем симметрических функций трехзначной логики с указанной сложностью.

Пусть $\{s_{0,i}(x_i), s_{1,i}(x_i), \ldots, s_{k-1,i}(x_i)\}$ — множество, образующее базис функций одной переменной, обобщенным вектором поляризации называется набор таких множеств для переменных $x_1, \ldots, x_n$. Каждая функция k-значной логики однозначно представляется ПФ, в которой сомножители в слагаемых только из этих базисных множеств [14, 15]. Получаем обобщенно поляризованные ПФ (ОППФ), если для каждого базисного множества степени полиномов от 0 до $k-1$, и квазиполиномиальные формы (КВПФ), если базисные множества без дополнительных ограничений. Найдены следующие оценки в классах ОППФ и КВПФ: $L_k^{\text{ОППФ}}(n) \leq \frac{k}{k+1} \cdot k^n$ [14], $L_k^{\text{ОППФ}}(n) \leq \frac{k+(k-1)^{-1}-1}{k+(k-1)^{-1}} \cdot k^n$ [10], $\frac{k-1}{k} \cdot k^n \lesssim L_k^{\text{ОППФ}}(n)$ [14], $L_k^{\text{КВПФ1}}(n) \leq \frac{k}{k+1} \cdot k^n$ [15], где КВПФ1 — подкласс квазиполино-

мов, в которых базисные множества по всем переменным, за исключением x_1, — $\{1, x_i, \ldots, x_i^{k-1}\}$, $L_k^{\text{КВПФ}}(n) \le \frac{k-1}{k-k^{1-k}} \cdot k^n$ [16]. Вектором коэффициентов ПФ из класса K, в котором функции k-значной логики представляются однозначно, называется вектор с k^n коэффициентами этой ПФ при всех возможных слагаемых в каком-то их упорядочении. Матрица перехода от вектора коэффициентов полинома функции f к вектору коэффициентов ее ПФ в классах ППФ, ОППФ, КВПФ является кронекеровым произведением n матриц размера $k \times k$. Классы ППФ, ОППФ, КВПФ можно определять как классы матричных кронекеровых форм [16, 10].

Полиномиальной нормальной формой (ПНФ) называется сумма по модулю k произведений поляризованных переменных $x_i + d$, $d \in E_k$. В отличие от ППФ в ПНФ поляризация переменной может меняться от слагаемого к слагаемому. Получены следующие оценки в классе ПНФ: $L_k^{\text{ПНФ}}(n) \lesssim 2 \cdot \frac{k^n}{n} \cdot \ln n$ [17], $\frac{k^n}{n \log_k (k(k-1)+1)} \lesssim L_k^{\text{ПНФ}}(n)$ [17], $L_k^{\text{ПНФ}}(n) = \Theta\left(\frac{k^n}{n}\right)$ [18]. Отсюда с учетом нижней мощностной оценки следует, что для сложности систем с m функциями в классе ПНФ справедливо $L_k^{\text{ПНФ}}(m,n) = \Theta\left(m \cdot \frac{k^n}{n}\right)$ при $m = o(n)$ и $L_k^{\text{ПНФ}}(m,n) = \Theta\left(k^n\right)$ при $n = O(m)$.

Третья часть доклада посвящена приближению функций k-значных логик полиномами при $k \ge 2$.

Рассматриваются длина и ранг полиномов, приближающих функции k-значной логики с заданной точностью. Если k — простое число, то каждая функция k-значной логики f представима однозначным полиномом $P(f)$, в котором степени переменных не выше $k-1$. Функция $g(x_1, \ldots, x_n)$ называется приближением функции $f(x_1, \ldots, x_n)$ с точностью δ, $0 \le \delta \le 1$, если доля наборов значений переменных, в которых функции f и g различаются, не превосходит δ. Полином $P(g)$ приближает функцию k-значной логики f с точностью δ, если функция g является приближением функции f с точностью δ.

Длиной $l(P)$ полинома P называется число его попарно различных слагаемых с ненулевыми коэффициентами, рангом $r(P)$ полинома P называется наибольшее число различных переменных, перемножающихся в его слагаемых с ненулевыми коэффициентами, $r(0) = 0$. Рангом $r^\delta(f)$ (длиной $l^\delta(f)$) функции k-значной логики f с точностью δ наименьший ранг (наименьшая длина) среди всех полиномов, приближающих функцию f с точностью δ. Рассматриваются наибольший ранг $r_k^{\delta_n}(n)$ и наибольшая длина $l_k^{\delta_n}(n)$ с точностью δ_n

функций k-значной логики, зависящих от n переменных. Всегда считаем, что $\delta_n \to 0$ при $n \to \infty$. Случай $\delta_n = \frac{q}{k^n}$ будем обозначать $r_k^{(q)}(n)$ и $l_k^{(q)}(n)$, приближение с точностью до q точек.

Получены следующие оценки ранга полиномов, приближающих функции k-значной логики с заданной точностью: $r_2^\delta(n) = 0$ при $\delta \geq \frac{1}{2}$ [19], $r_k^\delta(n) = 0$ при $\delta \geq \frac{k-1}{k}$ [20], $r_2^\delta(n) \sim \frac{1}{2} \cdot n$ при $0 < \delta < \frac{1}{2}$ [19], $r_k^\delta(n) \sim \frac{k-1}{k} \cdot n$ при $0 < \delta < \frac{k-1}{k}$ [20], $r_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot n$ при $\frac{1}{k^n} = o(\delta_n)$ [20], $r_k^{(q)}(n) = n$ при $n \geq n_0$, $k \geq 3$ [20], $r_2^{(q)}(n) = n-2$ при $n \geq n_0$, $q \geq 2$ [20] (совм. с В.Б. Алексеевым (2015 г.)), $r_2^{(1)}(n) = n - 1$ [20].

Найдены следующие оценки длины полиномов, приближающих функции k-значной логики с заданной точностью: $l_2^\delta(n) = 1$ при $\delta \geq \frac{1}{2}$ [19], $l_k^\delta(n) = 1$ при $\delta \geq \frac{k-1}{k}$ [20], $l_2^\delta(n) \leq \frac{1}{2} \cdot (1-\delta) \cdot 2^n + o(2^n)$ при $0 < \delta < \frac{1}{2}$ [19], $l_k^\delta(n) \leq \frac{k-1}{k} \cdot (1-\delta) \cdot k^n + o(k^n)$ при $0 < \delta < \frac{k-1}{k}$ [20], $l_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot k^n$ при $\delta_n \geq (\frac{k-1}{k})^n$ [20], $l_2^{(q)}(n) \sim \frac{1}{2} \cdot 2^n$ при $q \geq 1$ [20].

Список литературы

1. Яблонский С. В. Функциональные построения в k-значной логике // Труды Математического института им. В. А. Стеклова АН СССР. — 1958. — Т. 51. — С. 5–142.

2. Sasao T., Besslich P. On the complexity of mod-2 sum PLA's // IEEE Trans. on Comput. — 1990. — V. 39, N 2. — P. 262–266.

3. Супрун В. П. Сложность булевых функций в классе канонических поляризованных полиномов // Дискретная математика. — 1993. — Т. 5, вып. 2. — С. 111–115.

4. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, вып. 3. — С. 323–326.

5. Селезнева С. Н. Сложность систем функций алгебры логики и систем функций трехзначной логики в классах поляризованных полиномиальных форм // Дискретная математика. — 2015. — Т. 27, вып. 1. — С. 111–122.

6. Even S., Kohavi I., Paz A. On minimal modulo 2 sums of products for switching functions // IEEE Trans. Elect. Comput. — 1967. — P. 671–674.

7. Кириченко К. Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная математика. — 2005. — Т. 17, вып. 3. — С. 80–88.

8. Cooper J. N., Ellis R. B., Kahng A. B. Asymmetric binary covering codes // Journal of Combinatorial Theory. Series A. — 2002. — V. 100,

N 2. — P. 232–249.

9. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.

10. Балюк А. С., Янушковский Г. В. Верхние оценки функций над конечными полями в некоторых классах кронекеровых форм // Известия Иркутского государственного университета. Серия: Математика. — 2015. — Т. 14. — С. 3–17.

11. Алексеев В. Б., Вороненко А. А., Селезнева С. Н. О сложности реализации функций k-значной логики поляризованными полиномами // Сб. Труды V Международной конференции «Дискретные модели в теории управляющих систем» (Ратмино, 26–29 мая 2003 г.). — М.: МАКС Пресс, 2003. — С. 8–9.

12. Селезнева С. Н. О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 117–121.

13. Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — вып. 3. — С. 40–45.

14. Селезнева С. Н. О сложности обобщенно-поляризованных полиномов k-значных функций // Дискретная математика. — 2009. — Т. 21, вып. 4. — С. 20–29.

15. Селезнева С. Н. О сложности k-значных функций в одном классе полиномов // Сб. Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Издательство Нижегородского университета, 2011. — С. 430–434.

16. Балюк А. С. О верхней оценке сложности задания квазиполиномами функций над конечными полями // Известия Иркутского государственного университета. Серия: Математика. — 2014. — Т. 10. — С. 3–12.

17. Селезнева С. Н., Дайняк А. Б. О сложности обобщенных полиномов k-значных функций // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2008. — вып. 3. — С. 34–39.

18. Башов М. А., Селезнева С. Н. О длине функций k-значной логики в классе полиномиальных нормальных форм по модулю k // Дискретная математика. — 2014. — Т. 26, вып. 3. — С. 3–9.

19. Джавадов Р. М. О сложности приближенного задания функций алгебры логики // Доклады АН СССР. — 1982. — Т. 265,

вып. 1. — С. 24–27.

20. Селезнева С. Н. О приближении с заданной точностью функций k-значных логик полиномами // Дискретная математика. — 2008. — Т. 20, вып 2. — С. 32–45.

ЗАДАЧА МИНИМИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ: УСЛОВИЯ МИНИМАЛЬНОСТИ И ВЕРОЯТНОСТНЫЙ МЕТОД

И. П. Чухров (Москва)

Задача минимизации булевых функций обычно рассматривается в двух эквивалентных моделях — аналитической и геометрической [1]. В аналитической модели используются понятия: булева функция, импликанта, дизъюнктивная нормальная форма(ДНФ), зависящие от n переменных. В геометрической модели эквивалентными понятиями являются подмножество вершин, грань, комплекс граней в n-мерном единичном кубе B^n. Задача минимизации булевых функций для аддитивной сложности является *задачей о покрытии* множества единичных вершин функции гранями единичного куба.

В обзорных статьях [2–4] изложены различные алгоритмические вопросы и подходы к решению задачи о покрытии. При точном решении задачи для уменьшения вычислительной сложности сначала выполняются преобразования, направленные на сокращение размерности задачи. Используемые для этого подходы приемлемой трудоемкости основаны на понятиях: связность, неприводимое покрытие, ядровые множества, доминирование. В результате итеративных преобразований исходная задача сводится к задаче о покрытии для

не сокращаемого множества, которое называется *циклическим ядром* [4]. Для таких задач точные алгоритмы обычно используют переборные схемы и относятся к методам ветвей и границ. Возможность выполнения перебора в значительной степени определяется применимостью достаточных условий минимальности, т. е. достижимостью нижних границ используемых для оценки минимальной сложности покрытия. При этом обычно используются нижние границы, основанные на понятии независимого множества. Численные эксперименты также показывают, что основные затраты приходятся на доказательство оптимальности решения [5].

Характерной чертой задачи минимизации булевых функций является возможность нахождения оптимального решения уменьшением ранга и удалением импликант. Такие преобразования реализуются локальными алгоритмами [6] конечного порядка и их трудоемкость считается приемлемой.

Полиэкстремальность задачи минимизации булевой функции заключается в возможности существования большого числа локальных экстремумов, в роли которых выступают тупиковые покрытия (ДНФ), среди которых содержатся глобальные экстремумы — минимальные покрытия (ДНФ).

Задача о поведении параметров $\mu(n)$ и $\tau(n)$ — максимальных значений числа тупиковых и минимальных ДНФ булевой функции с ростом числа переменных была поставлена С. В. Яблонским в связи с оценкой трудоемкости минимизации булевых функций алгоритмами, использующими переборные схемы поиска решения. Отношение числа минимальных к числу тупиковых ДНФ булевой функции является верхней оценкой вероятности нахождения минимальной ДНФ при случайном выборе тупиковой, которая в худшем случае не превосходит $\chi^{-1}(n)$, где $\chi(n)$ — максимальное значение отношения числа тупиковых к числу минимальных ДНФ.

Большинство задач, которые возникают при минимизации булевых функций, относится к полным или трудно решаемым комбинаторным задачам [7, 8]. Поэтому актуальными являются задачи выделения эффективно и неэффективно минимизируемых классов булевых функций, определения достаточных критериев минимальности и обоснованности сокращения перебора в алгоритмах минимизации.

Множество булевых функций n переменных обозначим через P_n.

Для функции $f \in P_n$ обозначим:

$\mathcal{T}(f)$ и $\tau(f)$ — множество и число тупиковых комплексов граней;

$\mathcal{M}_{\mathcal{L}}(f)$ и $\mu_{\mathcal{L}}(f)$ — множество и число $\mathcal{L}$-минимальных комплексов граней;

$\mathcal{M}_{\cap\mathbb{C}}(f)$ и $\mu_{\cap\mathbb{C}}(f)$ — множество и число минимальных комплексов граней относительно любой меры из класса мер сложности $\mathbb{C}$;

$\chi_{\mathcal{L}}(f) = \tau(f)/\mu_{\mathcal{L}}(f)$ — отношение числа тупиковых и $\mathcal{L}$-минимальных комплексов граней.

Максимальное значение параметра $q_v(f)$ на множестве функций P_n будем обозначать через $q_v(n)$, например, $\tau(n)$ или $\mu_{\mathcal{L}}(n)$.

Число тупиковых и $\mathcal{L}$-минимальных комплексов граней в кубе B^n обозначим через $T(n)$ и $M_{\mathcal{L}}(n)$ соответственно.

Обозначения параметра без указания меры сложности используются в утверждениях, которые справедливы одновременно для минимальных и кратчайших тупиковых комплексов.

Пояс куба B^n, состоящий из слоев $B_i^n = \{\tilde{x} \in B^n \colon \|\tilde{x}\| = i\}$ с номерами $i = m-k, \ldots, m$, где $0 \le k \le m \le n$, обозначим через $S_{m-k,m}^n$.

Функция называется *поясковой*, если множество единичных вершин функции совпадает с поясом единичного куба.

Функция называется *симметрической*, если она не меняет значения при любой перестановке переменных. Симметрическая функция однозначно представляется в виде дизъюнкции поясковых функций, которые являются компонентами связности. Множество симметрических функций n переменных обозначим через S_n.

Целую часть и верхнюю целую часть числа x обозначим через $\lfloor x \rfloor$ и $\lceil x \rceil$ соответственно. Сколь угодно малая положительная константа обозначается через ε. Под log понимается логарифм по основанию 2. Асимптотические оценки числовых параметров в единичном кубе B^n всюду получаются при $n \to \infty$.

Из очевидных соотношений $\mu(n) \le \tau(n)$, $\chi(n) \le \tau(n)$ и мощностных соображений получается верхняя оценка [9, стр. 125]:

$$\log \chi(n), \log \mu(n) \le \log \tau(n) \lesssim n2^n \log \tfrac{3}{2}.$$

Нижние оценки максимальных значений, полученные конструктивными методами, последовательно улучшались в работах С. В. Яблонского, Ю. И. Журавлёва, В. В. Глаголева, Ю. Л. Васильева, А. А. Сапоженко, И. П. Чухрова:

$$\log \mu(n) \ge \log \max_{f \in S_n} \mu(f) \sim n\binom{n}{\lfloor n/2 \rfloor} \sim \sqrt{2/\pi}\sqrt{n}2^n,$$

$$\log \chi(n) \ge \log \max_{f \in S_n} \chi(f) \ge \Theta\left(n\tbinom{n}{\lfloor n/2 \rfloor}\right) \asymp \sqrt{n}2^n.$$

Исследование *симметрических функций* и, в частности, поясковых функций объяснялось существованием гипотезы о достижимости значений $\tau(n)$ и $\mu(n)$ на симметрических функциях. При этом

отмечалось, что «для числа кратчайших ДНФ известна лишь оценка снизу его максимального значения нетривиальные оценки сверху, нетривиальные оценки типичных значений неизвестны» [9, стр. 102].

1. Меры сложности и доказательство минимальности [10]

Функционал $\mathcal{L}$, определенный на множестве комплексов граней, является мерой сложности, если он удовлетворяет аксиомам неотрицательности, монотонности, выпуклости и инвариантности относительно изоморфизма [11, стр. 298].

Комплекс граней называется $\mathcal{L}$-*минимальным*, если он имеет наименьшую меру сложности $\mathcal{L}$ среди эквивалентных комплексов граней.

Кратчайшим называется l-минимальный комплекс и *минимальным* называется L-минимальный комплекс, где l — число граней и L — сумма рангов граней в комплексе.

Грани I и I' называются *изоморфными*, если существует такая перестановка координат π, что $\pi(I') = I$.

Грань I *доминирует* грань I', если существует такая перестановка координат π, что $\pi(I') \subset I$.

Комплекс граней называется минимальным относительно класса мер сложности $\mathbb{C}$ или кратко $\mathbb{C}$-*минимальным*, если он является $\mathcal{L}$-минимальным для любой меры сложности $\mathcal{L}$ из класса $\mathbb{C}$.

В теории выбора рассматривается два подхода к сравнению альтернатив — *порядковый и количественный.*

Формализм порядкового подхода основан на теории бинарных отношений: сравнение любой пары альтернатив и выделение предпочтительной, что не требует их количественной оценки. Альтернативы представляются частично упорядоченным множеством и решение задачи заключается в нахождении недоминируемых альтернатив.

Формализм количественного подхода основан на представлении отношения предпочтения на множестве альтернатив функцией полезности. Решение задачи выбора сводится к решению оптимизационной задачи и нахождению альтернатив с максимальным значением функционала полезности.

Функционал меры сложности порождает линейное бинарное отношение на множестве комплексов граней единичного куба. Аксиомы неотрицательности, монотонности и выпуклости определяют свойство *нестрогого порядка* при уменьшении ранга или удаления грани комплекса. Аксиома инвариантности определяет свойство *эквивалентности* изоморфных комплексов граней, т. е. неразличимости по сложности. Обоснование минимальности или не минимальности комплекса граней выполняется с использованием порядковых

свойств, которые порождаются мерой сложности. Для этого определяются *классы мер сложности*, позволяющие установить эквивалентность или строгий порядок по сложности для комплексов граней:

Λ_π — меры сложности удовлетворяют усиленному свойству *инвариантности относительно изоморфизма*, т. е. при замене некоторых граней на изоморфные сложность комплекса не изменяется;

Λ_l — меры сложности удовлетворяют свойству *строгой монотонности относительно длины*, т. е. сложность комплекса уменьшается при удалении произвольной грани;

Λ_L — меры сложности удовлетворяют свойству *строгой монотонности относительно сложности*, т. е. сложность комплекса уменьшается при уменьшении ранга или удалении произвольной грани;

Λ_+ — меры сложности удовлетворяют свойству *аддитивности*, т. е. сложность комплекса граней равна сумме сложностей граней. Аддитивными являются меры сложности l и L, а также L_0 и L_1 — число направлений грани равных 0 и, соответственно, 1, т. е. число переменных с отрицанием и без отрицания в импликанте.

Комплекс граней называется *неприводимым*, если после удаления любой грани получается комплекс другой булевой функции. *Тупиковым* называется неприводимый комплекс граней, в котором все грани максимальные. Любой $\mathcal{L}$-минимальный комплекс является неприводимым для $\mathcal{L} \in \Lambda_l$ и является тупиковым для $\mathcal{L} \in \Lambda_L$.

Используемые при минимизации функционалы обычно являются мерами сложности из классов $\Lambda_\pi \cap \Lambda_l$ или $\Lambda_\pi \cap \Lambda_L$.

Каждая грань неприводимого комплекса M содержит хотя бы одну *собственную вершину* $\tilde{x}$, не принадлежащую другим граням комплекса. Такую грань обозначим через $I_{M,\tilde{x}}$.

Для множества вершин $Q \subseteq B^n$ подмножество вершин $X \subseteq Q$ называется *интервально независимым*, если любая допустимая грань для множества Q содержит не более одной вершины множества X.

Подмножество вершин называется *протыкающим* для комплекса граней, если в каждой грани комплекса содержится хотя бы одна вершина подмножества.

Утверждение. *Пусть $\mathcal{B}_M$ — подмножество собственных вершин для граней неприводимого комплекса M и определены условия:*

(i) $\mathcal{B}_M$ является интервально независимым и протыкающим для комплекса граней;

(ii) для каждой вершины $\tilde{x} \in \mathcal{B}_M$ ранг грани $I_{M,\tilde{x}}$ не больше ранга любой допустимой грани комплекса, содержащей $\tilde{x}$;

(iii) для каждой вершины $\tilde{x} \in \mathcal{B}_M$ грань $I_{M,\tilde{x}}$ изоморфна или

доминирует любую допустимую грань комплекса, содержащую $\tilde{x}$.

Тогда комплекс M *является кратчайшим, если выполнено условие* (i), *минимальным и кратчайшим, если выполнены условия* (i) *и* (ii), Λ_π*-минимальным, если выполнены условия* (i) *и* (iii).

Λ_π*-минимальные комплексы при выполнении условий* (i) *и* (iii) *обладают свойством суммируемости для компонент связности.*

Следствие. *Любой* L*-минимальный комплекс симметрической функции является* Λ_π*-минимальным и*

$$\log \mu_{\cap\Lambda_\pi}(n) \gtrsim \log M_{\cap\Lambda_\pi}(n) \gtrsim \sqrt{2/\pi}\,\sqrt{n}\,2^n.$$

2. Вероятностные методы получения оценок

Существенного улучшения нижних оценок $\tau(n)$ и $\mu(n)$ удалось добиться после отказа от построения и исследования свойств конкретных функций и переходу к *построению множеств тупиковых и минимальных комплексов граней* в кубе B^n.

Из известных нижних оценок следует, что $\log|P_n| = 2^n$ является величиной $o(\log\tau(n))$ и $o(\log\mu(n))$, соответственно, из соотношений

$$T(n)/|P_n| \le \tau(n) \le T(n),\ M(n)/|P_n| \le \mu(n) \le M(n)$$

следует, что $\log\tau(n) \sim \log T(n)$ и $\log\mu(n) \sim \log M(n)$ при $n \to \infty$. Это означает эквивалентность с точностью до асимптотики логарифма задач (i) о максимальном числе тупиковых или минимальных комплексов булевой функции n переменных и (ii) о числе тупиковых или минимальных комплексов в кубе B^n.

Отметим, что мощность множества комплексов различных граней в кубе B^n не превосходит $2^{o(n2^n)}$, если в комплексах множества: либо число граней равно $o(2^n)$, либо число граней равно $\Theta(2^n)$ и все грани размерности $o(n)$. Следовательно, существование тупиковых, кратчайших или минимальных комплексов граней, которые содержат порядка 2^n граней размерности порядка n в единичном кубе B^n, является *необходимым условием* для получения соответствующей нижней оценки по порядку логарифма равной $n2^n$.

Метод построения тупиковых комплексов граней [12]. Идея метода основана на обобщении доказательства существования такого тупикового комплекса T пояса $S = S^n_{m-k,m}$, что $l(T) \sim |S|$ при $k \le \Theta(\log\log n/\log\log\log n)$ и $\frac{1}{4}n \le m-k < m \le \frac{3}{4}n$ [13].

Грань минимальной размерности единичного куба, которая содержит вершины $\tilde{x}$ и $\tilde{y}$, обозначим через $I(\tilde{x},\tilde{y})$.

Для множеств $A \subset S \subset B^n$ и вершин, содержащихся в гранях допустимых для S и пересекающихся с A, определим два множества.

Множество (A,S)-внутренних вершин $W(A,S)$ содержит вершины $\tilde{x} \in S$, для которых существует такая вершина $\tilde{\alpha} \in A$, что грань $I(\tilde{x},\tilde{\alpha})$ является *допустимой, но не максимальной* для множества S.

Множество (A,S)-граничных вершин $G(A,S)$ содержит вершины $\tilde{x} \in S$, для которых грань $I(\tilde{\alpha},\tilde{x})$ для любой вершины $\tilde{\alpha} \in A$ является *либо максимальной, либо недопустимой* для множества S.

Обозначим через $\mathcal{T}(S,A)$ множество комплексов граней, в которых для каждой (A,S)-граничной вершины $\tilde{x}$ в комплекс включается грань $I(\tilde{x},\tilde{\alpha})$ для такой одной вершины $\tilde{\alpha} \in A$, что $I(\tilde{x},\tilde{\alpha})$ является максимальной гранью для S.

Лемма. *Для множеств вершин $A \subset S \subset B^n$ любой комплекс граней $T \in \mathcal{T}(S,A)$ является тупиковым и для грани $I(\tilde{x},\tilde{\alpha}) \in T$ вершина $\tilde{x} \in G(A,S)$ является собственной.*

Теорема. *Существует $A_\lambda \subset S^n_{m-k,m}$ и тупиковый комплекс граней $T \in \mathcal{T}\left(S^n_{m-k,m}, A_\lambda\right)$ такой, что*

$$\left|S^n_{m-k,m}\right|\left(1-e^{-\lambda}\right)\left(1-\frac{\lambda k}{m-2k}\right) \lesssim l(T) < \left|S^n_{m-k,m}\right|,$$

где $\varepsilon n \le m \le \frac{n}{2}$, $k \le \frac{m}{2}(1-\varepsilon)$, $\varepsilon < \lambda < \min\left\{\frac{m}{k} - 2 - \varepsilon, o(n)\right\}$.

Множество тупиковых комплексов в поясе $S^n_{m-k,m}$ образуется из пучков граней, которые получаются сечением по слою $m-k$ граней тупикового комплекса из пояса $S^n_{m-k_0,m}$, имеющих собственные вершины в поясе $S^n_{m-p,m}$, где $p < k < k_0$.

Метод построения ядровых комплексов граней [14]. Для множества вершин $A \subset B^n$ определим множество простых k-граничных вершин $G_k(A)$, которое содержит такие вершины $\tilde{x} \in B^n$, что $\rho(\tilde{\alpha},\tilde{x}) \ge k$ для любой вершины $\tilde{\alpha} \in A$ и существует единственная вершина $\tilde{\alpha} \in A$, обозначаемая через $\tilde{\varphi}_{A,k}(\tilde{x})$, для которой $\rho(\tilde{\alpha},\tilde{x}) = k$.

Будем говорить, что множество состоит из *изолированных* вершин, если в нем нет соседних вершин.

Лемма. *Для множества вершин $A \subset B^n$ и подмножества изолированных простых k-граничных вершин $G \subset G_k(A)$ ядровым является комплекс граней, в котором для каждой вершины $\tilde{x} \in G$ в комплекс включается грань $I(\tilde{x},\tilde{\alpha})$ для вершины $\tilde{\alpha} = \tilde{\varphi}_{A,k}(\tilde{x}) \in A$.*

Вершина $\tilde{x}$ является собственной для грани $I(\tilde{x},\tilde{\alpha})$ в таком ядровом комплексе.

Задача о максимальном числе k-мерных граней в ядровом комплексе сводится к доказательству существования множества вершин $A \subset B^n$, для которого число изолированных простых k-граничных вершин сравнимо с мощностью куба. Для этого используется вероятностный метод, основанный на случайном выборе вершин множества A и оптимизацией при подборе параметров для двух способов получения изолированных вершин.

Теорема. *Для $1 \le k < \frac{n}{2} - \eta(n)$, где $\eta(n)/\sqrt{n} \to \infty$ при $n \to \infty$, существуют множество $A \subset B^n$ и ядровой комплекс k-мерных граней M, построенный по множеству изолированных простых k-граничных вершин $G \subset G_k(A)$, для которого*

$$l(M) \gtrsim \frac{2^{n-1}}{e}\varphi_c\left(\frac{k}{n}\right),\ \varphi_c(x) = \frac{1-2x}{1-x}\max\left\{1, \frac{2x}{1-x}\right\}.$$

Множество Λ_π-минимальных комплексов граней образуется из пучков граней, которые получаются сечением по слоям $r - \left\lfloor \frac{k}{2} \right\rfloor$ и $r + \left\lceil \frac{k}{2} \right\rceil$ граней ядрового комплекса k_0-мерных граней, имеющих собственные вершины в поясе $S^n_{r-p,r+p}$, где $2p < k < k_0$ и $r = \left\lfloor \frac{n}{2} \right\rfloor$.

Подбор параметров и вычисление констант в нижних оценках выполняется методом нелинейного программирования.

3. Оценки максимальных значений

Тупиковые комплексы граней [12]. Доказано существование тупиковых комплексов k-мерных граней с числом граней порядка 2^n при $k \le \frac{n}{2}(1-\varepsilon)$ и асимптотически равном 2^n при $k = o(n)$.

Для числа тупиковых комплексов граней в кубе B^n и для максимального числа тупиковых комплексов граней функции n переменных получен порядок логарифма равный $n2^n$ с константой в нижней оценке, которая больше $1.355 \cdot 2^{-5}$. Нижние оценки достигаются на множестве тупиковых комплексов граней $\mathcal{T}^n_{m-k,m}$ и множестве функций $\mathcal{F}^n_{m-k,m}$, которые содержат только максимальные k-мерные грани пояса $S^n_{m-k,m}$.

Ядровые и кратчайшие комплексы граней [14]. Доказано существование ядровых комплексов k-мерных граней с числом граней порядка 2^n при $1 \le k \le \frac{n}{2}(1-\varepsilon)$.

Число кратчайших комплексов k-мерных граней совпадает по порядку логарифма с общим числом комплексов, которые состоят из не более 2^{n-1} различных k-мерных граней при $1 \le k \le \frac{n}{2}(1-\varepsilon)$.

Для числа кратчайших комплексов граней в кубе B^n и для максимального числа кратчайших комплексов граней функции n переменных получен порядок логарифма равный $n2^n$ с константой в нижней оценке, которая больше $1.0614 \cdot 2^{-5}$.

Минимальные комплексы граней [15]. Для комплексов граней размерности не более k число Λ_π-минимальных комплексов и число комплексов из не более 2^{n-1} различных граней совпадают по порядку логарифма при $k \leq \frac{n}{2}(1-\varepsilon)$.

Для числа Λ_π-минимальных комплексов граней в кубе B^n и для максимального числа Λ_π-минимальных комплексов граней функции n переменных получен порядок логарифма равный $n2^n$ с константой в нижней оценке, которая больше $0.5307 \cdot 2^{-5}$.

Мощность множества функций, для которых число Λ_π-минимальных комплексов равно по порядку логарифма $n2^n$, совпадает по порядку логарифма с числом функций n переменных.

Отношение числа тупиковых и минимальных комплексов граней [16]. Для получения нижних оценок используются свойства экстремальных функций из множества $\mathcal{F}^n_{m-k,m}$.

Максимальное значение по порядку логарифма равно $n2^n$:

(i) для отношения числа тупиковых и минимальных комплексов граней функции относительно всех мер сложности класса $\Lambda_\pi \cap \tilde{\Lambda}_l$;

(ii) для числа тупиковых комплексов граней функции при единственном минимальном комплексе граней функции относительно всех мер сложности класса $\Lambda_\pi \cap \tilde{\Lambda}_L$.

Мощности множеств функций по порядку логарифма равны 2^n, т. е. числу функций n переменных, для которых значение по порядку логарифма равно $n2^n$ для одного из параметров:

(i) число тупиковых комплексов,

(ii) отношение числа тупиковых и минимальных комплексов относительно всех мер сложности класса $\Lambda_\pi \cap \tilde{\Lambda}_l$,

(iii) число тупиковых комплексов при единственном минимальном комплексе относительно всех мер сложности класса $\Lambda_\pi \cap \tilde{\Lambda}_L$.

Для получения нижних оценок используются свойства экстремальных функций из множества $\mathcal{F}^n_{m-k,m}$ с большим числом тупиковых комплексов и методы доказательства минимальности комплексов граней для мер сложности из классов $\tilde{\Lambda}_l$ и $\tilde{\Lambda}_L$ (являются расширением классов Λ_l и Λ_L за счет исключения требования «строгой монотонности» для граней, содержащих вершину $\tilde{0}$ или $\tilde{1}$).

4. Оценки типичных значений [17]

Обозначим через $\tilde{P}_n$ подмножество почти всех функций из P_n, которые при $k_0 = \lceil \log n \rceil$, $k_1 = \lceil \log\log n + \log\log\log n \rceil$ и $k_2 = \lfloor \log\log n \rfloor$ обладают свойствами 1–5:

1. Нет допустимых граней размерности более k_0 [18].

2. Число допустимых граней $g(f) = 2^n n^{\log\log n(1+o(1))}$, почти все допустимые грани функции имеют размерность k_2 или k_2+1, $|N_f| \sim 2^{n-1}$ и допустимые грани функции размерности больше k_1 содержат не более $2^n n^{-\log\log n(1-o(1))}$ вершин функции [19].

3. Число максимальных граней $s(f) = 2^n n^{\log\log n(1+o(1))}$, почти все максимальные грани функции имеют размерность k_2 или k_2+1 и почти все k-мерные допустимые грани функции являются максимальными при $k_2 < k \le k_0$ [20].

4. $l_L(f) \sim l(f)$ и $L_l(f) \sim L(f) \sim n\, l(f)$, т. е. длина минимальных и кратчайших комплексов граней, сложность минимальных и кратчайших комплексов граней — асимптотически равны [21].

5. $l(f) \sim \bar{l}(n)$, где $\bar{l}(n)$ — среднее значение длины кратчайшего комплекса граней функции [22, стр. 94].

Оценкам длины кратчайших ДНФ для почти всех функций были посвящены работы В. В. Глаголева, Р. Г. Нигматуллина, А. А. Сапоженко, А. Д. Коршунова, С. Е. Кузнецова, А. Е. Андреева, Н. Пиппенджера. Наилучшие известные результаты следующие:

$$l(f) \sim \bar{l}(n) = \bar{c}_n 2^n / \log n \log\log n,$$

где $1 \le \bar{c}_n$ [23] и $\bar{c}_n \le 1.5$ [24] или $\bar{c}_n \le \omega(n)$ [25], при этом функция $\omega(n)$ зависит от *дробной части* $\log\log n + \log\log\log n$ и колеблется между $1.38826\ldots$ и $1.54169\ldots$ в зависимости от n.

Мощностная верхняя оценка $\mu_{\mathcal{L}}(f)$ при $l_{\mathcal{L}}(f) < g(f)/2$ имеет вид

$$\log \mu_{\mathcal{L}}(f) \le \log \sum\nolimits_{i=l(f)}^{l_{\mathcal{L}}(f)} \binom{g(f)}{i} < l_{\mathcal{L}}(f) \log \frac{e\, g(f)}{l_{\mathcal{L}}(f)}.$$

Следовательно, для кратчайших и минимальных комплексов почти всех булевых функций выполняется $\log \mu(f) \lesssim \bar{c}_n 2^n$.

Идея улучшения верхней оценки для кратчайших комплексов граней основана на сравнении этой оценки с мощностью множества кратчайших комплексов граней функций из множества $\tilde{P}_n$. Это множество, которое обозначим через $\mathcal{M}_l^n$, содержит комплексы граней, состоящие из не более $m \sim \bar{l}(n)$ различных граней размерности не

более $k \sim \log\log n$ и $o\left(\frac{2^n}{n}\right)$ граней большей размерности, но не более $k_0 = \lceil \log n \rceil$. Оказывается, что общее число комплексов граней с такими характеристиками с точностью до асимптотики логарифма не превосходит $\bar{c}_n 2^n$. Тогда, в силу неравенства Маркова, число кратчайших комплексов граней функций из $\tilde{P}_n$ не может по порядку логарифма превосходить среднего значения, т. е. $2^{-2^n} |\mathcal{M}_l^n|$. Поэтому с точностью до асимптотики логарифма возможно улучшение верхней оценки до величины $\log |\mathcal{M}_l^n| - 2^n \lesssim (\bar{c}_n - 1)\, 2^n$, что существенно меньше числа функций n переменных.

Теорема. *Если $l_{\mathcal{L}}(f) \sim l(f)$ для почти всех функций из P_n, то*

$$\log \mu_{\mathcal{L}}(f) \lesssim (\bar{c}_n - 1)\, 2^n$$

при $n \to \infty$, где $\bar{c}_n$ определяется из соотношения для среднего значения длины кратчайшего комплекса граней типичной булевой функции $\bar{l}(n) = \bar{c}_n 2^n / \log n \log\log n$.

Тогда для почти всех функций $\log \mu_l(f) \lesssim 2^{n-1}$ и $\log \mu_{\mathcal{L}}(f) \lesssim 2^{n-1}$, если $l_{\mathcal{L}}(f) \sim l(f)$, так как $\bar{c}_n \leq 1.5$ [24].

При определенных предположениях для аддитивных мер сложности асимптотически совпадают длины $\mathcal{L}$-минимальных и кратчайших комплексов для почти всех функций.

Теорема. *Для почти всех функций $l_{\mathcal{L}}(f) \sim l(f)$ при $n \to \infty$ для аддитивной меры сложности $\mathcal{L} \not\equiv 0$, если в единичном кубе B^n:*

(i) максимальная $\mathcal{L}$-сложность граней ограничена полиномом от n,

(ii) грани размерности не более $k_0 = \lceil \log n \rceil$ и содержащиеся в средних слоях куба ширины $\Theta(\sqrt{n} \log n)$ имеют асимптотически одинаковую $\mathcal{L}$-сложность.

Следствие. *Если для аддитивной меры сложности функционал имеет вид $L_q(I) = q(L_0(I), L_1(I))$, где $q(x, y)$ — полином двух переменных и I — грань куба, то для почти всех функций $l_{L_q}(f) \sim l(f)$ и $\log \mu_{L_q}(f) \lesssim (\bar{c}_n - 1)\, 2^n$.*

5. О минимизации одного множества булевых функций [26]

Обозначим через $\mathcal{F}_{n,\mathcal{L}}$ множество функций n переменных, которые для аддитивной меры сложности $\mathcal{L}$ обладают следующими свойствами: (i) множество единичных вершин функции является одной связной компонентой, (ii) множества тупиковых кратчайших и минимальных комплексов граней не пересекаются и (iii) длина кратчайших комплексов $l(f)$ равна мощности максимального интервально независимого множества вершин функции $m(f)$.

Для функции $f \in \mathcal{F}_{n,\mathcal{L}}$ в любом $\mathcal{L}$-минимальном комплексе граней нельзя выбрать интервально независимое множество собственных вершин из различных граней, так как он не является кратчайшим, т. е. число граней в комплексе больше $l(f) = m(f)$. Соответственно, для таких функций не применимы независимая минимизация для компонент связности и достаточные условия минимальности, основанные на интервально независимых множествах, позволяющие при минимизации сократить трудоемкость и исключить перебор всех минимальных комплексов граней. Задача заключается в получении нижних оценок $|\mathcal{F}_{n,\mathcal{L}}|$ и $\mu(\mathcal{F}_{n,\mathcal{L}})$ — мощности и максимального числа $\mathcal{L}$-минимальных комплексов граней для функций множества $\mathcal{F}_{n,\mathcal{L}}$.

Для построения функций множества $\mathcal{F}_{n,\mathcal{L}}$ выполняется преобразование функции s переменных в функцию n переменных, для которой можно описать все тупиковые комплексы граней и получить для них сравнительные оценки сложности. При преобразовании:

(i) каждая максимальная грань исходной функции преобразуется в пучок изоморфных максимальных граней функции $n-2$ переменных;

(ii) добавлением одномерных ядровых граней в двух новых измерениях, которые содержат все вершины функции $n-2$ переменных за исключением вершин исходной функции s переменных в фиксированной грани.

При специальном выборе параметров и выполнении определенных условий для $\mathcal{L}$-сложности граней различного ранга получаются функции из множества $\mathcal{F}_{n,\mathcal{L}}$. У такой функции будет единственный тупиковый кратчайший комплекс граней, $\mathcal{L}$-сложность которого больше, чем остальных тупиковых и, в том числе, $\mathcal{L}$-минимальных комплексов граней.

Теорема. *Если для функции $f \in P_s$ и параметров s, t и булева вектора $\tilde{\alpha}_{s+1,n} = (\alpha_{s+1}, \ldots, \alpha_n)$ для аддитивной меры сложности $\mathcal{L}$ выполняется: $l(f) > 1$ и $l_T^{\max}(f)\,\mathcal{L}_{s+t+2}^{\max} < \mathcal{L}_{n-s}^{\max} = \mathcal{L}\left(B_{s+1,\ldots,n}^{n,\alpha_{s+1},\ldots,\alpha_n}\right)$, то*

$$\log \mu(\mathcal{F}_{n,\mathcal{L}}) \geq l(f) \log |\mathcal{I}|\,,\ \log |\mathcal{F}_{n,\mathcal{L}}| \geq k(f)\,(|\mathcal{I}| - 1)\,,$$

где $\mathcal{L}_r^{\max}$ — максимальная $\mathcal{L}$-сложность грани ранга r; $k(f)$, $l(f)$, $l_T^{\max}(f)$ — число компонент связности, длина кратчайшего и максимальная длина тупикового комплексов граней функции f; $|\mathcal{I}|$ — максимальная мощность пучка изоморфных граней $\mathcal{I}$, которые имеют ранг t и содержат вершину $(\alpha_{s+1}, \ldots, \alpha_{n-2})$ в кубе B^{n-s-2}.

Аддитивная мера сложности $\mathcal{L}$ называется *линейной*, если $\mathcal{L}(I) = aL_0(I) + bL_1(I)$ для любой грани I, где $a, b \geq 0$ и $\max\{a, b\} > 0$.

Аддитивная мера сложности $\mathcal{L}$ называется *полиномиальной*, если $\mathcal{L}(I) = q(L_0(I), L_1(I))$ для любой грани I, где $q(x, y)$ — многочлен не ниже 2-ой степени с положительными коэффициентами.

Теорема. *Для аддитивной линейной меры сложности $\mathcal{L}$ выполняются соотношения:*

$$\log \mu(\mathcal{F}_{n,\mathcal{L}}) \gtrsim n \log n,\ \log |\mathcal{F}_{n,\mathcal{L}}| \geq \Theta\left(2^n/\sqrt{n}\right).$$

Для аддитивной меры полиномиальной сложности $\mathcal{L}$ выполняются соотношения:

$$\log \mu(\mathcal{F}_{n,\mathcal{L}}) \geq (\mathcal{L}_n^{\max})^{1-o(1)} \log n,\ \log |\mathcal{F}_{n,\mathcal{L}}| \geq \Theta\left(2^n/n^{3/2}\right).$$

Заключение

Существование мощных классов функций с экстремальными значениями характеристик, которые зависят от числа минимальных комплексов граней функции, доказано для классов мер сложности. Этот результат позволяет сделать вывод, что проблемы минимизации экстремальных булевых функций определяются свойствами области, на которой минимизируется функционал меры сложности, а не его свойствами.

Существование гипотезы о достижимости значений $\tau(n)$ и $\mu(n)$ на симметрических функциях объясняется справедливостью такого утверждения при небольших n. Соответствующие нижние оценки, которые по порядку логарифма равны $n2^n$ с константами $1.35 \cdot 2^{-5}$ и $0.53 \cdot 2^{-5}$, превосходят нижние оценки для симметрических функций, которые по порядку логарифма асимптотически равны $\sqrt{n}2^n$ с константой $\sqrt{2/\pi}$, только при $n > 256$.

Минимальные комплексы граней экстремальных функций содержат порядка 2^n граней, собственные вершины различных граней представляют независимое множество и каждая грань может быть выбрана из пучка мощности $2^{\Theta(n)}$. Построение таких функций возможно при числе переменных больше 30 и для их минимизации практически не применимы точные алгоритмы, а для приближенных алгоритмов представляются необоснованными используемые эвристики.

Многие открытые проблемы в задаче минимизации булевых функций связаны с невозможностью универсальных и эффективных методов обоснования минимальности. Например, представляется правдоподобным, что доля булевых функций, имеющих единственный минимальный или минимальный и не кратчайший комплекс граней, стремится к 0 с ростом n. Справедливость таких предположений означает, что у почти всех функций должно быть хотя бы два минимальных и все минимальные комплексы граней являются кратчайшими.

Работа выполнена при финансовой поддержке РФФИ (проект 16-01-00593а).

Список литературы

1. Яблонский С. В. Функциональные построения в k-значной логике // Тр. МИАН СССР. — 1958. — Т. 51. — С. 5–142.

2. Еремеев А. В., Заозерская Л. А., Колоколов А. А. Задача о покрытии: сложность, алгоритмы, экспериментальные исследования // Дискретный анализ и исследование операций. Серия 2. — 2000. — Т. 7, № 2. — С. 22–46.

3. Леонтьев В. К. Дискретная оптимизация // Журнал вычислительной математики и математической физики. — 2007. 47, № 2. — С. 338–352.

4. Coudert O., Sasao T. Two-level logic minimization // Logic synthesis and verification. — Norwell, MA, USA: Kluwer Academic Publishers. — 2002. — P. 1–27.

5. Забиняко Г. И. Реализация алгоритмов решения задачи о покрытии множеств и анализ их эффективности // Вычислительные технологии. — 2007. — Т. 12, № 6. — С. 50–58.

6. Журавлёв Ю. И. Теоретико-множественные методы в алгебре логики // Проблемы кибернетики. — 1962. — № 8. — С. 5–44.

7. Cook S. A. An overview of computational complexity // Communications of the ACM. — 1983. — Vol. 26, no. 6. — P. 401–408.

8. Umans C., Villa T., Sangiovanni-Vincentelli A. L. Complexity of Two-Level Logic Minimization // IEEE Trans. on CAD of Integrated Circuits and Systems. — 2006. — Vol. 25, no. 7. — P. 1230–1246.

9. Васильев Ю. Л., Глаголев В. В. Метрические свойства дизъюнктивных нормальных форм // Дискретная математика и математические вопросы кибернетики. — М.: Наука, 1974. — Т. 1. — С. 99–148.

10. Чухров И. П. О мерах сложности комплексов граней в единичном кубе // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 6. — С. 77–94.

11. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

12. Чухров И. П. О тупиковых комплексах граней в единичном кубе // Дискретная математика. — 2011. — Т. 23, № 1. — С. 132–158.

13. Глаголев В. В. О длине тупиковой дизъюнктивной нормальной формы // Математические заметки. — 1967. — Т. 2, № 6. — С. 665–672.

14. Чухров И. П. О ядровых и кратчайших комплексах граней в единичном кубе // Дискретный анализ и исследование операций. —

2011. — Т. 18, № 2. — С. 75–94.

15. Чухров И. П. О соотношении тупиковых и минимальных комплексов граней в единичном кубе // Дискретная математика. — 2012. — Т. 24, № 2. — С. 46–74.

16. Чухров И. П. О минимальных комплексах граней в единичном кубе // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 3. — С. 79–99.

17. Чухров И. П. Минимальные комплексы граней случайной булевой функции // Дискретный анализ и исследование операций. — 2014. — Т. 21, № 5. — С. 76–94.

18. Журавлёв Ю. И. Оценка для числа тупиковых д.н.ф. функций алгебры логики // Сибирский математический журнал. — 1962. — Т. 3, № 5. — С. 802–804.

19. Глаголев В. В. Некоторые оценки дизъюнктивных нормальных форм функций алгебры логики // Проблемы кибернетики. — 1967. — Т. 19. — С. 75–94.

20. Сапоженко А. А. Дизъюнктивные нормальные формы. — М.: Издательство МГУ, 1975.

21. Коршунов А. Д. Сравнение сложности длиннейших и кратчайших д.н.ф. и нижняя оценка числа тупиковых д.н.ф. для почти всех булевых функций // Кибернетика. — 1969. — Т. 4. — С. 1–11.

22. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991.

23. Кузнецов С. Е. О нижней оценке длины кратчайшей д.н.ф. почти всех булевых функций // Вероятностные методы и кибернетика. — Казань: Изд-во Казанского ун-та, 1983. — № 19. — С. 44–47.

24. Андреев А. Е. Об одной модификации градиентного алгоритма // Вестник МГУ. Мат. Мех. — 1985. — № 3. — С. 29–35.

25. Pippenger N. The shortest disjunctive normal form of a random Boolean function // Random Structures & Algorithms. — 2003. — Vol. 22, no. 2. — P. 161–186.

26. Чухров И. П. О задаче минимизации для одного множества булевых функций // Дискретный анализ и исследование операций. — 2015. — Т. 22, № 3. — С. 75–97.

ТРЕЙДЫ В КОМБИНАТОРНЫХ КОНФИГУРАЦИЯХ

Д. С. Кротов (Новосибирск)

Трейды отражают возможную разницу между двумя комбинаторными объектами (конфигурациями) одного и того же типа (системами Штейнера или блок-схемами с другими параметрами, подпространственными аналогами блок-схем, латинскими квадратами или латинскими гиперкубами, совершенными кодами, МДР кодами, MRD (maximum rank distance) кодами, ортогональными массивами и т.д.). Если C и C' — две конфигурации с одинаковыми параметрами (например, системы троек Штейнера $S(2,3,13)$), то пара $(C\backslash C', C'\backslash C)$ является битрейдом, а $C\backslash C'$ и $C'\backslash C$ — трейдами. (Следует отметить, что в литературе распространена также альтернативная терминология, когда пара называется трейдом, а сами множества — ногами, трейд-партнерами или др.) Однако, трейды обычно можно определить независимо от «полных» конфигураций данного типа, они не обязательно вложимы в такие конфигурации и даже могут существовать при параметрах, при которых полные конфигурации не существуют. Таким образом, изучение трейдов можно рассматривать как самостоятельное направление исследований, результаты которого находят применение в построении конфигураций с соответствующими параметрами. Если (T_0, T_1) — битрейд (определяемый в соответствии с параметрами некоторой конфигурации), и T_0 является подмножеством конфигурации C, то $T_1 \cup C\backslash T_0$ является конфигурацией с теми же параметрами. Эта замена называется свитчингом (трейд T_0 называют также свитинговой компонентой конфигурации C) и используется как в теоретических, так и в вычислительных [12] построениях. При таком подходе (то есть, когда трейды могут быть определены независимо), если конфигурация C содержит непересекающиеся трейды, то свитчинг может быть применен к каждому из трейдов независимо, таким образом из данной конфигурации можно получить 2^N других конфигураций с теми же параметрами, где N — число попарно непересекающихся трейдов в C. Во многих случаях, как правило, в случаях, когда растет размерность дискретного пространства, в котором рассматриваются конфигурации, эта оценка дает неплохое представление о росте числа различных конфигураций при росте размерности пространства.

В настоящем обзоре мы рассмотрим ограниченный класс комбинаторных конфигураций и соответствующих трейдов, который тем не менее охватывает несколько хорошо известных классов объектов, каждому из которых уделяется отдельное внимание в комбинаторике и посвящено немалое количество литературы. Мы рассмотрим

несколько общих утверждений из теории битрейдов, после чего перейдем к рассмотрению примеров конкретных классов конфигураций, упомянув, в частности, некоторые свежие результаты, связанные с оценкой числа объектов при помощи свитчинга трейдов.

1. Определения

Под графом будем понимать неориентированный граф без кратных ребер и петель. *Расстояние* $d(x, y)$ между двумя вершинами x, y в связном графе — это минимальная длина цепи с концами в данных вершинах. *Диаметр* $\mathrm{diam}(\Gamma)$ связного графа Γ — максимальное расстояние между двумя вершинами графа. *Клика* в графе — любое множество попарно смежных вершин. *Независимое множество* вершин графа — любое множество попарно несмежных вершин графа.

Дистанционно регулярный граф — такой связный граф, что для любых двух вершин v и w число $a_{i,j,k}$ вершин с расстоянием j от v и расстоянием k от w зависят только от j, k и расстояния $i = d(v, w)$ между v и w (и не зависят от выбора v и w). Коэффициенты $a_{i,j,k}$ называются *числами пересечений* дистанционно регулярного графа.

Характеристическая функция χ_C множества C вершин графа — действительнозначная функция, равная 1 на вершинах из C и 0 на всех остальных вершинах графа.

Весовым распределением действительнозначной функции f на вершинах связного графа Γ относительно вершины x графа назовем набор $\left(f(y), \sum_{y\in\Gamma_1(x)} f(y),\ \ldots,\ \sum_{y\in\Gamma_{\mathrm{diam}(\Gamma)}(x)} f(y)\right)$, где $\Gamma_i(x)$ — множество вершин графа Γ на расстоянии i от x.

Собственная функция графа $\Gamma = (V, E)$ — функция $f : V \to \mathbb{R}$, не равная тождественно нулю и удовлетворяющая соотношению $\sum_{y\in\Gamma_1(x)} f(y) = \theta f(x)$ для любой вершины x из V и некоторой константы θ, которая называется *собственным значением* графа Γ.

Дельсартова клика — клика мощности $1 - r/\theta$ в дистанционно регулярном графе, где r — степень, а θ — минимальное собственное значение графа. Известно [5], что в дистанционно регулярном графе не может быть клик большей мощности.

(r, s)-*Пара* — пара (Γ, S), где Γ — регулярный граф степени r, а S — такой непустой набор клик мощности $s+1$ графа Γ, что каждое ребро содержится в одном и том же (не зависящем от выбора ребра) числе клик из S. *Дельсартовой* (r, s)-пара (Γ, S) называется в том случае, когда граф Γ дистанционно регулярный и клики из S дельсартовы (то есть $-r/s$ — минимальное собственное число графа).

Клик-дизайн и клик-битрейд. Пусть (Γ, S) есть (r, s)-пара. Множество вершин C графа Γ назовем S-*дизайном*, или *клик-дизайном*

если оно пересекается с каждой кликой из S ровно в одной точке. Пару (T_0, T_1) непересекающихся непустых независимых множеств вершин графа Γ назовем *S-битрейдом*, или *клик-битрейдом*, если для каждой клики K из S верно $|K \cap T_0| = |K \cap T_1|$. Множество вершин графа назовем *S-трейдом*, *клик-трейдом*, или просто *трейдом*, если оно в паре с некоторым другим множеством образует S-битрейд. Очевидно, что для любых двух различных S-дизайнов C, C' пара $(C \backslash C', C' \backslash C)$ является S-битрейдом.

Двойным подсчетом числа пар (x, K): $K \in S$, $x \in M \cap K$ легко установить, что любое независимое множество M мощности $|V(\Gamma)|/(s+1)$ является S-дизайном для любой (r, s)-пары (Γ, S). Поэтому понятие клик-дизайна не зависит от выбора системы клик S, образующих с графом (r, s)-пару, важно лишь ее существование (примерами графов, для которых такая система может быть выбрана не единственным образом, являются полный $(s+1)$-дольный граф с равными долями, графы Джонсона $J(2k, k)$ и Грассмана $J_q(2k, k)$). Как следует из теоремы 1 в следующем разделе, то же верно и для клик-битрейдов.

2. Некоторые общие факты о битрейдах

Теорема 1 (характеристические свойства битрейда [8]). *Пусть (Γ, S) является (r, s) парой. Пусть $T = (T_0, T_1)$ — пара непустых непересекающихся независимых множеств вершин графа Γ. Следующие утверждения эквивалентны:*

(a) *T является S-битрейдом;*

(b) *функция $f^T(x) = \chi_{T_0}(x) - \chi_{T_1}(x)$ является собственной с собственным числом $\theta = -r/s$;*

(c) *двудольный подграф Γ^T графа Γ, индуцированный множеством вершин $T_0 \cup T_1$, является регулярным степени $-\theta = r/s$ (поскольку T_0 и T_1 — независимые множества, этот подграф двудольный).*

Кроме того, если граф Γ является дистанционно регулярным, то из (a)–(c) *следует, что пара (Γ, S) является дельсартовой, а собственное число $-r/s$ является наименьшим для графа Γ.*

Для оценки минимальной мощности битрейда в дистанционно регулярном графе полезен следующий факт.

Лемма 1. *Весовое распределение собственной функции f дистанционно регулярного графа Γ относительно вершины x равно $(f(x)W^i_{\Gamma,\theta})_{i=0}^{\mathrm{diam}(\Gamma)}$, где коэффициенты $W^i_{\Gamma,\theta}$ вычисляются через числа пересечений графа и собственное число θ, соответствующее f.*

Следствие 1 (граница весового распределения). *Собственная функция f дистанционно регулярного графа с собственным значением θ имеет не меньше чем $\sum_{i=0}^{\mathrm{diam}(\Gamma)} |W^i_{\Gamma,\theta}|$ ненулей.*

Теорема 2 (Характеристические свойства минимального битрейда [8]). *Пусть верны предположения и обозначения теоремы 1 и граф Γ является дистанционно регулярным. Следующие утверждения эквивалентны:*

(a) *T — минимальный, достигающий границы весового распределения, клик-битрейд;*

(b) *f^T — собственная функция графа Γ с собственным значением $-r/s$ и числом ненулей $\sum_{i=0}^{\mathrm{diam}(\Gamma)} |W^i_{\Gamma,-r/s}|$;*

(c) *Γ^T — регулярный изометричный подграф степени r/s (изометричность означает, что расстояние между вершинами в графе Γ^T совпадает с расстоянием между данными вершинами в Γ).*

Кроме того, при выполнении (a)–(c) *подграф Γ^T является дистанционно регулярным.*

3. Известные классы клик-дизайнов и трейдов

3.1. Графы Хэмминга: латинские гиперкубы. Граф Хэмминга $H(n,q)$ — граф на множестве слов длины n в алфавите $\{0,\dots,q-1\}$. Два слова смежны, если они различаются ровно в одной позиции. Граф $H(n,2)$ также известен как *n-куб*.

Дельсартовой кликой в графе $H(n,q)$ является множество из q слов, различающихся между собой в одной позиции. Множество всех дельсартовых клик образует с графом $(n(q-1), q-1)$-пару.

Латинские гиперкубы (в случае $n=3$, *латинские квадраты*) порядка q можно определить как клик-дизайны в графах $H(n,q)$. Элементы латинского квадрата часто представляют упорядоченными в виде таблицы q на q, где слову (a,b,c) соответствует ячейка в a-й строке и b-м столбце таблицы, в которой записано значение c.

Клик-битрейды в графах Хэмминга известны как *латинские битрейды* [21], наиболее изученным является случай $n=3$ [2], соответствующий трейдам в латинских квадратах.

Минимальная мощность латинского битрейда — 2^n, подграф, индуцированный таким битрейдом — n-куб $H(n,2)$.

Теорема 3 [9, 22]. *Обозначим через $L(n,q)$ число латинских гиперкубов в $H(n+1,q)$. При фиксированном $q \geq 4$ имеем $L(n,q) \geq e^{e^{cn}}$, где c — константа, зависящая от q.*

Формулы для c в известных оценках [9, 22] разные для четных q, нечетных $q>5$ и для $q=5$. Во всех случаях доказательство со-

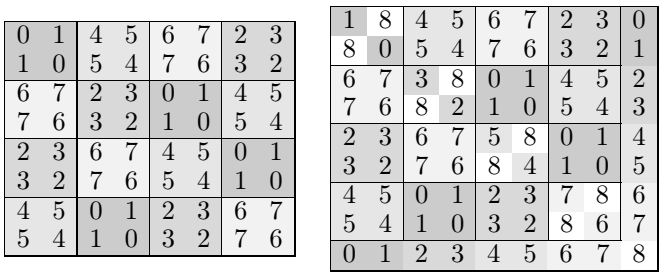


Рис. 1: Латинские квадраты, итерация которых дает латинские гиперкубы с большим числом независимых минимальных трейдов

стоит в построении латинского гиперкуба с экспоненциальным числом N попарно непересекающихся трейдов (например, для $q = 8$, 9 такие гиперкубы получаются многократной суперпозициех латинских квадратов, изображенных на Рис. 1), независимым свитчингом этих трейдов можно получить 2^N различных латинских гиперкубов.

В случае, когда мы рассматриваем асимптотику величины $L(n, q)$ при фиксированном n и растущем q, оценка 2^N не будет хорошей: она даст не более чем $e^{\text{const}\cdot q^n}$ различных объектов, поскольку число непересекающихся трейдов тривиально оценивается числом вершин в латинском гиперкубе. Оказывается, можно получить нижнюю оценку $e^{\text{const}\cdot q^n \ln q}$, если оценить число различных способов набрать систему непересекающихся трейдов в специально построенном латинском гиперкубе (при $q = 2^t$, в качестве такого латинского гиперкуба выбирается множество наборов $(x_1, \ldots, x_{n+1})$, задаваемое соотношением $x_{n+1} = x_1 + \ldots + x_n$ над группой $\mathbb{Z}_2^t$).

Теорема 4 [13]. *При фиксированном $n \geq 3$ логарифм числа $L(n, q)$ латинских гиперкубов в $H(n + 1, q)$ имеет порядок $q^n \ln q$.*

Верхняя оценка вида $L(n, q) \leq e^{\text{const}\cdot q^n \ln q}$ тривиальна, так как такой вид (при фиксированном n и растущем q) имеет число всевозможных функций из $\{0, \ldots, q-1\}^n$ в $\{0, \ldots, q-1\}$. Более сильная верхняя оценка $L(n, q) \leq \left((1 + o(1))\frac{q}{e^n}\right)^{q^n}$ получена в работе [11], авторы предполагают, что она асимптотически точна. Заметим, что для латинских квадратов ($n = 2$) утверждение теоремы также верно, но этот классический случай исследован при помощи других подходов, позволяющих получить более точные формулы.

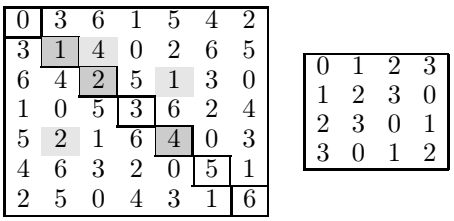


Рис. 2: Трансверсаль с минимальным трейдом, латинский квадрат без трансверсали

3.3. Графы латинских квадратов: трансверсали. Граф латинского квадрата строится на q^2 элементах латинского квадрата порядка $q \geq 2$, два различных элемента (x_1, x_2, x_3) и (y_1, y_2, y_3) соединены ребром, если они в одной строке (то есть $x_1 = y_1$), в одном столбце (то есть $x_2 = y_2$) или в них стоят одинаковые значения (то есть $x_3 = y_3$). Граф любого латинского квадрата порядка больше 2 является дистанционно регулярным диаметра 2 (такие графы известны также как сильно регулярные графы).

Множество из q элементов, содержащихся в одной строке, в одном столбце, или с одним и тем же значением, образуют дельсартову клику, набор всех $3q$ таких клик (отметим, что при $q = 3$ есть и другие дельсартовы клики) составляет с графом $(3(q-1), q-1)$-пару.

Трансверсаль латинского квадрата — клик-дизайн в соответствующем графе. Более традиционно, трансверсаль определяется как q ячеек латинского квадрата, пересекающихся с каждым столбцом, с каждой строкой и в которых встречаются все q различных значений. Заметим, что есть латинские квадраты без трансверсалей (рис. 2).

Минимальная мощность клик-битрейда в графах латинских квадратов — 6 (рис. 2), подграф, индуцированный таким битрейдом — полный двудольный граф $K_{3,3}$.

Теорема 5 [15]. *Обозначим через $R(q)$ максимальное, по всем квадратам порядка q, число трансверсалей в латинском квадрате. Тогда* $\ln R(q) \geq \frac{1}{6} q \ln q + O(q)$.

Учитывая, что число трансверсалей в латинском квадрате порядка q, очевидно, не превышает $q! = e^{O(q \ln q)}$, теорема 5 устанавливает порядок роста величины $\ln R(q) \sim q \ln q$. Доказательство теоремы основано на рассмотрении конкретной трансверсали конкретного латинского квадрата (при $q \equiv 1, 3 \bmod 6$ это главная диагональ

латинского квадрата, соответствующего произвольной системе троек Штейнера) и оценке числа способов набрать в этой трансверсали множество непересекающихся трейдов. Каждому такому способу соответствует трансверсаль, полученная свитчингом всех набранных трейдов. Заметим, что если мы зафиксируем набор трейдов данной трансверсали и рассмотрим независимые свитчинги каждого из них, то получится не больше чем $2^{q/3}$ различных трансверсалей, что по порядку логарифма всего лишь q.

К настоящему времени известны более точные оценки максимального числа трансверсалей в латинском квадрате. Верхняя оценка $R(q) \leq ((1+o(1))\frac{q}{e^2})^q$ была получена в [16] методом многомерных перманентов, в [4] доказано, что действительно $R(q) = ((1+o(1))\frac{q}{e^2})^q$ (нижняя оценка доказана вероятностными методами, то есть не предложено явной конструкции латинских квадратов, число трансверсалей которых имеет такой рост), в [3] показано, что такой рост числа трансверсалей имеет латинский квадрат нечетного порядка, соответствующий циклической группе.

3.4. Графы Джонсона: системы Штейнера. Граф Джонсона $J_q(v,k)$ строится на подмножествах мощности k данного множества V мощности v. Два k-подмножества смежны, если они имеют $k-1$ общих элементов. Далее считаем, что $2k \leq n$, поскольку графы $J(n,k)$ и $J(n,n-k)$ изоморфны.

Множество всех k-подмножеств, содержащих данные $k-1$ элементов, является дельсартовой кликой, набор всех $\binom{n}{k-1}$ таких клик (при $2k < v$ это все дельсартовы клики, а в случае $2k = v$ — только половина) составляет с графом $(k(v-k), v-k)$-пару.

Система Штейнера $S(k-1,k,v)$ — клик-дизайн в графе $J(v,k)$. Более традиционно, система Штейнера $S(t,k,v)$ определяется как t-$(v,k,1)$ схема, где t-(v,k,λ) — это пара (V,B) из конечного множества V и набора B его k-подмножеств (блоков) такая, что любое t-модмножество множества V входит ровно в λ блоков из B.

Битрейд Штейнера $T(k-1,k,v)$ — клик-битрейд в графе Джонсона (в литературе для этого случая чаще всего используется несколько другая терминология: пара (T_0,T_1) называется трейдом, а сами множества T_0, T_1 — ногами, или трейд-партнерами).

Известно, что минимальная мощность битрейда Штейнера $T(k-1,k,v)$ — 2^k, подграф, индуцированный таким битрейдом — k-куб $H(k,2)$. Самым известным примером трейда Штейнера является конфигурация Паша (Pasch configuration), см. рис. 3.

Давно известно, что порядок роста логарифма числа систем тро-

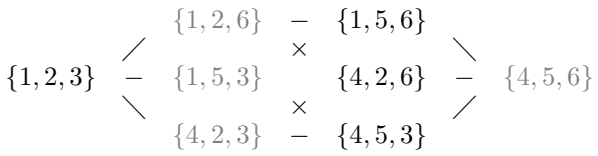


Рис. 3: 3-куб, порожденный битрейд-парой конфигураций Паша

ек Штейнера $S(2,3,v)$ — $v^2 \log v$. Более точно [18], [10],

$$\left(\frac{v}{e^2 3^{3/2}}\right)^{\frac{v^2}{6}} \leq |S(2,3,v)| \leq \left((1+o(1))\frac{v}{e^2}\right)^{\frac{v^2}{6}}.$$

Недавно [14] был установлен порядок роста логарифма числа систем четверок Штейнера.

Теорема 6 [14]. *Логарифм числа систем четверок Штейнера $S(3,4,v)$ имеет порядок $v^3 \ln v$, $v \equiv 2,4 \bmod 6$ (то есть для всех v, для которых существуют $S(3,4,v)$).*

Верхняя оценка тривиальна. Доказательство нижней оценки напрямую не использует трейды, но используется теорема 4: при помощи нескольких известных и одной новой конструкции для каждого случая $v \bmod 36$ строится $S(3,4,v)$, в которую «встроен» произвольный латинский куб порядка v/const.

3.5. Графы Грассмана: q-аналоги систем Штейнера. Граф Грассмана $J_q(v,k)$ строится на подпространствах размерности k данного v-мерного пространства V над полем мощности q. Два k-мерных подпространства смежны, если они их пересечение имеет размерность $k-1$. Как и в случае графов Джонсона, графы $J_q(n,k)$ и $J_q(n,n-k)$ изоморфны, поэтому далее полагаем $2k \leq n$.

Множество всех k-мерных подпространств, содержащих данное $(k-1)$-мерное подпространство, является дельсартовой кликой, набор всех таких клик составляет с графом $(k(v-k), v-k)$-пару.

Структура Штейнера $S_q(k-1,k,v)$ — клик-дизайн в графе $J_q(v,k)$. Более общо, структуры Штейнера $S_q(t,k,v)$, соответствующие битрейды $T_q(t,k,v)$ и t-$(v,k,\lambda)_q$ схемы являются подпространственными аналогами (в англоязычной литературе известные также как subspace designs) классических систем Штейнера, битрейдов и блок-схем, где вместо множества V рассматривается конечномерное пространство над полем порядка q, а вместо k-подмножеств (t-подмножеств) — k-мерные (t-мерные) подпространства.

В настоящее время известен только один набор параметров, а именно $S_q(2,3,13)$ [1], при котором нетривиальные $S_q(t,k,v)$ существуют, кроме случая $t=1$, который соответствует разбиениям пространства на подпространства, известным как «spreads». Минимальные битрейды $T_q(k-1,k,v)$, являющиеся клик-битрейдами в $J_q(v,k)$, существуют при любых v, $k \le v/2$ и q — степени простого числа:

Теорема 7 [8]. *Набор k-мерных подпространств v-мерного пространства, $v \ge 2k$, все элементы которых удовлетворяют уравнениям $x_1x_{1+k}+\ldots+x_kx_{2k}=0$, $\quad x_{2k+1}=\ldots=x_v=0$, будучи записанными в виде наборов $(x_1,\ldots,x_v)$ в некотором фиксированном базисе, разбивается на два поднабора, образующих битрейд $T_q(k-1,k,v)$. Число таких подпространств $\prod_{i=0}^{k-1}(1+q^i)$, что совпадает с границей весового распределения для мощности клик-битрейда в $J_q(v,k)$.*

Подграф графа $J_q(n,k)$, индуцированный такими подпространствами, — *дуальный полярный граф* $[D_k(q)]$ (дуальными полярными называются графы нескольких классов, из них только $[D_k(q)]$ являются двудольными).

3.6. Половинные гиперкубы: 1*-совершенные коды. Половинным (halved) n-кубом* $\frac{1}{2}H(n,2)$ называется граф, построенный да одной доле графа n-куба $H(n,2)$ (без потери общности, на двоичных n-словах с четным числом единиц). Ребром соединены вершины на расстоянии Хэмминга 2.

Окрестность слова с нечетным числом единиц в $H(n,2)$ является дельсартовой кликой в $\frac{1}{2}H(n,2)$ тогда и только тогда, когда n четно. Множество всех таких клик образует $(n(n-1)/2, n-1)$-пару, при четном n являющуюся дельсартовой.

Определение клик-дизайна в $\frac{1}{2}H(n,2)$ эквивалентно определению двоичного расширенного 1-совершенного кода, или кода с параметрами расширенного кода Хэмминга. Такие коды существуют при любом n равном степени двойки. Соответствующие же битрейды существуют при любом четном n, минимальная мощность битрейда — $2^{n/2}$, подграф, индуцированный таким битрейдом, изоморфен $\frac{n}{2}$-кубу $H(\frac{n}{2},2)$. В недавней работе [6] получена классификация клик-битрейдов в графах $\frac{1}{2}H(8,2)$ и $\frac{1}{2}H(10,2)$, а также в $\frac{1}{2}H(12,2)$ в случае, когда трейды состоят только из слов с 6-ю единицами (что эквивалентно битрейдам Штейнера $T(5,6,12)$).

Большое число 1-совершенных кодов (и, следовательно, расширенных 1-совершенных кодов) было построено в классической работе [19]. Нижняя оценка числа таких кодов (клик-дизайнов в

$\frac{1}{2}H(n,2)$), вытекающая из [19], имеет вид $2^{N(1+o(1))}$, где $N = 2^{\frac{n}{2}}/n$ — число трейдов минимальной мощности, на которые разбивается один код. Полученные после [19] нижние оценки [7] не улучшили асимптотику логарифма, а известные верхние [23] находятся в рамках $2^{2^{n-o(n)}}$.

3.7. Двудольные и антиподальные графы. В случае, когда сам дистанционно регулярный граф Γ двудольный, ребра графа суть дельсартовы клики, клик-дизайном является каждая из долей графа, пара долей образует единственный битрейд.

Более интересен случай антиподальных графов. Граф Γ называется *антиподальным*, если соотношение «быть на расстоянии $\mathrm{diam}(\Gamma)$» является эквивалентностью (наиболее легко представимый, но не единственно возможный случай — когда классы эквивалентности имеют мощность 2). Отождествление вершин каждого класса эквивалентности приводит к другому дистанционно регулярному графу, называемому *свернутым* (folded). Эта операция также приводит к сворачиванию изометричного двудольного подграфа Γ^T из теоремы 2. В случае, если после сворачивания Γ^T остается двудольным, он соответствует минимальному клик-битрейду в свернутом Γ. Это происходит в случаях, когда Γ — половинный n-куб $\frac{1}{2}H(n,2)$ или граф Джонсона $J(n,n/2)$, при n кратных 4. Таким образом, свернутый k-куб $\overline{H}(k,2)$ при четном k пополняет небогатую коллекцию (k-куб $H(k,2)$, дуальный полярный граф $[D_k(q)]$, полный двудольный граф) двудольных дистанционно регулярных графов, встречающихся в качестве подграфа Γ^T.

4. Другие трейды, число ненулей собственных функций

Мы не рассмотрели кратные клик-дизайны (каждая клика содержит λ элементов дизайна) и соответствующий, более общий, класс битрейдов (без условия независимости для T_0 и T_1). Кроме того, для многих комбинаторных конфигураций (таких, как t-(v,k,λ) схемы и их подпространственные аналоги, совершенные коды в $H(n,q)$, $q>2$, МДР- и MRD-коды с расстоянием больше 2, корреляционно-иммунные функции, ортогональные массивы, совершенные раскраски) битрейды определяются естественным образом (хотя и не укладываются в концепцию клик-битрейдов) и часто изучаются в той или иной альтернативной терминологии. Более того, как и в частном случае клик-битрейдов, во многих случаях битрейды связаны с собственными функциями графа, поскольку спектр их характеристической $\{0,\pm1\}$-функции состоит из небольшого числа собственных значений графа. Поскольку в каждом случае актуальна задача

нахождения минимального размера битрейда, которая имеет непосредственное отношение к оценкам числа объектов, вопрос о размере минимального носителя (то есть о минимальном числе ненулей) собственной функции графа также интересен в этом контексте, хотя этот вопрос естественный и с общематематической точки зрения.

В настоящее время, минимальное число ненулей собственной функции неизвестно даже для графов Хэмминга $H(n,q)$, $q \geq 3$ (в частности, в недвоичном случае неизвестен минимальный размер трейда, соответствующего 1-совершенным кодам). В общем случае известны некоторые оценки [20] и точные формулы для максимального собственного значения (q^n, тривиально), минимального (2^n, согласно границе весового распределения), и для второго наибольшего собственного значения ($2(q-1)q^{n-2}$, это новый результат [17]).

Для двоичного случая размер $2^{(n+|\theta|)/2}$ минимального носителя собственной функции графа $H(n,2)$ находится достаточно просто, хотя этот известный факт, по-видимому, нигде не опубликован. Нижняя граница доказывается индукцей по $n-|\theta|$. База индукции — случай $|\theta| = n$ (максимальное и минимальное собственное значение). Индукционный шаг основан на том факте, что для собственной функции f с собственным значением θ функции

$$f(x_1,\dots,x_{i-1},0,x_i,\dots,x_{n-1}) \pm f(x_1,\dots,x_{i-1},1,x_i,\dots,x_{n-1})$$

являются собственными функциями графа $H(n-1,2)$ с собственными значениями $\theta \pm 1$ (или тождественно нулевыми, что невозможно для всех i в случае $|\theta| \neq n$). Пример минимального носителя — множество $\{(x,x,y) : x \in \{0,1\}^{(n-|\theta|)/2},\ y \in \{0,1\}^{|\theta|}\}$, собственная функция на нем равна 1 или -1, в зависимости от четности числа единиц в x, если θ положительно, или в (x,y), если θ отрицательно.

Работа поддержана Российским научным фондом (14-11-00555).

Список литературы

1. Braun M., Etzion T., Östergård P. R. J., Vardy A., Wassermann A. Existence of q-analogs of Steiner systems // ArXiv.org: 1304.1462, 2013.

2. Cavenagh N. J. The theory and application of latin bitrades: A survey // Math. Slovaca — 2008. — Vol. 58, no. 6. — P. 691–718.

3. Eberhard S., Manners F., Mrazović R. Additive triples of bijections, or the toroidal semiqueens problem // ArXiv.org: 1510.05987, 2015.

4. Glebov R., Luria Z. On the maximum number of Latin transversals // J. Comb. Theory, Ser. A. — 2016. — Vol. 141. — P. 136–146.

5. Hoffman A. J. On eigenvalues and colourings of graphs // Graph

Theory and Its Applications. — New York : Acad. Press, 1970. — P. 79–91.

6. Krotov D. S. The extended 1-perfect trades in small hypercubes // ArXiv.org: 1512.03421, 2015.

7. Krotov D. S., Avgustinovich S. V. On the number of 1-perfect binary codes: A lower bound // IEEE Trans. Inf. Theory. — 2008. — Vol. 54, no. 4. — P. 1760–1765.

8. Krotov D. S., Mogilnykh I. Y., Potapov V. N. To the theory of q-ary Steiner and other-type trades // Discrete Math. — 2016. — Vol. 339, no. 3. — P. 1150–1157.

9. Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n-ary quasigroups and switching subquasigroups // Quasigroups Relat. Syst. — 2008. — Vol. 16, no. 1. — P. 55–67.

10. Linial N., Luria Z. An upper bound on the number of Steiner triple systems // Random Struct. Alg. — 2013. — Vol. 43, no. 4. — P. 399–406.

11. Linial N., Luria Z. An upper bound on the number of high-dimensional permutations // Combinatorica. — 2014. — Vol. 34, no. 4. — P. 471–486.

12. Östergård P. R. J. Switching codes and designs // Discrete Math. — 2012. — Vol. 312, no. 3. — P. 621–632.

13. Potapov V. N. On the number of latin hypercubes, pairs of orthogonal latin squares and MDS code // ArXiv.org: 1510.06212, 2015.

14. Potapov V. N. On the number of SQS. // ArXiv.org: 1606.02426, 2016.

15. Potapov V. N. On the number of transversals in latin squares // Discrete Appl. Math. — 2016. — Vol. 202. — P. 194–196.

16. Taranenko A. A. Multidimensional permanents and an upper bound on the number of transversals in latin squares // J. Comb. Des. — 2015. — Vol. 23, no. 7. — P. 305–320.

17. Valyuzhenich A. A. Minimal supports of eigenfunctions of Hamming graphs // ArXiv.org: 1512.02606, 2015.

18. Wilson R. M. Nonisomorphic Steiner triple systems // Mathematische Zeitschrift. — 1974. — Vol. 135, no. 4. — P. 303–313.

19. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. Вып. 8. — М.: Физматгиз, 1962. — С. 337–339.

20. Воробьёв К. В., Кротов Д. С. Оценки мощности минимального 1-совершенного битрейда в графе Хэмминга // Дискрет. анализ и исслед. операций. — 2014. — Т. 21, № 6. — С. 3–10.

21. Потапов В. Н. Многомерные латинские битрейды // Сиб. мат. ж. — 2013. — Т. 54, № 2. — С. 407–416.

22. Потапов В. Н., Кротов Д. С. О числе n-арных квазигрупп конечного порядка // Дискр. мат. — 2012. — Т. 24, № 1. — С. 60–69.

23. Сапоженко А. А. К вопросу о числе совершенных кодов // Проблемы теоретической кибернетики. Материалы XVI Межд. конф. — Н. Новгород: Изд-во Нижегородского гос. ун-та, 2011. — Р. 416–419.

СЕМЕЙСТВА ЗАМКНУТЫХ КЛАССОВ В P_k, ОПРЕДЕЛЯЕМЫЕ АДДИТИВНЫМИ И ПОЛИНОМИАЛЬНЫМИ ПРЕДСТАВЛЕНИЯМИ ФУНКЦИЙ

Д. Г. Мещанинов (Москва)

Как обычно, $E_k = \{0, 1, \ldots, k-1\}$ для натурального $k \geq 2$, $P_k = \{f : E_k^n \to E_k,\ n = 0, 1, 2, \ldots\}$ — класс всех функций k-значной логики, Pol_k — замкнутый класс функций из P_k, представимых полиномами над кольцом вычетов $\mathbb{Z}_k$. В дальнейшем под полиномами будем понимать именно полиномы над $\mathbb{Z}_k$, символами $+, -, \cdot$ обозначаем операции кольца $\mathbb{Z}_k$ (иные случаи их употребления будут специально оговариваться). Будем использовать верхний индекс в скобках для указания числа переменных: $f^{(n)}$ — функция f зависит от n переменных, $\Phi^{(n)}$ — подмножество некоторого класса Φ функций, состоящее из функций от n переменных. Буквами p, q, возможно, с индексами, будем обозначать простые числа. Бинарные отношения и операции над наборами длины n выполняются покомпонентно.

Исторические корни

Известному результату А. В. Кузнецова, изложенному С. В. Яблонским в 1958 г. [1], о том, что *равенство $Pol_k = P_k$ имеет место*

тогда и только тогда, когда число k простое, предшествовали следующие.

В 1863 г. Ш. Эрмит [1], анализируя так называемые перестановочные многочлены над полем $GF(p^m)$, установил, что при простом k любая функция из $P_k^{(1)}$ представима полиномом.

В 1921 г. О. Кемпнер [2] вычислил мощность $|Pol_k^{(1)}|$ для $k = p^m$, откуда следует, что равенство $Pol_k^{(1)} = P_k^{(1)}$ справедливо в точности при $m = 1$ (позже мощность $|Pol_k^{(1)}|$ вычислена для всех значений k, а результат Кемпнера получил более краткий вывод [2–7]).

Кроме условия равенства $Pol_k = P_k$ А. В. Кузнецовым получена

Теорема 1 [1]. *При составном k класс Pol_k не является предполным в P_k.*

Если $p_1|k$, $p_2|k$, $p_1 \neq p_2$, то $Pol_k \subseteq C(p_1) \cap C(p_2) \subset P_k$, где $C(d)$ — замкнутый класс функций, сохраняющих сравнение по модулю d, $d|k$ (т. е. сохраняющих разбиение множества E_k).

Если $k = p^m, m \geq 2$, то существует замкнутый класс K такой, что $Pol_k \subseteq K \subset C(p) \subset P_k$. Класс K состоит из функций f таких, что для всех $\tilde{y}$ из E_k^n функции $f(\tilde{x} + p\tilde{y})$ по модулю p^2 линейны относительно $py_1, \ldots py_n$:

$$f(\tilde{x} + p\tilde{y}) \equiv c_0(\tilde{x}) + py_1c_1(\tilde{x}) + \cdots + py_nc_n(\tilde{x}) \pmod{p^2}.$$

В связи с этим при составном k возникает две проблемы, решению которых и посвящена данная работа.

1. Нахождение условий, при которых функция из P_k принадлежит классу $Polk$ (условий полиномиальности).

2. Описание замккнутых классов, содержащих Pol_k, и решетки таких классов по отношению включения.

Обзор критериев полиномиальности

Очевидный способ проверить полиномиальность функции и построить реализующий ее полином состоит в анализе системы линейных уравнений над кольцом $\mathbb{Z}_k$ для коэффициентов полинома. В этой связи важна

Теорема 2 [8]. *Если $k = p^m$ и $f \in Pol_k$, то существует такой полином, представляющий функцию f, в который каждая переменная входит в степени не выше $mp - 1$.*

Как выяснить разрешимость системы уравнений для коэффициента полинома? Как ее решить? В каком виде искать реализующий данную функцию полином?

Перечислим полученные к настоящему моменту критерии полиномиальности.

1. Л. Карлиц в 1964 г. установил следующие критерии для функций из $P_k^{(1)}$ и $P_k^{(2)}$ при $k = p^m$.

Теорема 3 [9]. *При $k = p^m$ функция $f(x)$ принадлежит классу $Pol_k^{(1)}$ тогда и только тогда, когда для всех $c \in E_p$, $r \in E_{p^{m-1}}$ выполняется соотношение*

$$\sum_{s=0}^{m}(-1)^{r-s}\binom{r}{s}f(c+s) \equiv 0 \pmod{p^{\nu(rp)}},$$

где $\nu(t) = \min\{m, \mu(t)\}$, $\mu(t)$ — показатель наибольшей степени p, делящей $t!$.

Теорема 4 [9]. *При $k = p^m$ функция $f(x)$ принадлежит классу $Pol_k^{(1)}$ тогда и только тогда, когда для всех $l \in \mathbb{Z}$ существуют функции $f_1, \ldots, f_{m-1} \in P_k^{(1)}$ такие, что*

$$f(x + lp) = f_0(x) + lpf_1(x) + (lp)^2 f_2(x) + \cdots + (lp)^{m-1} f_{m-1}(x).$$

Теорема 5 [9]. *При $k = p^m$ функция $f(x, y)$ принадлежит классу $Pol_k^{(2)}$ тогда и только тогда, когда для всех $r, s \in E_k$ выполняется соотношение*

$$\sum_{i=0}^{r}\sum_{j=0}^{s}(-1)^{r+s-i-j}\binom{r}{i}\binom{s}{j} \equiv 0 \pmod{p^E},$$

$E = \min\{m, \mu(rp) + \mu(sp)\}$.

Теорема 6 [9]. *При $k = p^m$ функция $f(x, y)$ принадлежит классу $Pol_k^{(2)}$ тогда и только тогда, когда для всех $r, s \in \mathbb{Z}$ существуют функции $f_{i,j} \in P_k^{(2)}$ такие, что*

$$f(x + rp, y + sp) = \sum_{i+j<m}(rp)^i(sp)^j f_{ij}(x, y) = 0.$$

2. В 1971 г. Н. Н. Айзенберг и И. В. Семйон установили два критерия полиномиальности: один из них есть в точности теорема 4 Л. Карлица, другой же состоит в следующем.

Теорема 7 [8]. *Если $p_1, \ldots, p_s$ — попарно различные простые числа и $k = p_1 \cdots p_s$, то имеет место равенство $Pol_k = M_k$, где*

M_k — класс функций, сохраняющих сравнения по всем модулям-делителям числа k, т. е. удовлетворяющих для каждого p_i, $i = 1, \dots s$, условиям: если $\tilde{a} \equiv \tilde{b} \pmod{p_i}$, то $f(\tilde{a}) \equiv f(\tilde{b}) \pmod{p_i}$.

В 1986 г. А. Н. Череповым [10] и независимо в 1987 Д. Г. Мещаниновым [11, 12] установлено, что *равенство $Pol_k = M_k$ справедливо только при $k = p_1 \cdots p_s$*.

3. И. Розенберг в 1974 г. [13] обобщил теоремы 4 и 6 на случай произвольного составного k и произвольного числа n переменных.

4. А. Н. Черепов в 1986 г. [10] вывел критерий полиномиальности для любых k и n, основанный на свойствах конечных разностей и интерполяционных формулах в кольце функций над $\mathbb{Z}$.

5. Д. Г. Мещаниновым в 1986–1987 гг. [11, 14] получены критерии полиномиальности в терминах конечных разностей для всех k, не делящихся на куб простого числа.

6. В 1989 г. А. Б. Ремизов [15] вывел специальный критерий для случая $k = p^2$ с помощью разложения функций, аналогичного разложению чисел в p-ичной позиционной системе счисления.

7. В 1992 г. Д. Г. Мещанинов [16] установил критерий полиномиальности для $k = p^3$, формулируемый также на языке конечных разностей с шагом p (p-разностей).

8. В 1995 г. Д. Г. Мещанинов [17] вывел конечно-разностный критерий для произвольного k, предложил алгоритм проверки полиномиальности и построения полинома, оценил временную сложность такого алгоритма для $k = p^m$ (сводящегося к вычислению и анализу p-разностей порядка $m - 1$) как $O(N \log N^m)$, где $N = k^n$ — размер входных данных, таблицы n-местной функции.

9. В 2011 г. С. Н. Селезнева [18] предложила критерий полиномиальности, основанный на теореме 2 и результатах [6, 7], и наилучший по сложности ($O(N)$) алгоритм построения полинома особого канонического вида при любых k и n.

Классы сохранения сравнений

Пусть $d|k$. Функция $f(\tilde{x})$ из P_k *сохраняет сравнение по модулю d*, если из условия $\tilde{a} \equiv \tilde{b} \pmod{d}$ следует, что и $f(\tilde{a}) \equiv f(\tilde{b}) \pmod{d}$. Если при этом $f(\tilde{a}) = f(\tilde{b})$, то функция называется *d-периодической*.

Функции, сохраняющие сравнение по модулю d, образуют замкнутый класс $C(d)$, предполный в P_k, если $d \neq 1$, $d \neq k$. При этом $C(1) = C(k) = P_k$. Для нескольких делителей $d_1, \dots d_s$ числа k введем также классы $C(d_1, \dots, d_s) = C(d_1) \cap \cdots \cap C(d_s)$ и $M_k = \bigcap_{d|k} C(d)$.

Тогда

$$\forall d|k\ Pol_k \subseteq M_k \subseteq C(d) \subseteq P_k$$

Решетка всех классов, содержащих M_k, описана А. Н. Череповым [10, 19]. Тем самым, в силу теоремы 9, *описана решетка всех классов, содержащих* Pol_k *при* $k = p_1 \cdots p_s$. *Если* $k = p^m$, *то решетка всех классов, находящихся между* Pol_k *и* M_k, *изоморфна* $(m-1)$*-мерному кубу* [10–12].

Теорема 8 [20, лемма 2]. *Класс* $C(d)$ *состоит из всех функций вида*

$$f(\tilde{x}) = g(\tilde{x}) + dh(\tilde{x}), \tag{1}$$

где функция $g(\tilde{x})$ *является* d*-периодической.*

Определим функции

$$g_d(\tilde{x}) = \begin{cases} 1, & \tilde{x} \equiv \tilde{0} \pmod d, \\ 0, & \tilde{x} \not\equiv \tilde{0} \pmod d, \end{cases} \qquad j_{\tilde{0}}(\tilde{x}) = \begin{cases} 1, & \tilde{x} = \tilde{0}, \\ 0, & \tilde{x} \neq \tilde{0}, \end{cases}$$

Следствие 1. *Система функций* $\{x + y, g_d(x, y), dj_{00}(x, y)\}$ *образует базис в классе* $C(d)$. *При некоторых условиях на числа* k *и* d *базисные функции* $g_d(x, y)$ *и* $dj_{00}(x, y)$ *можно заменить на одноместные.*

При $d = k \neq 2$ эти результаты выражают известные *вторую форму* функций и базис $\{x + y, j_0(x)\}$ в P_k.

Теорема 9. *При* $k = p^m$ *класс* M_k *состоит из всех функций вида*

$$f(\tilde{x}) = \sum_{i=0}^{m-2} p^i h_i(\tilde{x}) + p^{m-1} h(\tilde{x}), \tag{2}$$

где каждая функции $h_i(\tilde{x})$ *является* p^{i+1}*-периодической.*

Аналогичным образом выделяются и базисы в классах $C(d_1, \ldots, d_r)$. Для класса M_k при $k = p^m$ доказательство равносильного теореме 9 утверждения и полноты в M_k соответствующей системы функций изложено в 1996 г. Г. П. Гавриловым [21, предложение 2, замечание 4].

Решеточное представление

Пусть $d|k, \tilde{a} \in E_d^n$. Множество $\{\tilde{x} \in E_k^n : \tilde{x} \equiv \tilde{a} \pmod d\}$ называется *d-решеткой*. Рассмотрим представление

$$f(\tilde{x}) = \sum_{\tilde{a} \in E_d^n} f^{\tilde{a}}(\tilde{x}), \text{ где } f^{\tilde{a}}(\tilde{x}) = \begin{cases} f(\tilde{x}), & \tilde{x} \equiv \tilde{a} \pmod d, \\ 0, & \tilde{x} \not\equiv \tilde{0} \pmod d. \end{cases} \tag{3}$$

Функции $f^{\tilde{a}}$ называются *d-решеточными ограничениями* функции f. Они могут быть проще исходной функции f и позволяют сводить многие задачи принадлежности функции классам, содержащим $x+y$, к тем же задачам относительно ее решеточных ограничений. В частности, таким способом установлена

Теорема 10 [11, 14]. *Если $p|k$ и функция f из M_k является p-периодической, то $f \in Pol_k$.*

Справедливость теоремы для одноместных функций при $k = p^m$ отмечена Л. Карлицем [9].

Теорема 11 [11, 22]. *Если $d|k, d = d_1 \cdots d_s$, где $s \geq 2$, а числа $d_1, \ldots, d_s$ попарно взаимно простые, и функция f класса $C(d_1, \ldots d_s)$ является d-периодической, то справедливо представление*

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{i=1}^{s} (d/d_i) f_i(\tilde{x}), \tag{4}$$

где каждая функция f_i является d_i-периодической.

Следствие 2. *Если $p_1, \ldots p_s$ — различные простые делители числа k, а функция f из M_k является $p_1 \cdots p_s$-периодической, то $f \in Pol_k$.*

Сохранение разностей

Далее для $\tilde{t}$ из $\mathbb{Z}_+^n$ полагаем $\sigma(\tilde{t}) = t_1 + \cdots + t_n$, сумма вычисляется в кольце $\mathbb{Z}$.

Пусть $d|k, f \in P_k^{(n)}, \tilde{x} \in E_k^n, \tilde{r} \in \mathbb{Z}_+^n, R = \sigma(\tilde{r})$. Величины

$$\Delta^R(\tilde{r}) f(\tilde{x}) = \sum_{s_1=0}^{r_1} \cdots \sum_{s_n=0}^{r_n} (-1)^{R-\sigma(\tilde{r})} \binom{r_1}{s_1} \cdots \binom{r_n}{s_n} f(\tilde{x} + d\tilde{s})$$

называются *d-разностями типа $\tilde{r}$ и порядка R функции f в точке $\tilde{x}$*. Если $\tilde{a} \in E_d^n$, то d-разностями ограничения $f^{\tilde{a}}$ функции f называются ее d-разности в точках $\tilde{x} \equiv \tilde{a} \pmod{d}$. Функция f *сохраняет d-разности порядка R*, если для каждого $\tilde{r}$, $\sigma(\tilde{r}) = R$, и каждого $\tilde{a} \in E_d^n$ разности $\Delta^R(\tilde{r}) f^{\tilde{a}}(\tilde{x})$ равны при всех $\tilde{x} \equiv \tilde{a} \pmod{d}$.

Теорема 12 [17]. *Если $k = p^m$ и $f \in M_k^{(n)}$, то функция f принадлежит классу Pol_k тогда и только тогда, когда она сохраняет p-разности порядка $m-1$ и для каждого $\tilde{r}$, $\sigma(\tilde{r}) = R$, все ее p-разности типа $\tilde{r}$ кратны $p^R r_1! \cdots r_n!$. При этом каждая функция*

$f^{\tilde{a}}$, $\tilde{a} \in E_p^n$, *представляется полиномом вида*

$$f^{\tilde{a}}(\tilde{x}) = g_p(\tilde{y}) \sum_{\tilde{t}:\ \sigma(\tilde{t}) \le R} b(\tilde{y}) y_1^{t_1} \cdots y_n^{t_n}, \tag{5}$$

где $\tilde{y} = \tilde{x} - \tilde{a}, R \le m-1, b(\tilde{y}) \in E_k$.

Случай произвольного k сводится к случаю $k = p^m$ с помощью периодических функций. Пусть $k = p_1^{m_1} \cdots p_s^{m_s}$, $s \ge 2$. Положим $d = k$, $d_i = p_i^{m_i}$ для $i = 1, \ldots, s$ и рассмотрим формулу (4) для функции f класса M_k. Присутствующие в ней функции f_i также принадлежат M_k, а условие $f \in Pol_k$ равносильно условиям $f_i \in Pol_k$ для всех $i = 1, \ldots, s$. Для $p_i^{m_i}$-периодической функции f_i из M_k условие принадлежности классу Pol_k аналогично случаю $k = p_i^{m_i}$, а полином $f_i^{\tilde{a}}$ имеет вид

$$f_i^{\tilde{a}}(\tilde{x}) = (k/d_i) g_{p_i}(\tilde{y}) \sum_{\tilde{t}:\ \sigma(\tilde{t}) \le R} b(\tilde{y}) y_1^{t_1} \cdots y_n^{t_n}, \tag{6}$$

$\tilde{y} = \tilde{x} - \tilde{a}, \tilde{a} \in E_{p_i}^n, R \le m_i - 1, b(\tilde{y}) \in E_k$.

Сохранение первых d-разностей

Величины

$$\Delta_i f(x_1, \ldots, x_i, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x_i + d, x_{i+1}, \ldots, x_n) - f(\tilde{x})$$

называются (первыми) *d-разностями функции f по переменной x_i в точке $\tilde{x}$*. Функция f *сохраняет d-разности*, если при фиксированных i и $\tilde{a} \in E_d^n$ величины $\Delta_i f^{\tilde{a})}(\tilde{x})$ не зависят от $\tilde{x}$. Функция *абсолютно сохраняет d-разности*, если разности $\Delta_i f^{\tilde{a}}(\tilde{x})$ не зависят и от $\tilde{a}$. Функции, сохраняющие и абсолютно сохраняющие d-разности, образуют замкнутые классы $R(d)$ и $L(d)$.

Теорема 13 [12, 22]. *Классы $R(d)$ и $L(d)$ обладают следующими свойствами.*

1. *Если $d \ne 1$ и $d \ne k$, то $L_k \subset L(d) \subset R(d) \subset C(d)$, где $L_k = L(1) = R(1)$ — класс всех линейных по модулю k функций. Кроме того, $L(k) = R(k) = P_k$.*

2. *Если $d_1 | d_2$, то $R(d) \subseteq R(d_2)$ и $L(d_1) \subseteq L(d_2)$. Классы $R(d)$ образуют решетку, изоморфную решетке делителей числа k. Такую же решетку образуют классы $L(d)$.*

3. *Класс $R(d)$ состоит из всех функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + g(\tilde{x}) + \sum_{\tilde{a}\in E_d^n} \sum_{j=1}^{n} b_j(\tilde{a}) y_j g_d(\tilde{y}). \tag{7}$$

Класс $L(d)$ состоит из всех функций вида

$$f(\tilde{x}) = l(\tilde{x}) + g(\tilde{x}) + \sum_{j=1}^{n} b_j d\lfloor x_j/d \rfloor. \tag{8}$$

В этих формулах $l(\tilde{x}) \in L_k$, функция $g(\tilde{x})$ является d-периодической, $\tilde{y} = \tilde{x} - \tilde{a}$ и $b_j(\tilde{a}), b_j \in E_k$.

4. *Условия "класс $R(d)$ является предполным в $C(d)$", "класс $L(d)$ является предполным в $R(d)$" и равенство $k = pd$ эквивалентны.*

Теорема 14 [12]. *Пусть $p_1, \ldots, p_s, q_1, \ldots, q_t$ — различные простые числа, $s \geq 1$, $k = p_1^2 \cdots p_s^2 Q$, $d_i = k/p_i$, $i = 1, \ldots, s$, где $Q = 1$ или $Q = q_1 \cdots q_t$. Тогда $Pol_k = M_k \cap R(d_1) \cap \cdots R(d_s)$, а классы Pol_k, M_k и все классы, находящиеся между ними, образуют решетку, изоморфную s-мерному кубу.*

С помощью свойств сохранения разностей можно описать надструктуру не только класса Pol_k но и класса L_k при $k = p_1 \cdots p_s$.

Классы, содержащие L_k

Теорема 15 [22]. *Пусть $k = p_1 \cdots p_s$, $s \geq 2$, $d_i = k/p_i$, $i = 1, \ldots, s$. Тогда справедливо следующее.*

1. *Классы $M_k = Pol_k$, $R(p_i)$ и $R(p_j)$ $i \neq j$ несравнимы по включению.*

2. *Для каждого $i = 1, \ldots, s$ класс $M_k \cap R(d_i)$ состоит в точности из функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + \sum_{j\neq i} d_j h_j(\tilde{x}), \tag{9}$$

где $l(\tilde{x}) \in L_k$, а каждая функция h_j является p_j-периодической.

3. *Выполняется равенство $Pol_k = M_k \cap R(d_1) \cap \cdots \cap R(d_s)$,*

4. *Классы L_k, M_k и все классы, находящиеся между ними, образуют решетку, изоморфную s-мерному кубу.*

При $k = p$ (и только при нем) класс L_k является предполным в $Pol_k = P_k$ [1]. В [23] построена решетка всех классов, содержащих L_k при $k = 4$. Ее обобщение на все $k = p^2$ анонсировано в [24].

Результаты других авторов

При $k = p^m$ применяется разложение функций в сумму функций p-значной логики с коэффициентами $1, p, p^2, \dots p^{m-1}$ (координатных функций). Оно равносильно представлению в виде суммы с периодическими слагаемыми, подобному (3). Таким способом А. А. Нечаевым найден критерий полноты в P_k системы, порождающей Pol_k, [25] (аналогичный критерий для $k = p_1 \cdots p_s$ найден А. Н. Череповым [19]). Весьма важен результат А. Б. Ремизова.

Теорема 16 [15]. *Если $p^3|k$, то между классами Pol_k и M_k имеется бесконечная цепь замкнутых классов.*

При помощи координатных функций Г. П. Гавриловым [21] выделена цепь классов $V_m(l)$, $l = 1, \dots m-1$, состоящих из функций вида

$$f(\tilde{x}) = \pi(\tilde{x}) + p^l h(\tilde{x}). \tag{10}$$

Класс $V_3(2)$ был описан ранее на языке p-разностей порядка 2, он оказался предполным в M_{p^3} [16].

С помощью координатных функций Г. П. Гаврилов описал также семейство классов в P_k при $k = p^m$, обобщающих класс K Кузнецова (см. теорему 1) [26]. Некоторые свойства классов, обобщающих K, анонсированы в [27].

Также М. В. Заец [28, 29] описал на языке координатных функций цепь классов длины 3 или 4 с минимумом Pol_k и максимумом M_k, $k = p^m$.

Итак, указаны аддитивные представления (1)–(10), определяющие замкнутые классы, содержащие все полиномы или все линейные функции. Многие из них переносятся и на случай частично определенных функций. Некоторые результаты по этой теме анонсированы в [30,31].

Список литературы

1. Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН СССР. — 1958. — Т. 51. — С. 5–142.

2. Hermit Ch. Sur les fonctions des sept lettres // C. R. Acad. Sci. Paris. — 1863. — 57. — P. 750–757.

3. Kempner A. J. Polynomials and their residue systems // Trans. AMS. — 1921. — V. 22. — 240-288.

4. Redei L., Szele T. Algebraisch-Zahlentheoretisch Betrachtungen über Ringe, II // Acta Math. — 1950. — 82. — P. 240–291.

5. Keller G, Olson F. R. Counting polynomial functions $(\mathrm{mod}\ p^n)$ // Duke Math. J. — 1968. — 35:4. — P. 835–838.

6. Айзенберг Н. Н., Семйон И. В., Циткин А. И. Мощность класса функций k-значной логики от n переменных, представимых полиномами по модулю k // Многоустойчивые элементы и их применение — М.: Сов. радио, 1971. — С. 79–83.

7. Singmaster D. On polynomial functions $(\mathrm{mod}\ m)$ // J. Number Theory. — 1974. — 6:5. — P. 345–352.

8. Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k-значной логики полиномами по модулю k // Многоустойчивые элементы и их применение — М.: Сов. радио, 1971. — С. 84–88.

9. Carlitz L. Functions and polynomials $(\mathrm{mod}\ p^n)$ // Acta Arithm. — 1964. — 9. — P. 66–78.

10. Черепов А. Н. Надструктура класса сохранения отношений сравнения в k-значной логике по всем модулям-делителям k. Автореф. дисс. канд. физ.-мат. н. — М., 1986.

11. Мещанинов Д. Г. О полиномиальной реализации функций k-значной логики. — Деп. ВИНИТИ 23.10.87, № 7441-В87.

12. Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Математические вопросы кибернетики. Вып. 7. — М.: Наука, 1998. — С. 265–280.

13. Rosenberg I. G. Polynomial functions over finite rings //Glasnik Matematiki. — 1975. — 10:1. — P. 25–33.

14. Мещанинов Д. Г. Некоторые условия представимости функций из P_k полиномами по модулю k // Докл. АН СССР. — 1988. — 299:1. — С. 50–53.

15. Ремизов А. Б. О надструктуре замкнутого класса полиномов по модулю k // Дискретная математика. — 1989. — 1:1. — С. 3–15.

16. Мещанинов Д. Г. О вторых p-разностях функций p^α-значной логики // Дискретная математика. — 1992. — 4:4. — С. 131–139.

17. Мещанинов Д. Г. Метод построения полиномов для функций k-значной логики // Дискретная математика. — 1995. — 7:3. — С. 48–60.

18. Селезнева С. Н. Быстрый алгоритм построения для k-значных функций полиномов по модулю k при составных k // Дискретная математика. — 2011. — 23:3. — С. 3–22.

19. Черепов А. Н. Описание структуры замкнутых классов в P_k, содержащих класс полиномов // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 5–18.

20. Мещанинов Д. Г. О некоторых свойствах надструктуры класса полиномов в P_k // Матем. заметки. — 1988. — 44:5. — С. 673–681.

21. Гаврилов Г. П. О надструктуре класса полиномов в многозначных логиках // Дискретная математика. — 1996. — 8:3. — С. 90–97.

22. Мещанинов Д. Г. О замкнутых классах k-значных функций, сохраняющих первые d-разности // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 219–230.

23. Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов // Дискретная математика. — 1997. — 9:2 — С. 24–39.

24. Мещанинов Д. Г. О замкнутых классах полиномов над кольцом Z_k // Труды IX Междунар. конф. "Дискретные модели в теории управляющих систем" (20–22 мая 2015 г.) — М.: МАКС-Пресс, 2015. — С. 161–163.

25. Нечаев А. А. Критерий полноты систем функций p^n-значной логики, содержащих операции сложения и умножения по модулю p^n // Методы дискретного анализа в решении комбинаторных задач. Вып. 34. — Новосиб., 1980. — С. 74–89.

26. Гаврилов Г. П. О замкнутых классах многозначной логики, содержащих класс полиномов // Дискретная математика. — 1997. — 9:2. — С. 12–23.

27. Мещанинов Д. Г. О классе Кузнецова в p^a-значной логике // Проблемы теоретической кибернетики. Тез. докл. XI Междунар. конф. Ульяновск, 10–14 июня 1996 г. — М.: Изд-во РГГУ, 1996. — С. 142–143.

28. Заец М. В. Классификация функций над примарным кольцом вычетов в связи с методом покоординатной линеаризации // Прикл. дискретная математика. Приложение. — 2014. — 7. — С. 16–19.

29. Заец М. В. О классе вариационно-координатно-полиномиальных функций над примарным кольцом вычетов // Прикл. дискретная математика. — 2014. — №3 (25). — С. 12–27.

30. Мещанинов Д. Г. О надструктуре класса полиномов в частичной k-значной логике // Труды VII Междунар. конф. "Дискретные модели в теории управляющих систем". Покровское. 4–6 марта 2006 г. — С. 248–250.

31. Мещанинов Д. Г. Классификация аддитивных представлений частичных и всюду определенных функций k-значной логики // Труды VIII Междунар. конф. "Дискретные модели в теории управляющих систем" (6–9 апреля 2009 г.) — М.: МАКС-Пресс. 2009. — С. 214–218.

ОБ ОЦЕНКЕ ЧИСЛА И ЭФФЕКТИВНОМ ПОИСКЕ ПОВТОРОВ И ПАЛИНДРОМОВ С РАЗРЫВАМИ В ФОРМАЛЬНЫХ СЛОВАХ

Р. М. Колпаков (Москва)

В данной работе рассматриваются вопросы, связанные с оценкой числа и эффективным поиском регулярных фрагментов в формальных словах. Классическим примером регулярных фрагментов являются периодичности. Под периодичностью в слове формально понимается любой фрагмент, порядок которого не меньше 2, где порядок слова определяется как отношение длины слова к его минимальному периоду. Периодичности имеют фундаментальное начение для комбинаторных свойств слов и активно используются в различных алгоритмах, работающих с формальными словами, в частности, в алгоритмах поиска образцов в слове, алгоритмах сжатия слов, алгоритмах анализа биологических последовательностей и т. д. Простейшим частным случаем периодичности является квадрат, т. е. подслово вида uu, где u — произвольное непустое слово, которое называется корнем данного квадрата. Аналогичным образом периодичность вида uuu, где u — произвольное непустое слово, называется кубом. В общем случае, для любого целого $k \geq 2$ периодичность вида $u^k = \underbrace{uu\ldots u}_{k}$, где u — произвольное непустое слово, называется k-ой степенью слова u. Слово называется примитивным, если оно не является степенью меньшего слова. Длину произвольного слова w будем обозначать через $|w|$.

При изучении квадратов в формальных словах естественным образом можно ограничиться примитивными квадратами, т.е. квадратами, имеющими примитивные корни. В [1] показано, что максимальное число примитивных квадратов в слове длины n равно по порядку $\Theta(n \log n)$, и все примитивные квадраты в слове длины n могут быть найдены за оптимальное время $\Theta(n \log n)$. В [2,3] предложены алгоритмы проверки существования квадрата в слове длины n за время $O(n)$. В [4] показано, что все примитивные квадраты могут быть найдены в слове длины n за время $\Theta(n \log k + S)$, где k — размер алфавита слова, а S — число примитивных квадратов в слове (тем самым в случае алфавита константного размера и сравнительно небольшого числа примитивных квадратов в слове данный алгоритм может оказаться эффективнее алгоритма, предложенного в [1]).

Естественным обобщением периодичностей, содержащих целое

число корней, являются "дробные" периодичности вида $\underbrace{uu\ldots u}_{k}u'$, где $k \geq 2$ и u' — префикс непустого слова u. Такая периодичность в слове называется максимальной, если она не является частью большей периодичности с тем же минимальным периодом, т.е. не может быть расширена в слове ни на один символ с сохранением своего минимального периода. Отметим, что любая периодичность в слове является частью некоторой максимальной периодичности с тем же минимальным периодом, т. е. максимальные периодичности задают в слове все остальные периодичности любого другого типа: квадраты, кубы, целые степени и т. д., полностью определяя таким образом периодическую структуру слова. В [5] показано, что в слове длины n все максимальные периодичности могут быть найдены за время $\Theta(n \log n)$, при этом в случае алфавита неограниченного размера и вычислительной модели, допускающей только попарные сравнения символов с целью проверки их равенства, полученная оценка времени поиска является оптимальной по порядку. В [6] установлено, что максимальное число максимальных периодичностей в слове длины n равно по порядку $\Theta(n)$, и все максимальные периодичности в слове длины n могут быть найдены за время $\Theta(n \log k)$, где k — размер алфавита слова. Таким образом, в случае алфавита константного размера предложенный в [6] алгоритм является оптимальным. Данный результат был усилен в [7], где показано, что в слове длины n над полиномиально ограниченным алфавитом все максимальные периодичности могут быть найдены за время $\Theta(n)$ (алфавит называется полиномиально ограниченным, если существует вычисляемое за константное время соответствие между символами алфавита и натуральными числами, не превосходящими по величине некоторого полинома от n). Дальнейшие исследования [8, 9] в данной области связаны с уточнением времени поиска всех максимальных периодичностей для случая линейно упорядоченного алфавита неограниченного размера и вычислительной модели, допускающей попарные сравнения символов относительно определенного на алфавите линейного порядка (в [10] было высказано предположение, что в этом случае все максимальные периодичности в слове также могут быть найдены за линейное время). Наилучший к настоящему времени результат для данного случая получен в [11], где предложен алгоритм поиска всех максимальных периодичностей в слове длины n за время $O(n \cdot \kappa(n))$, где $\kappa(\cdot)$ — функция, обратная к функции Аккермана.

В [6] на основе компьютерных экспериментов была высказана гипотеза, что число максимальных периодичностей в слове не превос-

ходит его длины. После длительных активных исследований, опубликованных в многочисленных работах на эту тему, эта гипотеза доказана в [12]. В данной работе установлено, что каждой максимальной периодичности в слове можно сопоставить некоторый содержащийся в этой периодичности символ слова, отличный от самого первого символа, так, что разным периодичностям сопоставляются разные символы, из чего непосредственно следует, что число максимальных периодичностей в слове строго меньше его длины. Наилучшая к настоящему времени верхняя оценка числа максимальных периодичностей в словах фиксированной длины получена в [13], где доказано, что число максимальных периодичностей в слове длины n не превосходит $22n/23$.

Квадраты в словах естественным образом обобщаются на случай фрагментов вида uvu, где u и v — некоторые непустые слова. Такой фрагмент называется повтором с разрывом, при этом слова u называются левой и правой копиями этого повтора, а слово v — его разрывом. Периодом повтора с разрывом называется суммарная длина копии и разрыва повтора. Отметим, что один и тот же фактор в слове может рассматриваться в качестве различных повторов с разрывом, имеющих разные периоды, т.е. повторы с разрывом, имеющие разные периоды, могут иметь одновременно одинаковые начальные и конечные позиции в слове. Такие повторы считаются различными. Повтор с разрывом в слове называется максимальным, если выполняются следующие два условия:

1) если повтор не является префиксом слова, то символ, предшествующий в слове левой копии повтора, отличен от символа, предшествующего его правой копии;

2) если повтор не является суффиксом слова, то символ, следующий в слове за правой копией повтора, отличен от символа, следующего за его левой копией.

Другими словами, повтор с разрывом является максимальным, если он не содержится в более длинном повторе с разрывом или более длинной периодичности, имеющих тот же период. Таким образом, любой повтор с разрывом однозначным образом расширяется с сохранением периода либо до некоторой периодичности, либо до некоторого максимального повтора в разрывом. Поэтому, с учетом возможности эффективного поиска периодичностей в словах посредством упомянутых выше в данной работе алгоритмов, задача эффективного поиска повторов в разрывом в словах сводится к задаче эффективного поиска максимальных повторов с разрывом. Важным частным случаем повторов с разрывом являются α-повторы при

$\alpha > 1$: повтор с разрывом называется α-повтором, если отношение его периода к длине его копии не превосходит α. Понятие α-повтора введено в работе [14], где было показано, что глово длины n содержит $O(\alpha^2 n)$ максимальных α-повторов, которые могут быть найдены за время $\Theta(\alpha^2 n \log k)$, где k — размер алфавита.

Наряду с периодичностями можно рассматривать в словах факторы порядка меньшего, чем 2. Мы называем такие факторы субпериодичностями. Субпериодичность называется δ-субпериодичностью, где $0 < \delta < 1$, если ее порядок не меньше $1 + \delta$. Аналогично понятию максимальной периодичности, субпериодичность называется максимальной, если она не содержится в более длинной периодичности или субпериодичности с тем же минимальным периодом, т.е. не может быть расширена в слове ни на один символ с сохранением своего минимального периода. Нетрудно заметить, что каждая максимальная δ-субпериодичность в слове однозначным образом представляется в виде некоторого максимального $1/\delta$-повтора с разрывом, период которого совпадает с минимальным периодом субпериодичности. Тем самым в слове существует взаимно однозначное соответствие между всеми максимальными δ-субпериодичностями и максимальными $1/\delta$-повторами с разрывом, представляющими эти субпериодичности. Поэтому в любом слове число максимальных δ-субпериодичностей не превосходит числа максимальных $1/\delta$-повторов с разрывом.

Алгоритмы поиска всех максимальных δ-субпериодичностей в слове на основе поиска $1/\delta$-повторов впервые были предложены предложены в [14]. В работе [15] показано, что в не содержащем периодичностей слове над константным алфавитом за линейное относительно длины слова время можно вычислить максимальный порядок содержащихся в этом слове субпериодичностей и найти все субпериодичности этого порядка. Используя идеи данной работы, в [16] предложен алгоритм поиска всех максимальных α-повторов в слове длины n над константным алфавитом за время $O(\alpha n + S)$, где S — число таких повторов в слове. В [17] показано, что в слове длины n над полиномиально ограниченным алфавитом максимальный α-повтор с разрывом, имеющий наибольшую длину, может быть вычислен за время $\Theta(\alpha n)$. В [18] установлено, что максимальное число максимальных α-повторов с разрывом в слове длины n равно по порядку $\Theta(\alpha n)$ и на основе подхода, предложенного в [17], предъявлен оптимальный алгоритм поиска всех максимальных α-повторов в слове длины n над константным алфавитом за время $O(\alpha n)$. В работе [19] было независимо показано, что в слове длины n содержится не более $18\alpha n$ максимальных α-повторов с разрывом,

которые могут быть найдены за время $\Theta(\alpha n)$ в более общем случае слова над полиномиально ограниченным алфавитом. Из полученной оценки $O(\alpha n)$ числа α-повторов вытекает, что слово длины n содержит $O(n/\delta)$ максимальных δ-субпериодичностей, и данная оценка для максимальных δ-субпериодичностей является оптимальной по порядку в случае слов над алфавитом неограниченного размера (вопрос об оптимальности данной оценки в случае слов над константным алфавитом остается пока открытым). Кроме того, пользуясь модификацией алгоритмов, предложенных в [14], с учетом полученной оценки числа α-повторов, можно показать, что в слове длины n все максимальные δ-субпериодичности могут быть найдены за время $\Theta(n \log k + \frac{n \log\log n}{\delta})$, где k — размер алфавита, или за среднее ожидаемое время $O(n \log n + \frac{n}{\delta} \log \frac{1}{\delta})$.

На основе компьютерных экспериментов в [18] выдвинута следующая гипотеза.

Гипотеза 1. *В слове длины n содержится не более αn максимальных α-повторов с разрывом.*

В поддержку данной гипотезы имеются также следующие косвенные соображения. Отметим, что период повтора с разрывом можно также формально определить как дистанцию между начальными позициями копий повтора. В таком случае понятие α-повтора можно обобщить также на случай $\alpha \leq 1$: при $\alpha \leq 1$ под α-повтором в слове будем понимать фрагмент, состоящий из двух смежных или пересекающихся копий таких, что отношение дистанции между начальными позициями копий к длине копий не превосходит α. Нетрудно заметить, что каждый максимальный 1-повтор представляет собой в качестве фрагмента слова некоторую максимальную периодичность, минимальный период которой является делителем периода 1-повтора. Таким образом, каждому максимальному 1-повтору однозначно сопоставляется максимальная периодичность. С другой стороны, каждой максимальной периодичности сопоставляется при этом по крайней мере один максимальный 1-повтор, период которого равен минимальному периоду периодичности, причем максимальной периодичности порядка, не меньшего 4, сопоставляется несколько максимальных 1-повторов (на самом деле насложно заметить, что каждой максимальной периодичности r сопоставляется $\lfloor e(r)/2 \rfloor$ различных максимальных 1-повторов). Таким образом, в любом слове число максимальных 1-повторов не меньше числа максимальных периодичностей и может быть больше числа максимальных периодичностей при наличии в слове периодичностей достаточно большого порядка. Тем не менее, пользуясь несложной модификацией пред-

ложенного в [10] доказательства того, что число максимальных периодичностей в слове меньше его длины, можно также доказать, что число максимальных 1-повторов в слове меньше его длины, тем самым гипотеза 1 справедлива для $\alpha = 1$. Данное наблюдение позволяет также предположить, что гипотеза 1 справедлива также при $0 < \alpha < 1$. Отметим также, что, согласно компьютерным экспериментам, в словах с максимально возможным числом максимальных периодичностей не содержится периодичностей большого порядка, тем самым имеется взаимно однозначное соответствие между максимальными 1-повторами и сопоставленными им максимальными периодичностями. Поэтому в [18] выдвинута также следующая гипотеза.

Гипотеза 2. *Для любого n в словах длины n максимальное число максимальных 1-повторов равно максимальному числу максимальных периодичностей.*

Одним из дальнейших направлений исследований в данной области является изучение повторов с разрывами, на длины которых накладываются произвольные ограничения, зависящие от длин копий. Пусть $f : \mathbf{N} \to \mathbf{R}$, $g : \mathbf{N} \to \mathbf{R}$ — две функции такие, что для любого $x \in \mathbf{N}$ выполняется $0 < g(x) \leq f(x)$. f, g-повторами будем называть повторы uvu с разрывом, удовлетворяющие условию $g(|u|) \leq |v| \leq f(|u|)$. Например, α-повторы с разрывами являются частным случаем f, g-повторов для $g(x) = \min\{1, \alpha - 1\}$, $f(x) = (\alpha - 1)x$. f, g-повторы впервые рассматривались в работе [20], в которой предложен алгоритм поиска всех максимальных f, g-повторов в слове длины n за время $O(n \log n + S)$, где S — число таких повторов в слове. Для частного случая $f(x) = g(x) = d$ в [21] предложен алгоритм поиска всех f, g-повторов в слове длины n за время $O(n \log d + S)$. Таким образом, получение оценок для максимального возможного числа f, g-повторов в слове заданной длины является важным для оценки эффективности алгоритмов поиска f, g-повторов в заданном слове.

Пусть $f(x)$ — функция из $\mathbf{N}$ в $\mathbf{R}$. Для каждого $x \in \mathbf{N}$ положим $\partial_f^+(x) = (f(x+1) - f(x))$, если $f(x+1) \geq f(x)$, и $\partial_f^+(x) = 0$ в противном случае. Положим также $\partial_f^-(x) = (f(x) - f(x+1))$, если $f(x) \geq f(x+1)$, и $\partial_f^-(x) = 0$ в противном случае. Обозначим через ∂_f^+ (∂_f^-) супремум $\sup_x\{\partial_f^+(x)\}$ ($\sup_x\{\partial_f^-(x)\}$), если этот супремум существует. Пусть $f(x)$, $g(x)$ — две функции из $\mathbf{N}$ в $\mathbf{R}$ такие, что $f(x) \geq g(x)$ для любого $x \in \mathbf{N}$. Если обе величины ∂_f^+ и ∂_g^- существуют, обозначим $\max\{\partial_f^+, \partial_g^-\}$ через $\partial_{f,g}^a$. Если обе величины ∂_f^- и ∂_g^+ существуют,

обозначим $\max\{\partial_f^-, \partial_g^+\}$ через $\partial_{f,g}^b$. Пусть хотя бы одна из величин $\partial_{f,g}^a$, $\partial_{f,g}^b$ существует. Тогда определим $\partial_{f,g}$ как $\min\{\partial_{f,g}^a, \partial_{f,g}^b\}$ если обе величины $\partial_{f,g}^a$, $\partial_{f,g}^b$ существуют; в противном случае, т.е. если существует только одна из величин $\partial_{f,g}^a$, $\partial_{f,g}^b$, положим $\partial_{f,g}$ равным этой величине. Положим также $\Delta_{f,g}(x) = \frac{1}{x}(f(x) - g(x)) \geq 0$ для каждого $x \in \mathbf{N}$ и $\Delta_{f,g} = \sup_x\{\Delta_{f,g}(x)\}$, если этот супремум существует.

Теорема. *Пусть для функций $f(x)$, $g(x)$ существуют обе величины $\partial_{f,g}$, $\Delta_{f,g}$. Тогда в слове длины n содержится не более чем $O(n(1 + \max\{\partial_{f,g}, \Delta_{f,g}\}))$ максимальных f,g-повторов.*

Другим классическим примером регулярных фрагментов являются палиндромы. Палиндромом называется слово $w = a_1a_2\dots a_n$, совпадающее со словом $w^R = a_na_{n-1}\dots a_1$. Аналогично квадратам, палиндромы обобщаются на случай палиндромов с разрывами. Под палиндромом с разрывом в слове понимается фрагмент вида uvu^R, где u, u^R — непустые слова, называемые рукавами палиндрома, а v — непустое слово, называемое разрывом палиндрома. Палиндром с разрывом в слове называется максимальным, если выполняются следующие два условия:

1) если палиндром не является ни префиксом, ни суффиксом слова, то символ, предшествующий в слове левому рукаву палиндрома, отличен от символа, следующего за его правым рукавом;

2) символ, следующий в слове за левым рукавом палиндрома, отличен от символа, предшествующего его правому рукаву.

Другими словами, палиндром с разрывом является максимальным, если его рукава не могут быть расширены ни на один символ ни влево, ни вправо. Аналогично понятию α-повтора с разрывом, при $\alpha > 1$ палиндром uvu^R с разрывом называется α-палиндромом, если $|u| + |v| \leq \alpha|u|$. Несложно заметить, что любой α-палиндром с разрывом однозначным образом расширяется либо до некоторого палиндрома, либо до некоторого максимального α-палиндрома в разрывом. Поэтому, с учетом возможности эффективного поиска палиндромов в словах с помощью уже известных алгоритмов [22, 23], задача эффективного поиска α-палиндромов в слове сводится к задаче поиска всех максимальных α-палиндромов. Исходя из соображений симметрии, методы, предложенные в [18, 19] могут быть легко модифицированы для того, чтобы показать, что в слове длины n

содержится $O(\alpha n)$ максимальных α-палиндромов (в частности, с помощью методов, предложенных в [19], можно показать, что в слове длины n содержится не более чем $28\alpha n + 7n$ максимальных α-палиндромов) и в слове длины n над полиномиально ограниченным алфавитом все максимальные α-палиндромы могут быть найдены за время $\Theta(\alpha n)$.

Работа выполнена при поддержке РФФИ, проект № 14-01-00598.

Список литературы

1. Crochemore M. An optimal algorithm for computing the repetitions in a word // Information Processing Letters. — 1981. — T. 12. — C. 244–250.

2. Crochemore M. Recherche lineare d'un carre dans un mot // Comptes Rendus Acad. Sci. Paris Ser. I Math. — 1983. — V. 296. — P. 781–784.

3. Main M., Lorentz R. Linear time recognition of square free strings // Combinatorial Algorithms on Words, NATO Advanced Science Institutes, Series F. — 1985. — V. 12. — P. 271–278.

4. Gusfield D., Stoye J. Linear time algorithms for finding and representing all the tandem repeats in a string // Journal of Computer and System Sciences. — 2004. — V. 69. — N. 4. — P. 525–546.

5. Main M., Lorentz R. An $O(n \log n)$ algorithm for finding all repetitions in a string // Journal of Algorithms. — 1984. — V. 5. — N. 3. — P. 422–432.

6. Kolpakov R., Kucherov G. On maximal repetitions in words // Journal of Discrete Algorithms. — 2000. — V. 1. — N. 1. — P. 159–186.

7. Crochemore M., Ilie L., Smyth W. A simple algorithm for computing the Lempel-Ziv factorization // Proceedings of Data Compression Conference (DCC 2008), IEEE Computer Society. — 2008. — P. 482–488.

8. Kosolobov D. Computing runs on a general alphabet // Information Processing Letters. — 2016. — V. 116. — N. 3. — P. 241–244.

9. Gawrychowski P., Kociumaka T., Rytter W., Walen T. Faster longest common extension queries in strings over general alphabets // Proceedings of 27th Annual Symposium on Combinatorial Pattern Matching (CPM'16), LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. — 2016. — V. 54. — P. 5:1–5:13.

10. Breslauer D. Efficient string algorithmics // PhD thesis, Columbia University. — 1992.

11. Crochemore M., Iliopoulos C., Kociumaka T., Kundu R., Pissis S., Radoszewski J., Rytter W., Walen T. Near-optimal computation of runs over general alphabet via non-crossing LCE queries // CoRR, abs/ 1606. 08275. — 2016.

12. Bannai H., I T., Inenaga S., Nakashima Y., Takeda M., Tsuruta K. A new characterization of maximal repetitions by Lyndon trees // CoRR, abs/1406.0263. — 2014.

13. Fischer J., Holub S., I T., Lewenstein M. Beyond the runs theorem // Lecture Notes in Computer Science. — 2015. — V. 9309. — P. 277–286.

14. Kolpakov R., Podolskiy M., Posypkin M., Khrapov N. Searching of gapped repeats and subrepetitions in a word // Lecture Notes in Computer Science. — 2014. — V. 8486. — P. 212–221.

15. Badkobeh G., Crochemore M., Toopsuwan C. Computing the maximal-exponent repeats of an overlap-free string in linear time // Lecture Notes in Computer Science. — 2012. — V. 7608. — P. 61–72.

16. Tanimura Y., Fujishige Y., I T., Inenaga S., Bannai H., Takeda M. A faster algorithm for computing maximal α-gapped repeats in a string // Lecture Notes in Computer Science. — 2015. — V. 9309. — P. 124–136.

17. Gawrychowski P., Manea F. Longest α-gapped repeat and palindrome // Lecture Notes in Computer Science. — 2015. — V. 9210. — P. 27–40.

18. Crochemore M., Kolpakov R., Kucherov G. Optimal bounds for computing α-gapped repeats // Lecture Notes in Computer Science. — 2016. — V. 9618. — P. 245–255.

19. Gawrychowski P., I T., Inenaga S., Koppl D., Manea F. Efficiently finding all maximal α-gapped repeats // Proceedings of 33rd Symposium on Theoretical Aspects of Computer Science (STACS 2016). — 2016. — P. 39:1–39:14.

20. Brodal G., Lyngso R., Pedersen C., Stoye J. Finding maximal pairs with bounded gap // Journal of Discrete Algorithms. — 2000. — V. 1. — N 1. — P. 77–104.

21. Kolpakov R., Kucherov G. Finding repeats with fixed gap // Proceedings of 7th International Symposium on String Processing and Information Retrieval (SPIRE'00). — 2000. — P. 162–168.

22. Manacher G. A new linear-time "on-line" algorithm for finding the smallest initial palindrome of a string // Journal ACM. — 1975. — V. 22. — N 3. — P. 346–351.

23. Gusfield D. Algorithms on strings, trees, and sequences: computer science and computational biology. — Cambridge University Press, 1997.

Секция «Синтез, сложность и надежность управляющих систем»

О k-ЗНАЧНЫХ ФУНКЦИЯХ СПЕЦИАЛЬНОГО КЛАССА

М. А. Алехина (Пенза)

Пусть $k, n \in \mathbf{N}$, $k \geq 3$, $E_k = \{0, 1, ..., k-1\}$, а P_k — множество всех функций k-значной логики, то есть функций $f(x_1, ..., x_n) : (E_k)^n \to E_k$. Рассмотрим реализацию функций из множества P_k схемами из ненадежных функциональных элементов в произвольном полном конечном базисе B.

Будем считать, что схема из ненадежных элементов реализует функцию $f(\tilde{x}^n)$ ($\tilde{x}^n = (x_1, ..., x_n)$), если при поступлении на входы схемы набора $\tilde{a}^n$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a}^n)$.

Предполагается, что все базисные элементы ненадежны, переходят в неисправные состояния независимо друг от друга, а сами неисправности могут быть произвольными (например, инверсными или константными).

Пусть схема S реализует функцию $f(\tilde{x}^n)$, $\tilde{a}^n$ — произвольный входной набор схемы S, $f(\tilde{a}^n) = \tau$. Обозначим через $P_i(S, \tilde{a}^n)$ вероятность появления значения i ($i \in E_k$) на выходе схемы S при входном наборе $\tilde{a}^n$, а через $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)$ — вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}^n$. Ясно, что $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n) = P_{\tau+1}(S, \tilde{a}^n) + P_{\tau+2}(S, \tilde{a}^n) + ... + P_{\tau+k-1}(S, \tilde{a}^n)$. (В выражениях $\tau + 1$, $\tau + 2$,..., $\tau + k - 1$ сложение осуществляется по модулю k.)

Ненадежностью схемы S, реализующей функцию $f(\tilde{x}^n)$, будем называть число $P(S)$, равное наибольшей из вероятностей появления ошибки на выходе схемы S. *Надежность* схемы S равна $1 - P(S)$.

Пусть $\tilde{\alpha}^m$, $\tilde{\beta}^m$ — наборы с компонентами из множества E_k длины m ($m \geq 3$). Обозначим через $\rho(\tilde{\alpha}^m, \tilde{\beta}^m)$ число координат, в которых наборы $\tilde{\alpha}^m$ и $\tilde{\beta}^m$ различаются.

Пусть для функции $g(\tilde{x}^m)$ существуют такие различные наборы $\tilde{\alpha}_1^m$, $\tilde{\alpha}_2^m, ..., \tilde{\alpha}_k^m$, что:

1) значения $g(\tilde{\alpha}_i^m)$ и $g(\tilde{\alpha}_j^m)$ попарно различны при $i \neq j$ $(i, j \in \{1, 2, ..., k\})$;
2) при всех допустимых значениях i и любого набора $\tilde{\alpha}^m$ такого, что $\rho(\tilde{\alpha}^m, \tilde{\alpha}_i^m) \leq 1$, верно равенство $g(\tilde{\alpha}^m) = g(\tilde{\alpha}_i^m)$.

Наборы $\tilde{\alpha}_1^m,\ \tilde{\alpha}_2^m, ...,\ \tilde{\alpha}_k^m$ будем называть *характеристическими* наборами функции $g(\tilde{x}^m)$.

Замечание. *Если $\tilde{\alpha}_1^m,\ \tilde{\alpha}_2^m, ...,\ \tilde{\alpha}_k^m$ — характеристические наборы функции $g(\tilde{x}^m)$, то любые два из них отличаются не менее чем в трех координатах.*

Пример. Нетрудно проверить, что:

1) функция $g_1(\tilde{x}^4) = \max\{\min(x_1, x_2), \min(x_3, x_4)\}$ лежит в G, а $(0000), (1111), ..., (k-1, k-1, k-1, k-1)$ — ее характеристические наборы;

2) функция $g_2(\tilde{x}^3) = x_1 + x_2 + x_3 \pmod k$ не лежит в G.

Обозначим через G_m множество функций $g(\tilde{x}^m)$ с перечисленными свойствами. Пусть

$$G = \bigcup_{m=3}^{\infty} G_m$$

.

Теорема 1. *Для числа $|G_m|$ функций из множества G_m справедливы неравенства*

$$k^{k^m - k^2 m + (k+1)m - k} \prod_{i=1}^{k-1} (k^m - ia) \leq |G_m| \leq k^{k^m - k^2 m + 2mk - k},$$

где $a = (k-1)m + 1 + C_m^2 (k-1)^2$.

В теореме 2 получено рекуррентное соотношение для ненадежностей исходной схемы и новой схемы S, построенной с использованием схемы S_g, реализующей функцию $g(\tilde{x}^m) \in G$.

Теорема 2. *Предположим, что любую функцию $f \in P_k$ можно реализовать схемой с ненадежностью не больше p. Пусть $g(\tilde{x}^m) \in G$, $\tilde{\alpha}_1^m,\ \tilde{\alpha}_2^m, ...,\ \tilde{\alpha}_k^m$ — ее характеристические наборы, причем $g(\tilde{\alpha}_1^m) = 0,\ g(\tilde{\alpha}_2^m) = 1, ...,\ g(\tilde{\alpha}_k^m) = k-1$. Пусть схема S_g реализует функцию $g(\tilde{x}^m) \in G$ с ненадежностью $P(S_g)$, а $v^0,\ v^1, ...,\ v^{k-1}$ — вероятности ошибок схемы S_g на характеристических наборах $\tilde{\alpha}_1^m,\ \tilde{\alpha}_2^m, ...,\ \tilde{\alpha}_k^m$ соответственно. Тогда функцию f можно реализовать такой схемой S, что $P(S) \leq \max\{v^0,\ v^1, ...,\ v^{k-1}\} + mpP(S_g) + (2^m - m - 1)p^2$.*

Доказательства теорем 1 и 2 можно найти в работе [3] $(k \geq 3)$.

Таким образом, описаны свойства функций, схемы которых можно использовать для повышения надежности схем, а также приведены оценки (снизу и сверху) для числа таких функций.

В списке литературы приведены работы, в которых ранее были описаны аналогичные свойства функций при $k = 2$ [1], $k = 3$ [4] и $k = 4$ [2]. Отметим, что при $k = 2$ для повышения надежности неветвящихся программ с оператором условной остановки также используются неветвящиеся программы, реализующие булевы функции с описанными свойствами [5].

Исследование выполнено при финансовой поддержке РФФИ (проект 14-01-00273).

Список литературы

1. Alekhina M. A. Synthesis and complexity of asymptotically optimal circuits with unreliable gates // Fundamenta Informaticae. — 2010. — 104(3). — P. 219–225.

2. Алехина М. А., Каргин С. П. О синтезе схем из ненадежных элементов в P_4 // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2014. — №4 — С. 47–56.

3. Алехина М. А. Синтез схем из ненадежных элементов в P_k // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — №3 — С. 8–10.

4. Алехина М. А., Барсукова О. Ю. О надежности схем, реализующих функции трехзначной логики // Дискретный анализ и исследование операций. — 2014. — Т. 21. вып. 4. — С. 12–24.

5. Грабовская С. М. Асимптотически оптимальные по надежности неветвящиеся программы с оператором условной остановки // Дис. канд. физ.-мат. наук. — Пенза, 2012. — 89 с.

О СЛОЖНОСТИ ПРОВЕРКИ РАВЕНСТВА ПОЛИНОМОВ, ПОЛЯРИЗОВАННЫХ ПО РАЗНЫМ ВЕКТОРАМ

А. В. Бухман (Москва)

Определение. Пусть $E_2 = \{0, 1\}$. *Булевой функцией* от n переменных будем называть любое отображение $f : E_2^n \to E_2$.

Определение. *Элементарной конъюнкцией* (ЭК) над переменными $x_1, \ldots, x_n$ будем называть выражение вида $x_{i_1}^{\sigma_1} \ldots x_{i_s}^{\sigma_s}$, где

$x^0 = x, x^1 = \bar{x}$, а коэффициенты $i_1, \ldots, i_s$ попарно различны. Элементарные конъюнкции, отличающиеся только порядком переменных будем считать равными.

Определение. *Обобщённым полиномом* назовём сумму по модулю 2 конечного числа различных элементарных конъюнкций. Если каждая переменная входит в обобщённый полином только с отрицанием или только без отрицания, то такой полином называют *поляризованным*. Для поляризованного полинома от n переменных введём понятие *вектора поляризации*. Пусть переменная x_i входит в запись поляризованного полинома только с отрицанием, тогда положим $\alpha_i = 1$, если эта переменная входит только без отрицания, то положим $\alpha_i = 0$. Вектор $(\alpha_1, \ldots, \alpha_n)$ назовём вектором поляризации полинома.

Заметим, что полином Жегалкина является поляризованным полиномом, у которого вектор поляризации равен $(0, \ldots, 0)$.

Рассмотрим следующую задачу **(1)**: на вход подаются два поляризованных полинома, с разными векторами поляризации. Нужно проверить, будут ли эти полиномы задавать одинаковые функции.

Данная задача является обобщением задачи проверки чётности функции [1] и задачи проверки периодичности функции [2].

Для оценки сложности алгоритма введём алгоритмическую модель. В качестве вычислителя будем рассматривать PAM машину, которая описана в [3]. Ей на вход будут подаваться записи двух полиномов. Таким образом, если длина первого полинома была l_1, а второго l_2, то длина входного слова будет $N = n(l_1 + l_2)$, где n — число переменных от которых зависят функции. Под сложностью алгоритма будем понимать время его работы (количество тактов работы PAM машины) в худшем случае на всех входах длины N.

Отметим, что в такой постановке задачи тривиальная проверка равенства полиномов как функций займёт в общем случае экспоненциальное время. Другой очевидный способ решить эту задачу — это сложить два полинома, заменить все вхождения $\bar{x}$ на $x \oplus 1$, раскрыть скобки привести подобные слагаемые и проверить равенство полинома 0. Но и в этом случае можно подобрать полиномы и вектора поляризации так, что сложность будет экспоненциально зависеть от входа. В данной работе показано существование полиномиального алгоритма.

Для начала упростим задачу. Пусть на вход даны полином P_1, поляризованный по вектору τ и полином P_2, поляризованный по вектору σ. Если в первом полиноме формально заменить все $x_i^{\tau_i}$ на $x_i^{\tau_i \oplus \sigma_i}$, то получим новый полином P_1' поляризованный по вектору $(\tau_1 \oplus \sigma_1, \ldots, \tau_n \oplus \sigma_n)$. В полиноме P_2 просто уберем отрицания у

всех переменных, получим полином Жегалкина P_2'. Функции, задаваемые полиномами P_1, P_2 равны тогда и только тогда, когда равны функции, задаваемые полиномами P_1', P_2'. Таким образом можно упростить исходную задачу **(1)** до следующей задачи **(2)**: на вход подаётся поляризованный полином и полином Жегалкина, проверить задают ли они равные функции.

Идея построения полиномиального алгоритма состоит в ограничении перебора. Рассмотрим вспомогательную лемму.

Лемма. *Пусть поляризованный полином P_1 и полином Жегалкина P_2 задают равные функции. Пусть K — произвольное слагаемое полинома P_1, заменим в K все переменные с отрицанием $\bar{x}_i$ на $x_i \oplus 1$, раскроем скобки приведём подобные слагаемые, получим полином Жегалкина P_K. Тогда верно, что $l(P_K) \leq l(P_1) + l(P_2)$, где $l(P)$ — длина полинома P.*

Теорема. *Существует PAM машина, которая, получив на вход записи двух поляризованных (по различным векторам) полиномов, проверяет, задают ли эти полиномы одинаковые функции. Причём время работы данной машины $O(N^3)$, где $N = n(l_1 + l_2)$ — длина записи входного слова.*

Идея алгоритма состоит в следующем. Сначала преобразуем входные полиномы, чтобы свести задачу **(1)** к задаче **(2)**. Далее для каждого слагаемого поляризованного полинома делаем замену $\bar{x}_i = x_i \oplus 1$. Если длина нового полинома будет больше суммы длин исходных полиномов, то по лемме функции не могут быть равны, и алгоритм выда т ответ — НЕТ. Иначе мы можем раскрыть скобки и получим новый полином, длина которого есть $O(N)$. Проверяем его на равенство 0. Сложность такой проверки потребует $O(N^3)$ тактов работы машины.

Список литературы

1. Селезнева С. Н. О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина // Дискретная математика. — 1997. — Т. 9, вып. 5. — С. 24–31.

2. Бухман А. В. О свойствах полиномов периодических функций и сложности распознавания периодичности по полиному булевой функции // Дискретная математика. — 2014. — Т. 11, вып. 3. — С. 129–137.

3. Гэри М. Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

КВАНТОВОЕ ХЕШИРОВАНИЕ ДЛЯ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

А. В. Васильев (Казань)

Данная работа посвящена обобщению предложенного нами ранее метода квантового хеширования. Предлагаемый подход позволяет конструировать квантовую хеш-функцию для произвольной конечной абелевой группы на основе ее неприводимых представлений. Учитывая необходимость обеспечения криптографических свойств квантового хеширования, предлагаемая нами функция оказывается асимптотически оптимальной по размеру получаемых квантовых хеш-кодов.

Как нами было показано ранее [1], основными свойствами квантовой криптографической хеш-функции являются эффективная вычислимость, устойчивость к восстановлению прообраза и устойчивость к коллизиям, причем все эти свойства тесно связаны.

В частности, свойства эффективной вычислимости и устойчивости к восстановлению прообраза часто объединяют в свойство односторонности — как и в классическом случае односторонняя функция должна быть эффективно вычислима, но сложна при восстановлении прообраза. В квантовом случае чаще всего прообраз и вовсе невозможно достоверно получить благодаря фундаментальному результату из области квантовой информации, известному как теорема Холево [2]. Из данной теоремы следует, что из s-кубитного состояния невозможно извлечь более $O(s)$ бит классической информации. Поэтому при построении квантовой хеш-функции требуется, чтобы размер получаемого квантового состояния был намного меньше (чаще всего экспоненциально меньше) исходного сообщения.

В данной работе предлагается обобщенная квантовая хеш-функция, основанная на так называемых множествах с ε-отклонением (в англоязычной литературе — ε-biased set). Данный комбинаторный объект имеет ряд важных приложений в различных областях, таких как дерандомизация, теория графов, теория чисел и т.д. Приведем его определение согласно [3].

Пусть G — это конечная абелева группа. Следовательно, ее неприводимые представления одномерны и совпадают с характерами. Обозначим их χ_a, пронумеровав элементами группы $a \in G$.

Определение. *Множество $B = \{b_1, b_2, \ldots, b_d\} \subseteq G$ называется множеством с ε-отклонением, если для любого нетривиального*

характера χ_a *выполняется неравенство*

$$\frac{1}{|B|}\left|\sum_{j=1}^{|B|}\chi_a(b_j)\right| \leq \varepsilon.$$

Как было доказано в [4], существует такое множество с ε-отклонением, что его размер имеет порядок $O\left(\frac{\log|G|}{\varepsilon^2}\right)$, а в статье [3] приводится явная конструкция такого множества.

Для дальнейших построений зафиксируем $\varepsilon \in (0,1)$ и положим, что $B \subseteq G$ является множеством с ε-отклонением размера $O\left(\frac{\log|G|}{\varepsilon^2}\right)$.

Определение. *Классически-квантовой будем называть функцию, значениями которой являются единичные векторы из пространства* $(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \cdots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}$ *—* 2^s*-мерного гильбертова пространства, описывающего состояния* s *квантовых бит.*

Определение. *Определим классически-квантовую функцию* $\psi_B : G \to (\mathcal{H}^2)^{\otimes \log|B|}$ *следующим образом:*

$$|\psi_B(a)\rangle = \frac{1}{\sqrt{|B|}}\sum_{j=1}^{|B|}\chi_a(b_j)\,|j\rangle.$$

Теорема. *Функция* ψ_B *является криптографической квантовой хеш-функцией.*

Доказательство. Докажем наличие у ψ_B свойств квантовой криптографической хеш-функции [1].

Устойчивость к коллизиям. Согласно определению устойчивости к квантовых коллизиям [1] необходимо доказать ограниченность значения скалярного произведения различных образов функции ψ_B.

Пусть $a_1, a_2 \in G$, $a_1 \neq a_2$. Тогда $\chi_{a_1}(x), \chi_{a_2}(x)$ являются различными характерами G. $\chi^*_{a_1}(x)$ также является характером G, как и функция $\chi(x) = \chi^*_{a_1}(x)\chi_{a_2}(x)$.

$\chi(x)$ является нетривиальным характером G, поскольку $\chi_{a_1}(x) \not\equiv \chi_{a_2}(x)$ и $\chi(x) = \chi^*_{a_1}(x)\chi_{a_2}(x) \not\equiv \chi^*_{a_1}(x)\chi_{a_1}(x) \equiv \mathbf{1}$, где $\mathbf{1}$ обозначает тривиальный характер G.

Поскольку B является множеством с ε-отклонением, получаем

$$|\langle\psi_B(a_1)\,|\,\psi_B(a_2)\rangle| = \frac{1}{|B|}\left|\sum_{j=1}^{|B|}\chi^*_{a_1}(b_j)\chi_{a_2}(b_j)\right| = \frac{1}{|B|}\left|\sum_{j=1}^{|B|}\chi(b_j)\right| \leq \varepsilon.$$

Устойчивость к восстановлению прообраза. Необратимость функции ψ_B следует теоремы Холево [2], поскольку по построению размер образа ψ_B равен $\log|B|$. При этом согласно [4] существует множество с ε-отклонением B размера $O\left(\frac{\log|G|}{\varepsilon^2}\right)$. Следовательно, в таком случае размер образа ψ_B равен $\log|B| = O(\log\log|G| - \log\varepsilon)$, и эта же оценка справедлива для количества информации о прообразе, которую можно извлечь из такого квантового состояния.

Эффективная вычислимость. Эффективная вычислимость следует из размера образа квантовой хеш-функции, который экспоненциально меньше размера исходных данных. Известно, что произвольный квантовый алгоритм на q кубитах представим в виде последовательности $O(q^2 4^q)$ базисных операций. Поскольку $q = \log|B| = O(\log\log|G| - \log\varepsilon)$, время вычисления квантовой хеш-функции полиномиально зависит от длины входных данных.

Работа выполнена при финансовой поддержке РФФИ (проекты 14-07-00878, 15-37-21160).

Список литературы

1. Ablayev F. M., Vasiliev A. V. Cryptographic quantum hashing // Laser Physics Letters. — 2014. — Vol. 11, I. 2. — P. 025202.

2. Holevo A. S. Some estimates of the information transmitted by quantum communication channel (russian) // Probl. Pered. Inform. [Probl. Inf. Transm.]. — 1973. — Vol. 9, I. 3. — P. 3–11.

3. Chen S., Moore C., Russell A. Small-bias sets for nonabelian groups // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. — 2013. — Vol. 8096. — P. 436–451.

4. Alon N., Roichman Y. Random Cayley graphs and expanders // Random Structures & Algorithms. — 1994. — Vol. 5, I. 2. — P. 271–284.

ВЫЧИСЛИТЕЛЬНАЯ МОЩЬ КОНЕЧНЫХ АВТОМАТОВ, РЕШАЮЩИХ УНАРНЫЕ ЗАДАЧИ ОТДЕЛИМОСТИ

А. Ф. Гайнутдинова (Казань)

Исследование сравнительной сложности квантовых и классических вычислительных моделей — актуальное направление математической кибернетики. Конечные автоматы являются одной из простейших моделей, для которой известно следующее: вероятностные конечные автоматы (ВКА) с ограниченной ошибкой распознают в

точности класс регулярных языков, квантовые конечные автоматы (ККА), использующие единственное измерение в конце вычислений, распознают собственное подмножество регулярных языков. Также известно, что число состояний как ВКА, так и ККА не может быть меньше по порядку чем логарифм от числа состояний минимального детерминированного автомата (ДКА), распознающего тот же язык.

Задача отделимости двух непересекающихся языков является обобщением задачи распознавания языков, когда вместо задачи отделения множества L слов языка от его дополнения $\Sigma^* \setminus L$ решается задача отделения множеств слов двух непересекающихся языков L и L', при этом $L \cup L' \neq \Sigma^*$ в общем случае [1]. Мы показываем, что при решении задач отделимости 1) ККА решают больший класс задач, чем ВКА и ДКА; 2) ККА и ВКА демонстрируют большую эффективность, чем при распознавании языков.

Приведем необходимые определения. ВКА $\mathcal{P} = (S, \Sigma, \{M_\sigma \mid \sigma \in \Sigma\}, \mu_0, Acc)$, где S, Σ — конечные множество состояний и входной алфавит, μ_0 — $|S|$-мерный стохастический вектор начального распределения вероятностей состояний автомата, $M_\sigma(\sigma \in \Sigma)$ — стохастические по столбцам $|S| \times |S|$-матрицы, где $M_\sigma(j,i)$ — вероятность перехода автомата из состояния s_i в s_j при считывании символа σ, $Acc \subseteq S$ множество принимающих состояний.

На входе $w = w_1 \dots w_n \in \Sigma^*$ автомат начинает работу с распределения μ_0, на каждом шаге j $(j = 1, \dots, n)$ считывает очередную букву и преобразует вектор распределения состояний: $\mu_j = A_{w_j}\mu_{j-1}$, Вероятность принятия входного слова определяется по финальному вектору $\mu_{|w|}$ как $Pr^{\mathcal{P}}_{acc}(w) = \sum_{s_j \in Acc} \mu_{|w|}(j)$.

Если вектор μ_0 и матрицы $M_\sigma(\sigma \in \Sigma)$ содержат только нули и единицы, то в этом случае мы имеем определение ДКА. ДКА D принимает слово w, если он завершает обработку слова w в состоянии из множества Acc, в противном случае D отвергает w.

В литературе рассматриваются различные модели ККА. В работе мы исследуем модель “один раз измеряемых” ККА, впервые определенную в [2], которая использует унитарные преобразования на каждом вычислительном шаге и заключительное измерение в конце вычисления, как процедуру извлечения результата вычисления. ККА $\mathcal{M} = (S, \Sigma, \{U_\sigma \mid \sigma \in \Sigma\}, |\psi_0\rangle, Acc)$. Отличием от модели ВКА являются: $|\psi_0\rangle$ — d-мерный комплекснозначный вектор начального распределения амплитуд состояний автомата, при этом $|||\psi\rangle||_2 = 1$; $U_\sigma(\sigma \in \Sigma)$ — унитарные матрицы переходов, где $U_\sigma(j,i)$ — амплитуда перехода автомата из состояния s_i в s_j. Вероятность

принятия слова w определяется по финальному вектору $|\psi_n\rangle$ как $Pr^{\mathcal{M}}_{acc}(w) = \sum_{s_j \in Acc} ||\psi_{|w|}\rangle(j)|^2$.

Пусть имеются два языка L_{yes}, L_{no} ($L_{yes}, L_{no} \subseteq \Sigma^*, L_{yes} \cap L_{no} = \emptyset$). Будем говорить, что ДКА D отделяет язык L_{yes} от языка L_{no}, если он принимает все слова из L_{yes} и отвергает все слова из L_{no}. Будет говорить, что ВКА (ККА) M отделяет язык L_{yes} от языка L_{no} с ограниченной ошибкой, если существует ε ($0 \leq \varepsilon < 1/2$) такое, что M принимает все слова из L_{yes} с вероятностью $1-\varepsilon$ и отвергает все слова из L_{no} с вероятностью $1-\varepsilon$. В случае, если автомат принимает слова из L_{yes} с вероятностью 1 будем говорить, что автомат отделяет язык L_{yes} от языка L_{no} с односторонней ограниченной ошибкой ε.

Будем говорить, что автомат M решает задачу отделимости $L = (L_{yes}, L_{no})$, если он отделяет язык L_{yes} от языка L_{no}. Если Σ — унарный алфавит, то $L = (L_{yes}, L_{no})$ — унарная задача отделимости.

Следующий результат показывает, ККА решают больший класс задач отделимости, чем ВКА.

Пусть φ иррациональный угол, не кратный π. Для произвольного $\theta \in (0, \frac{\pi}{4})$ определим унарную задачу отделимости $\mathtt{L}^\theta = \{\mathtt{L}^\theta_{\mathtt{yes}}, \mathtt{L}^\theta_{\mathtt{no}}\}$:

- $\mathtt{L}^\theta_{\mathtt{yes}} = \{a^k \mid k\varphi \in [l\pi - \theta, l\pi + \theta]$ для некоторого $l \geq 0\}$,
- $\mathtt{L}^\theta_{\mathtt{no}} = \{a^k \mid k\varphi \in [l\pi + \frac{\pi}{2} - \theta, l\pi + \frac{\pi}{2} + \theta]$ для некоторого $l \geq 0\}$.

Теорема 1. *Существует ККА $\mathcal{M}$ с двумя состояниями, решающий задачу отделимости $\mathtt{L}^\theta$ с односторонней ограниченной ошибкой.*

Теорема 2. *Не существует ВКА, который решает задачу отделимости $\mathtt{L}^\theta$ с ограниченной ошибкой.*

Следующая серия результатов относится к сравнительной сложности ККА, ВКА и ДКА, решающих унарные задачи отделимости.

Для произвольного $n \in \mathbf{Z}^+$ определим семейство унарных задач отделимости $F_n = \{\mathtt{L}^{\mathtt{k,n}} \mid k \in \mathbf{Z}^+\}$ следующим образом. Обозначим через p_j j-ое по порядку простое число, через $P_{k,n} = \{p_n, p_{n+1}, \ldots, p_{n+k-1}\}$ множество простых чисел с n-го по $(n+k-1)$-ое, $N = p_n \cdot p_{n+1} \cdots p_{n+k-1}$. Определим задачу отделимости $\mathtt{L}^{\mathtt{k,n}} = \{\mathtt{L}^{\mathtt{k,n}}_{\mathtt{yes}}, \mathtt{L}^{\mathtt{k,n}}_{\mathtt{no}}\}$:

- $\mathtt{L}^{\mathtt{k,n}}_{\mathtt{yes}} = \{a^m \mid m \equiv 0 \pmod N\}$,
- $\mathtt{L}^{\mathtt{k,n}}_{\mathtt{no}} = \{a^m \mid m \pmod p)_j \in \left[\frac{p_j}{8}, \frac{3p_j}{8}\right] \cup \left[\frac{5p_j}{8}, \frac{7p_j}{8}\right]$ для более чем $\frac{2k}{3}$ различных p_j из множества $P_{k,n}\}$.

Используя китайскую теорему об остатках можно показать, что как $\mathtt{L}^{\mathtt{k,n}}_{\mathtt{yes}}$, так и $\mathtt{L}^{\mathtt{k,n}}_{\mathtt{no}}$ содержат бесконечное множество слов.

Теорема 3. *Для произвольного $n \in \mathbf{Z}^+$ существует ККА, имеющий $2k$ состояний, который решает задачу отделимости $\mathtt{L}^{\mathtt{k,n}}$ с односторонней ограниченной ошибкой $\frac{1}{3}$.*

Теорема 4. *Любой ВКА, решающий задачу отделимости $\mathtt{L}^{\mathtt{k,n}}$ с ограниченной ошибкой, имеет $\Omega(k(n+k)\log n)$ состояний.*

Теорема 5. *Для любого $n > 0$ существует ВКА $\mathcal{P}_{k,n}$ с $O(k(n+k)\log(n+k))$ состояниями, решающий задачу отделимости $\mathtt{L}^{\mathtt{k,n}}$ с односторонней ограниченной ошибкой $\frac{1}{3}$.*

Теорема 6. *Для любого $n > 0$ любой ДКА, решающий задачу отделимости $\mathtt{L}^{\mathtt{k,n}}$, имеет $\Omega(n\log(n))^{\frac{k}{3}}$ состояний.*

Теорема 7. *Для любого $n > 0$ существует ДКА $\mathcal{D}_{k,n}$, имеющий $O((n+\frac{k}{3})\log(n+\frac{k}{3}))^{\frac{k}{3}}$ состояний, который решает задачу отделимости $L^{k,n} \in F_n$.*

Доказанные оценки для ВКА и ДКА являются почти точными. При выборе $n = 2^k$ мы имеем экспоненциальное преимущество как ККА над ВКА, так и ВКА над ДКА.

Список литературы

1. Трахтенброт Б. А., Барздинь Я. М. Конечные автоматы. Поведение и синтез. — М.: Наука, 1970.

2. Moore C., Crutchfield J. P. Quantum Automata and Quantum Grammars // Theoretical Computer Science. — 2000. — 237 (1–2) — P. 275–306.

О РЕАЛИЗАЦИИ МУЛЬТИПЛЕКСОРНОЙ ФУНКЦИИ СХЕМАМИ КОНТАКТНОГО ТИПА, ВЛОЖЕННЫМИ В ЕДИНИЧНЫЕ КУБЫ

Е. Л. Довгалюк (Москва)

В настоящее время распространенной моделью реализации функций алгебры логики (ФАЛ) являются различные схемы контактного типа. Во многих случаях для эффективного использования схем необходима их геометрическая реализация, то есть вложение в некоторую геометрическую структуру. В данной работе в качестве такой структуры используется единичный многомерный куб.

Рассмотрим так называемые гомеоморфные вложения некоторых графов в единичные кубы, при которых ребро вкладываемого графа может переходить в цепочку ребер того графа, в который происходит вложение, а также их модификации — квазигомеоморфные вложения.

В данной работе исследуется квазигомеоморфное вложение некоторых схем контактного типа, реализующих мультиплексорную функцию в единичный куб минимально возможной размерности.

Из ранее полученных в [1] результатов следует, что квазигомеоморфное вложение древовидной двоичной решающей диаграммы с "подводкой" переменных, реализующей мультиплексорную функцию от n переменных в единичный куб возможно при размерности куба, равной $n + 8$. В данной работе эта оценка была значительно улучшена и доведена до $n + 3$. Построено вложение контактной схемы, реализующей мультиплексорную функцию с асимптотически минимальной сложностью, которое оставляет свободными гораздо большее число вершин куба, чем при использовании древовидной BDD.

Определим основные понятия, связанные с реализацией ФАЛ и их гомеоморфными вложениями в единичный куб (те понятия, которые в данной работе не определяются, см., например, в [2]).

Определение. *Двоичная решающая диаграмма* (*BDD*) *от БП* $x = (x_1, \ldots, x_n)$ — это ориентированный ациклический граф $\Sigma = \Sigma(x)$ с одним истоком, в котором каждому стоку приписывается либо 0, либо 1, а каждой вершине, отличной от стока, приписывается БП x_i, $i \in \{1, \ldots, n\}$, и предполагается, что из такой вершины выходит 2 ребра, одно из которых помечено символом 0, а другое — символом 1.

При этом BDD, в которых вершины, соответствующие выходным значениям 0, сходятся к одному стоку, а все вершины, соответствующие выходным значениям 1 — к другому, будем называть 2-*BDD*.

Пусть $B = \{0, 1\}$ и B^n — единичный n-мерный куб.

Определение. *Мультиплексорная функция порядка* n — это функция вида

$$\mu_n(x_1, \ldots, x_n, y_0, \ldots, y_{2^n-1}) = \bigvee_{\alpha=(\alpha_1,\ldots,\alpha_n)\in B^n} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \cdot y_{\nu(\alpha)},$$

где первые n переменных называются адресными, оставшиеся 2^n — информационными, а значение функции равно значению той ее информационной переменной, номер которой поступил на адресные входы.

Реализуем мультиплексорную функцию с помощью древовидной BDD и древовидной 2-BDD Σ_n и $\hat{\Sigma}_n$ соответственно. Рассмотрим также реализующую ее асимптотически оптимальную по сложности контактную схему K_n, которая описана в [3].

Определение. *Подразбиением первого типа* графа G называется любой граф $\hat{G}$, получающийся из G в результате замены его ребер простыми цепями, которые не имеют общих внутренних вершин и не проходят через вершины графа G. При этом неориентированные (ориентированные) ребра заменяются цепями из неориентированных (соответственно, ориентированных в том же направлении) ребер.

Определение. *Гомеоморфным вложением графа G' в граф G''* называется отображение, задающее изоморфизм некоторого подразбиения первого типа $\hat{G}'$ графа G' на граф $\hat{G}''$ — основной подграф вложения, который либо является подграфом графа G'', либо может быть получен из такого подграфа в результате придания ориентации некоторой части его неориентированных ребер.

Определение. *Подразбиением второго типа* графа G называется любой граф $\hat{G}$, получающийся из G в результате замены его вершин связными графами, которые не имеют общих вершин и ребер как друг с другом, так и с графом G. При этом ребра графа G, ведущие в вершины, замененные связными графами, в новом графе ведут к любой вершине соответствующего графа.

Определение. *Квазигомеоморфным вложением графа G' в граф G''* называется отображение, задающее изоморфизм некоторого графа $\hat{G}'$, полученного с помощью применения подразбиений первого и второго типов к графу G', на граф $\hat{G}''$ (основной подграф), который либо является подграфом графа G'', либо может быть получен из него в результате придания ориентации некоторой части его неориентированных ребер.

Определение. *Квазигомеоморфным вложением BDD Σ в граф G'' с подводкой переменных* — это квазигомеоморфное вложение BDD Σ, при котором вершины, соответствующие переменнной x_i ($i \in \{1, \ldots, n\}$) соединены неориентированными ребрами так, чтобы они образовывали связный неориентированный граф, не имеющий общих ребер с основным подграфом $\hat{G}''$.

Пусть $R(G)$ — минимальная размерность единичного куба, допускающего квазигомеоморфное вложение некоторого графа G, а $\hat{R}(\Sigma)$ — минимальная размерность единичного куба, допускающего квазигомеоморфное вложение с подводкой переменных некоторой BDD Σ.

Справедливы следующие утверждения:

Теорема 1. *Для любого* $n > 2$ *выполняется равенство* $\hat{R}(\Sigma_n) = n + 3$.

Теорема 2. *Для любого* $n > 2$ *выполняются неравенства:*

$$n + 2 \leqslant \hat{R}(\hat{\Sigma}_n) \leqslant n + 3.$$

Теорема 3. *Для любого* $n > 8$ *выполняется неравенство* $R(K_n) \leqslant n + 2$, *причем существует такое вложение в куб размерности* $n + 2$, *при котором остаются свободными* $2^n - 448$ *вершин куба.*

Список литературы

1. Седелев О. Б. О реализации функций алгебры логики схемами из функциональных элементов, вложенными в единичный куб // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2008. — № 1. — С. 44–50.

2. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел ВМК МГУ, 2004.

3. Власов Н. В. О сложности мультиплексорных функций в некоторых классах схем. — Дисс. канд. физ.-мат. наук. — М.: 2013

ИЕРАРХИЯ ДЛЯ ДВУСТОРОННИХ ВЕРОЯТНОСТНЫХ АВТОМАТОВ

Р. Н. Ибрагимов (Казань)

В данной работе рассматривается известная модель — двусторонние вероятностные автоматы. В частности, рассматривается вопрос иерархии классов сложности по количеству состояний для вероятностной версии двусторонних неоднородных автоматов, описанных в работе [2]. С одной стороны, такая модель является близкой к модели $OBDD$, а с другой — вбирает специфику автоматов. В данной модели рассматривается вычисление булевой функции, по аналогии с моделью $OBDD$, это можно трактовать как вычисление характеристической функции языка, распознаваемого автоматом. Заметим, что ранее иерархии по количеству состояний для вероятностных моделей не рассматривались. В данной работе развиты подходы, примененные в работах [1, 3].

Полученные результаты. Определим классы языков, относительно которых будет построена иерархия.

Определение. $\mathsf{2PSIZE}(d)$ — класс языков, распознаваемых двусторонним неоднородным вероятностным автоматом размера d.

Был получен следующий результат .

Теорема 1. *Пусть* $d : \mathbb{N} \to \mathbb{N}$ *отличная от константы функция, такая что* $d^2(n) < n$. *Тогда* $\mathsf{2PSIZE}\left(\left\lfloor \frac{\sqrt{(d+9)}/13-2}{4(8+3\log t)} \right\rfloor\right) \subsetneq \mathsf{2PSIZE}\,(d)$.

Для доказательства теоремы используются свойства булевой функций Shuffled Address Function $\mathsf{2\text{-}SAF_w}$ [2]. Сначала представим необходимые условия представимости языка двусторонним автоматом.

Необходимое условие вычисления автоматом булевой функции. Рассмотрим булеву функцию $f = f(X)$ и разбиение $\pi = (X_A, X_B)$ переменных X. Для каждого фиксированного набора σ будем рассматривать отображение $\rho : X_A \to \sigma$. Подфункция $f|_\rho$ над переменными из множества X_B получается из функции f фиксированием переменных из множества X_A в соответствии с отображением ρ.

Обозначим за $N^\pi(f)$ количество различных подфункций, получаемых при рассмотрении всех возможных σ.

Рассмотрим множество Θ всех возможных перестановок чисел от 1 до n. Для $\theta = (j_1, ..., j_n)$ обозначим через $X^{\theta,u}$ множество переменных $(x_{j_1}, ..., x_{j_u})$.

Через $\Pi(\theta)$ обозначим множество разбиений $\Pi(\theta) = \{\pi : \pi = (X^{\theta,u}, X \setminus X^{\theta,u})\}$, где $1 \le u \le n$.

Определение. *Количеством подфункций* для порядка $\theta \in \Theta$ для булевой функции f назовем величину $N^\theta(f) = \max_{\pi\in\Pi(\theta)} N^\pi(f)$.

Заметим, что если $id = (1, ..., n)$ и f — характеристическая фукнция языка L, то величина $N^{id}(f)$ совпадает с рангом языка L (количеством классов эквивалентности отношения $\equiv_L$).

Свойства функции $\mathsf{2\text{-}SAF_w}$.

Лемма 1 [2]. *Для целого* $w = w(n)$, *удовлетворяещего неравенству* $2w(2w + \lceil \log 2w \rceil) < n$, *выполняется неравенство* $N(\mathsf{2\text{-}SAF_w}) \ge w^{w-2}$.

Лемма 2 [2]. *Существует* $2KA$ A *размера* $13w+4$, *распознающий язык, характеристической функцией которого является функция* $\mathsf{2\text{-}SAF_w}$.

Матричное представление 2BA. Пусть L — язык, распознаваемый двусторонним вероятностным автоматом A, а $f(x)$ — характеристическая функция языка L. Для оценки количества подфункций функции $f(x)$ воспользуемся коммуникационным подходом представления работы автомата.

Определим матрицу $M_A(\sigma,\gamma)$, описывающую работу автомата A на входном слове $v=(\sigma,\gamma)$ в соответствии с разбиением π:

$$M_A(\sigma,\gamma)=\left[\begin{array}{cc|c} 0 & & M_A(\sigma) \\ \hline 0 & I_2 & 0 \\ \hline M_A(\gamma) & & 0 \end{array}\right],$$

где I_2 — единичная 2×2 матрица; $M_A(\sigma)$ — $(d+1)\times d$ матрица, которая описывает работу автомата на σ (компонент (i,j) определяет вероятность перехода в конфигурацию b_{j+d+3} из конфигурации b_i раньше, чем в любую другую конфигурацию b_r, $r\geq d+3$); $M_A(\gamma)$ — $d\times(d+3)$ матрица, которая описывает работу автомата на γ (компонент (i,j) определяет вероятность перехода в конфигурацию b_j из конфигурации b_{i+d+3} раньше, чем в любую другую конфигурацию b_r, $r\leq d+3$).

Заметим, что сумма элементов в каждой строке матриц $M_A(\sigma)$ и $M_A(\gamma)$ равна единице.

Определение. Числа a и b называются β-близкими по модулю λ, если $a\leq\lambda$ и $b\leq\lambda$ или $\beta^{-1}\leq\frac{a}{b}\leq\beta$.

Лемма 3. *Пусть $\mathcal{M}$ — множество всех возможных попарно не $\beta-$ близких по модулю λ матриц размера $d\times d'$. Тогда $|\mathcal{M}|\leq\left\lceil\frac{-2\log\lambda}{\log\beta}\right\rceil^{d\cdot d'}$.*

Определение. Пусть P — марковская цепь. Обозначим вероятность попадания в поглощающее состояние через $a(P)$.

Определение. Пусть P — марковская цепь. Обозначим математическое ожидание числа шагов до попадания в поглощающее состояние через $t(P)$.

Лемма 4. *Пусть P, P' — две марковские цепи с m состояниями и $a(P)\geq\frac{1}{2}+\varepsilon$. Пусть $t=\max(t(P),t(P'),m)$, $\lambda=\frac{\varepsilon^2}{256t^3}$ и $\beta=\sqrt[2m]{\frac{1+\varepsilon+\varepsilon^2}{1+\varepsilon}}$. Тогда если P и P' β-близки по модулю λ, то $a(P')\geq\frac{1}{2}+\varepsilon/4$.*

Теорема 2. *Если язык L распознается $2BA$ A с ε-изолированной точкой сечения и математическим ожиданием числа шагов автомата t, то $N(f)\leq\left\lceil\frac{4d(8+3\log t)}{\log(1+2\varepsilon)(1+\varepsilon)}\right\rceil^{(d+1)^2}$.*

Используя приведенные верхние оценки и свойства функции $\mathsf{2\text{-}SAF_w}$, мы можем доказать теорему 1.

По лемме 1, лемме 2, теореме 2 получаем, что $\mathsf{2\text{-}SAF_d}\in\mathsf{2PSIZE}(13d+4)$ и $\mathsf{2\text{-}SAF_d}\notin\mathsf{2PSIZE}\left(\left\lfloor\frac{\sqrt{d+1}-2}{4(8+3\log t)}\right\rfloor\right)$.

Список литературы

1. Dwork C., Stockmeyer L. A time complexity gap for two-way probabilistic finite-state automata // SIAM Journal on Computing. — 19 (6). — 1990. — P. 1011–1023.

2. Khadiev K., Yakaryilmaz A. New size hierachies for two-way non-uniform automata // Sixth Workshop on Non-Classical Models of Automata and Applications (NCMA 2014) Short Papers. — 2014. — P. 13–18.

3. Хадиев К. Р., Ибрагимов Р. Н. Иерархия для двухсторонних детерменированных и недетерменированных автоматов // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г — М.: МАКС Пресс, 2015. — С. 252–254.

О ПОРЯДКЕ РОСТА МОЩНОСТИ ПЛОСКИХ СХЕМ ДЛЯ ЗАМКНУТЫХ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ

Г. В. Калачев (Москва)

Плоская схема — это схема из функциональных элементов, уложенная на плоскость так, чтобы каждому входу и выходу соответствовала некоторая сторона клетки, в которой находится элемент. Таким образом, в такой схеме могут использоваться любые функциональные элементы, у которых в сумме не более четырех контактов. Понятие плоской (клеточной) схемы ввел Кравцов С. С. в работе [1] и показал, что порядок площади плоских схем, реализующих булевы функции от n переменных, равен 2^n.

Мы в качестве меры сложности будем рассматривать максимальную, а также среднюю мощность схемы. Под мощностью схемы мы будем понимать электрическую мощность, потребляемую схемой (эта величина также называется активностью схемы). В работе [2] было показано, что порядок функции Шеннона мощности плоских схем, реализующих функции от n переменных, равен $2^{n/2}$.

В этой работе исследуется порядок функции Шеннона средней и максимальной мощности плоских схем для класса монотонных функций, и как следствие получаются порядки функции Шеннона для всех замкнутых классов.

Чтобы сформулировать результаты, введем несколько определений. Рассмотрим плоскую схему K, реализующую булеву функцию от n переменных. Входы схемы K, а также выходы всех ее элементов

назовем *узлами* схемы K. Функцию, реализуемую схемой K обозначим f_K.

Потенциалом схемы K *на наборе* x назовем количество узлов схемы K, принимающих значение 1, когда на вход схемы подан набор x. Будем обозначать эту величину $u_K(x)$. *Максимальным потенциалом* схемы K назовем величину $\widehat{U}(K) = \max\limits_{x\in\{0,1\}^n} u_K(x)$. *Максимальным потенциалом булевой функции* f назовём величину $\widehat{U}(f) = \min\limits_{K:f_K=f} \widehat{U}(K)$. *Средним потенциалом* схемы K назовём величину

$$U_P(K) = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} u_K(x).$$

Средним потенциалом булевой функции f назовём величину $U_P(f) = \min\limits_{K:f_K=f} U_P(K)$.

Введем функцию Шеннона для среднего и максимального потенциала функций из класса $\mathcal{F}$ от n переменных:

$$\widehat{U}_{\mathcal{F}}(n) = \max_{f\in\mathcal{F}\cap P_2(n)} \widehat{U}(f), \quad U_{\mathcal{F}}(n) = \max_{f\in\mathcal{F}\cap P_2(n)} U(f).$$

За M будем обозначать класс монотонных функций.

Теорема 1. *При* $n \to \infty$ *справедливы соотношения* $\widehat{U}_M(n) \asymp \frac{2^{n/2}}{\sqrt[4]{n}}$, $U_M(n) \asymp \frac{2^{n/2}}{n^{3/4}}$.

Здесь стоит отметить, что в отличие от P_2 для класса монотонных функций средняя и максимальная мощность отличаются по порядку.

Из результатов для класса монотонных функций и для P_2 можно получить порядок мощности для всех замкнутых классов. Чтобы сформулировать этот результат, разобьём все замкнутые классы на 4 множества.

$$\begin{aligned}
R =&\{P_2, T_0, T_1, T_{01}, S, S_{01}, I^\mu, I_1^\mu, I^\infty, I_1^\infty, O^\mu, O_0^\mu, O^\infty, O_0^\infty\};\\
R_M =&\{M, M_0, M_1, M_{01}, SM, MI^\mu, MI_1^\mu, MI^\infty, MI_1^\infty,\\
&\qquad MO^\mu, MO_0^\mu, MO^\infty, MO_0^\infty\};\\
R_L =&\{K, K_0, K_1, K_{01}, L, L_0, L_1, L_{01}, SL, D, D_0, D_1, D_{01}\};\\
R_C =&\{U, SU, MU, U_0, U_1, U_{01}, C, C_0, C_1\}.
\end{aligned}$$

Обозначения замкнутых классов взяты из [3].

Теорема 2. *Если* F *— замкнутый класс, то есть* 4 *случая.*

1. *Если* $F \in R$, *то* $\widehat{U}_F(n) \asymp U_F(n) \asymp 2^{n/2}$ *при* $n \to \infty$.

2. *Если* $F \in R_M$, *то* $\widehat{U}_F(n) \asymp \frac{2^{n/2}}{\sqrt[4]{n}}$, $U_F(n) \asymp \frac{2^{n/2}}{n^{3/4}}$ *при* $n \to \infty$.

3. *Если* $F \in R_L$, *то* $\widehat{U}_F(n) \asymp U_F(n) \asymp n$ *при* $n \to \infty$.

4. *Если* $F \in R_C$, *то* $\widehat{U}_F(n) \asymp U_F(n) = O(1)$.

Таким образом, все замкнутые классы делятся на 4 группы. Порядок мощности в любом замкнутом классе либо такой же, как в P_2, либо как в классе монотонных функций, либо линейный, либо константный.

Автор выражает искреннюю благодарность научному руководителю д.ф.-м.н., профессору Э. Э. Гасанову за постановку задачи и научное руководство.

Список литературы

1. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 285–293.

2. Калачев Г. В. Порядок мощности плоских схем, реализующих булевы функции // Дискретная математика. — 2014. — Т. 26, вып. 1. — С. 49–74.

3. Угольников А. Б. Классы Поста. Учебное пособие. — М.: Издательство ЦПИ при механико-математическом факультете МГУ им. М. В. Ломоносова, 2008.

О ТОЧНЫХ ЗНАЧЕНИЯХ СЛОЖНОСТИ ЧИСЕЛ ПРИ РЕАЛИЗАЦИИ СХЕМАМИ ИЗ ЕДИНИЧНЫХ СОПРОТИВЛЕНИЙ

О. М. Касим-Заде (Москва)

В данной работе рассматривается известная задача о синтезе идеализированных электрических схем наименьшей сложности из единичных сопротивлений. Имеется неограниченный запас электрических сопротивлений одинаковой величины, скажем, 1 Ом (единица измерения сопротивления не важна, далее опускаем ее наименование). Строятся двухполюсные схемы: выводы сопротивлений произвольным образом присоединяются друг к другу и к двум внешними зажимами — полюсам схемы; требуется создать между полюсами заданное сопротивление R. Сопротивление схемы отыскивают по известным формальным правилам электротехнических расчетов (законы Кирхгофа и Ома) [1].

Сопротивление всякой схемы из единичных сопротивлений выражается рациональным числом, и, наоборот, всякое (неотрицательное) рациональное число выражает сопротивление некоторой схемы. Под *сложностью схемы* понимается число содержащихся в ней единичных сопротивлений. Схема называется *минимальной*, если не существует схемы меньшей сложности с тем же сопротивлением. Сложность минимальной схемы с сопротивлением R, называется *сложностью числа* R и обозначается через $L(R)$. Задача состоит в том, чтобы для всякого рационального числа $R > 0$ найти величину $L(R)$ (в более сильном варианте — найти для R хотя бы одну минимальную схему). Эта задача в обоих вариантах представляется весьма трудной. Какие-либо алгоритмы ее решения с существенно меньшей трудоемкостью, чем полный перебор схем к настоящему времени не известны. Хотя задача известна давно — по крайней мере с середины 1930-х годов [2, задача 60], она еще весьма далека от окончательного решения. Существующие методы синтеза позволяют получать лишь верхние оценки сложности, минимальность соответствующих схем, как правило, остается под вопросом [1–3].

До последнего времени точные значения сложности были известны для небольшого количества конкретных рациональных чисел (найдены перебором), и лишь для двух бесконечных последовательностей: всех натуральных чисел и всех чисел, обратных к натуральным. Для всякого натурального n выполняются равенства $L(n) = L(n^{-1}) = n$, причем для каждого из чисел n, n^{-1} существует единственная минимальная схема: в первом случае это n последовательно соединенных единичных сопротивлений, во втором — n сопротивлений, соединенных параллельно (математический фольклор).

В данной работе предложен метод, позволяющий при некоторых условиях получать точные значения сложности для различных бесконечных последовательностей чисел. В частности, с его помощью в работе найдены точные значения сложности всех рациональных чисел, выражающихся дробями с числителями или знаменателями ≤ 6. Предлагаемый метод основан на некоторых утверждениях, представляющих самостоятельный интерес.

Для любого рационального числа $R > 1$ имеет место очевидное неравенство $L(R) \leq L(R-1) + 1$. Оказывается, что для достаточно больших, в некотором смысле, чисел R это неравенство обращается в равенство.

Теорема 1. *Если рациональное число $R > 1$ удовлетворяет условию $L(R) < 4R$, то $L(R) = L(R-1) + 1$.*

Теорема 2. *Если рациональное число $R_0 > 0$ удовлетворяет условию $L(R_0) < 4R_0 + 3$, то для всякого натурального числа k имеет место равенство $L(R_0 + k) = L(R_0) + k$.*

Таким образом, как только удается установить точное значение сложности некоторого удовлетворяющего указанным условиям числа R_0, автоматически становятся известными точные значения сложности всей последовательности чисел $R_0, R_0 + 1, R_0 + 2, R_0 + 3, \ldots$.

Числовую последовательность $f(1), f(2), f(3), \ldots$ будем называть *линейно-периодической*, если найдутся такие неотрицательные числа T (*период*) и s, что $f(x + T) = f(x) + 1$ для всякого $x \geq s + 1$; наименьшее возможное s называется *предпериодом* последовательности. Такая последовательность записывается в виде $[f(1), \ldots, f(s)](f(s + 1), \ldots, f(s + T))$ (при $s = 0$ квадратные скобки опускаем).

Для всякого n обозначим через L_n последовательность значений сложности дробей с одинаковым знаменателем n, упорядоченных по возрастанию числителя: $L(1/n), L(2/n), L(3/n), \ldots$

Теорема 3. *При любом фиксированном n последовательность L_n является линейно-периодической с периодом n.*

При этом можно показать, что для всякого n предпериод последовательности L_n не превосходит $n^2/3 - 1$.

Найдены в явном виде: $L_1 = (1)$; $L_2 = (2, 1)$; $L_3 = (3, 3, 1)$; $L_4 = (4, 2, 4, 1)$; $L_5 = [5](4, 4, 5, 1, 5)$; $L_6 = [6](3, 2, 3, 5, 1, 5)$. Таким образом, установлены точные значения сложности всех рациональных чисел, выражающихся обыкновенными дробями со знаменателем $n \leq 6$.

Все осуществленные выше построения можно провести в некотором смысле двойственным образом.

Теорема 1′. *Если число $R < 1$ удовлетворяет условию $L(R) < 4R^{-1}$, то $L(R) = L((R^{-1} - 1)^{-1}) + 1$.*

Теорема 2′. *Если обыкновенная дробь m/n удовлетворяет условию $L(m/n) < 4n/m + 3$, то для любого натурального числа k имеет место равенство $L(m/(n + km)) = L(m/n) + k$.*

Для всякого натурального числа m обозначим через L^m бесконечную последовательность значений сложности всех обыкновенных дробей с числителем m, упорядоченных по возрастанию знаменателя: $L(m/1), L(m/2), L(m/3), \ldots$

Теорема 3′. *При любом фиксированном m последовательность L^m является линейно-периодической с периодом m.*

Можно показать, что для всякого m предпериод последовательности L^m не превосходит $m^2/3 - 1$.

Последовательности L^m вычислены для всех $m \leq 6$. Оказалось,

что при всех $n \leq 6$ последовательности L_n и L^n совпадают. Неизвестно, совпадают ли эти последовательности при всех n.

Работа выполнена при финансовой поддержке РФФИ (проект №14–01–00598) и Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Бессонов Л. А. Теоретические основы электротехники. Электрические цепи. — М.: Высш. шк., 1996.

2. 400 задач. Избранные задачи из журнала “American Mathematocal Monthly”. — М.: Мир, 1977.

3. Касим-Заде О. М. О сложности схем из единичных сопротивлений и о некоторых свойствах чисел Фибоначчи // Тр. МИАН им. В. А. Стеклова. — 1997. — Т. 218. — С. 233–247.

О ЗАДЕРЖКЕ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ В КОНЕЧНЫХ БАЗИСАХ

А. В. Кочергин (Москва)

В работе исследуется глубина и задержка функций k-значной ($k \geq 2$) логики при реализации схемами из функциональных элементов над произвольным конечным базисом. Под базисом понимается произвольное множество функций k-значной логики, такое, что его замыкание относительно операции суперпозиции совпадает с множеством всех функций k-значной логики.

Под *глубиной схемы* понимается максимальное число функциональных элементов в ориентированных цепях, ведущих от какого-либо входа схемы к е$\ddot{\{}$е$\}$ выходу. *Глубиной функции f над базисом B*, обозначаемой через $D_B(f)$, называется минимальная глубина схем, реализующих функцию f над базисом B. *Функцией Шеннона глубины над базисом B* называется функция $D_B(n)$, определяемая при любом натуральном n соотношением $D_B(n) = \max D_B(f)$, где максимум берется по всем функциям f, зависящим от n переменных.

Пусть каждому функциональному элементу Φ_i базиса B соответствует некоторое положительное число t_i. Величину t_i будем называть *задержкой элемента Φ_i над базисом B*. Под *задержкой цепи схемы* будем понимать сумму задержек составляющих ее элементов.

Задержкой схемы над базисом B, обозначаемой через $T_B(S)$, называется максимальная задержка цепи, ведущей от некоторого входа схемы S к ее выходу. *Задержкой функции* f *над базисом* B будем называть величину $T_B(f) = \min T_B(S)$, где минимум берется по всем схемам S над базисом B, реализующим функцию f. *Функцией Шеннона для задержек над базисом* B называется функция $T_B(n)$, определяемая при всех натуральных n равенством $T_B(n) = \max T_B(f)$, где максимум берется по всем функциям k-значной логики f, зависящим от n переменных.

Заметим, что если задержка каждого функционального элемента базиса B равна единице, то задержка всякой схемы над базисом B совпадает с глубиной этой же схемы.

В работе [1] установлена асимптотика функции Шеннона глубины для произвольного базиса функций двузначной ($k = 2$) логики: доказано, что для всякого конечного базиса B функций двузначной логики при $n \to \infty$ выполняется соотношение

$$D_B(n) \sim \beta n,$$

где $\beta = (\log_2 m)^{-1}$ и m — максимальное число существенных переменных у функций из базиса B.

В работе [2] установлено, что для всякого конечного базиса B функций k-значной ($k > 2$) логики существует такая положительная константа α_B, что при $n \to \infty$ выполняется соотношение

$$D_B(n) \sim \alpha_B n.$$

Показано, что константа α_B представляется в виде $\alpha_B = \log_k \lambda_B$, где λ_B является алгебраическим числом. Указан алгоритм нахождения по произвольному конечному базису B функций k-значной логики многочлена с целыми коэффициентами, максимальным действительным корнем которого является число λ_B.

Для функций двузначной логики в работе [1] установлена асимптотика и функции Шеннона для задержек: показано, что для произвольного конечного базиса B функций двузначной логики и любых положительных задержек базисных элементов при $n \to \infty$ выполняется соотношение

$$T_B(n) \sim \gamma n,$$

где $\gamma = \min_i (\frac{t_i}{\log_2 m_i})$, t_i — задержка элемента Φ_i, а m_i — число существенных переменных у базисной функции f_i, соответствующей элементу Φ_i.

Результатом данной работы является следующее утверждение.

Теорема. *При любом натуральном k, $k \geq 3$, для произвольного конечного базиса B функций k-значной логики и любых положительных задержек базисных элементов существует такая положительная константа τ_B, что при $n \to \infty$ выполняется соотношение*

$$T_B(n) \sim \tau_B n.$$

Работа выполнена при финансовой поддержке РФФИ (проект 14-01-00598) и Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.

2. Кочергин А. В. О глубине функций k-значной логики в конечных базисах // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2013. — № 1. — С. 56–59.

ОБ УТОЧНЕНИИ НЕКОТОРЫХ МОЩНОСТНЫХ НИЖНИХ ОЦЕНОК

В. В. Кочергин, Д. В. Кочергин (Москва)

Рассматриваются асимптотические нижние оценки схемной сложности для двух неклассических с точки зрения реализации булевых функций вычислительных моделей.

1. *Схемная сложность булевых функций.*

Асимптотическая постановка задачи о сложности реализации булевых функций связана с изучением поведения той или иной функции Шеннона при растущем значении ее натурального аргумента. О. Б. Лупановым найдена асимптотика функции Шеннона для сложности булевых функций во всех основных модельных классах управляющих систем (см., например, [1]; там же можно найти все необходимые определения). В частности, для схем из функциональных элементов, построенных из элементов произвольного конечного полного базиса установлены оценки

$$\rho_B \frac{2^n}{n}\left(1+(1+o(1))\frac{\log n}{n}\right) \le L_B(n) \le \rho_B \frac{2^n}{n}\left(1+(3+o(1))\frac{\log n}{n}\right),$$

где $L_B(n)$ — функция Шеннона для базиса B, состоящего из функций φ_i, имеющих вес и число существенных переменных p_i и m_i соответственно, $\rho_B = \min\{p_i/(m_i-1)\}$ (минимум берется по функциям из базиса, имеющим не менее двух существенных переменных), а запись $\log x$ здесь и далее означает $\log_2 x$. Отметим, что нижняя оценка величины $L_B(n)$ выводится стандартным мощностным методом.

С. А. Ложкиным в работе [2] дано краткое схематичное описание метода, позволяющего следующим образом усилить верхнюю оценку: $L_B(n) \le \rho_B \frac{2^n}{n}\left(1+(1+\varkappa_B+o(1))\frac{\log n}{n}\right)$, где $\varkappa_B = 1$ в случае, когда базис B симметричный [2], и $\varkappa_B = 0$ в остальных случаях.

В тезисах [3] анонсировано получение верхней оценки $L_B(n) \le \rho_B \frac{2^n}{n}\left(1+(1+o(1))\frac{\log n}{n}\right)$, которая вместе с мощностной нижней оценкой дает равенство

$$L_B(n) = \rho_B \frac{2^n}{n}\left(1+(1+o(1))\frac{\log n}{n}\right). \qquad (1)$$

При этом стоит заметить, что доказательство заявленной верхней оценки, насколько известно авторам, до сих пор не опубликовано.

2. *Сложность сборки слов схемами конкатенации.*

Для функции Шеннона сложности получения слов схемами конкатенации [4] выявлена возможность усиления аналога мощностной нижней оценки из соотношения (1).

Дадим определение схем конкатенации, немного отличающееся от определения из [4]. Пусть операция конкатенации (склейки в одно слово) m_i двоичных слов (наборов) имеет вес (стоимость) p_i и доступно множество B операций конкатенации с числом аргументов $m_1, \ldots, m_s$. Схемы конкатенации над множеством операций B будем рассматривать как схемы из функциональных элементов, сами схемы имеют два входа, на которые подаются символы 0 и 1, а элементам схемы соответствуют операции из множества B. Под *сложностью* $L^c(S)$ схемы конкатенации S понимается сумма весов элементов схемы. Положим $L^c_B(\tilde{\alpha}) = \min L^c(S)$, где минимум берется по всем схемам конкатенации, реализующим двоичное слово $\tilde{\alpha}$ над множеством операций B. Соответсвующая функция Шеннона определяется стандартным образом: $L^c_B(n) = \max L^c_B(\tilde{\alpha})$, где максимум берется по всем двоичным словам $\tilde{\alpha}$ длины n.

При аккуратном применении известных методов можно получить следующие нижнюю и верхнюю оценки:

$$\rho_B \frac{n}{\log n}\left(1+(1+o(1))\frac{\log\log n}{\log n}\right) \le L_B^c(n) \le \rho_B \frac{n}{\log n}\left(1+(2+o(1))\frac{\log\log n}{\log n}\right),$$

где $\rho_B = \min\{p_i/(m_i-1)\}$.

Здесь мощностная нижняя оценка имеет такой же вид, что и нижняя оценка из соотношения (1) (с точностью до изменения логарифма количества реализуемых объектов с 2^n на n). Однако, как по-существу показано в [4], в отличие от случая реализации булевых функций для задачи о сложности сборки слов схемами конкатенации нижняя оценка может быть усилена:

Теорема 1. *При $n \to \infty$ справедливо равенство*

$$L_B^c(n) = \rho_B \frac{n}{\log n}\left(1 + (2+o(1))\frac{\log\log n}{\log n}\right).$$

Отметим, что теорема 1 естественным образом обобщается на случай схем конкатенации над произвольным конечным алфавитом.

3. *Сложность возведения в степень.*

Для задачи об эффективном возведении в степень [5, раздел 4.6.3] обозначим через $l(x^n)$ миниальное число операций умножения, достаточное для вычисления по переменной x степени x^n (результаты промежуточных вычислений можно использовать многократно). Положим $l(n) = \max l(x^k)$, где максимум берется по всем k, не превосходящим n.

А. Брауэр доказал (см., например, [5, раздел 4.6.3, теорема D]) верхнюю оценку

$$l(x^n) \le \log n + \frac{\log n}{\log\log n}\left(1 + (2+o(1))\frac{\log\log\log n}{\log\log n}\right),$$

которая вместе с очевидной нижней оценкой $l(x^n) \ge \log n$ устанавливает асимптотику роста величины $l(x^n)$ при $n \to \infty$.

П. Эрдёш усилил (см., например, [5, раздел 4.6.3, теорема E]) нижнюю оценку, показав, что для любого $\varepsilon > 0$ при всех достаточно больших n выполняется неравенство

$$l(n) \ge \log n + (1-\varepsilon)\frac{\log n}{\log\log n}.$$

Эта нижняя оценка состоит из двух слагаемых — первое присутствует в нижней оценке сложности возведения в любую степень и «отвечает» за величину показателя степени, а второе (мощностное) слагаемое имеет место для почти всех показателей степени и «отвечает» за «структуру» числа n.

Возникает вопрос — можно ли мощностную составляющую нижней оценки для величины $l(n)$ усилить хотя бы до вида, аналогичного нижней оценке из формулы (1), т. е. верно ли соотношение

$$l(n) \geq \log n + \tfrac{\log n}{\log\log n}\left(1 + (1+o(1))\tfrac{\log\log\log n}{\log\log n}\right)?$$

Этот вопрос оказался весьма непростым. Тем не менее в этом направлении получено следующее продвижение.

Теорема 2. *Пусть* $n \to \infty$. *Тогда* $l(n) - \left(\log n + \tfrac{\log n}{\log\log n}\right) \to \infty$.

Работа выполнена при финансовой поддержке РФФИ, проект № 14–01–00598.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.

2. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.

3. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности реализации булевских функций схемами из функциональных элементов // Труды II Международной конференции «Дискретные модели в теории управляющих систем» (23–28 июня 1997 г.) — Москва: Диалог-МГУ, 1997. — С. 37–39.

4. Кочергин В. В., Кочергин Д. В. Уточнение асимптотического поведения сложности сборки слов схемами конкатенации // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2016, № 2. — С. 12–18.

5. Кнут Д. Е. Искусство программирования, т. 2. 3-е изд. — М.: Издательский дом «Вильямс», 2000.

О НЕМОНОТОННОЙ СЛОЖНОСТИ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

В. В. Кочергин, А. В. Михайлович (Москва)

Исследуются различные обобщения известных теорем А. А. Маркова [1, 2] об инверсионной сложности систем булевых функций.

Пусть P_k $(k \geq 2)$ — множество всех функций k-значной логики, M — класс всех функций из P_k, монотонных относительно порядка $0 < 1 < \ldots < k-1$.

Предметом изучения является сложность реализации функций k-значной логики схемами из функциональных элементов над базисами B, имеющими вид: $B = M \cup \{\omega_1, \ldots, \omega_s\}$, где $\omega_i \in P_k \setminus M$,

$i = 1, \ldots, s$, причем функциям из множества M приписан нулевой вес, а функциям $\omega_1, \ldots, \omega_s$ — ненулевой (как правило, единичный).

Определим *немонотонную сложность* $I_B(S)$ *схемы* S *над базисом* B стандартным образом как суммарный вес элементов схемы S. В случае, когда все немонотонные функции базиса имеют одинаковый вес, который без ограничения общности можно считать единичным, величина $I_B(S)$ равна числу немонотонных элементов схемы S.

Немонотонную сложность над базисом B функции k-значной логики f (системы функций F) определим как минимальную немонотонную сложность схем, вычисляющих над базисом B функцию f (систему функций F). Для немонотонной сложности функции f (системы функций F) будем использовать обозначение $I_B(f)$ (соответственно, $I_B(F)$).

Обозначим $E_k = \{0, 1, \ldots, k-1\}$. Последовательность $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$ наборов из множества E_k^n назовем *цепью относительно порядка* $0 < 1 < \ldots < k-1$, если все наборы $\tilde{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{in})$ различны и выполняются неравенства $\alpha_{ij} \leq \alpha_{i+1,j}$, $i = 1, \ldots, r-1$, $j = 1, \ldots, n$.

Пусть $f(x_1, \ldots, x_n) \in P_k$. Упорядоченную пару наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\tilde{\alpha}, \tilde{\beta} \in E_k^n$, будем называть *обрывом для функции* f, если $\alpha_j \leq \beta_j$ для всех $j = 1, \ldots, n$, но при этом $f(\tilde{\alpha}) > f(\tilde{\beta})$.

Обрывом для системы функций будем называть любую пару наборов, являющуюся обрывом хотя бы для одной функции системы.

Под *падением* $d_C(F)$ *системы* $F \subset P_k$ *на цепи* C будем понимать число обрывов для системы F на парах соседних наборов цепи C.

Спад $d(F)$ системы F определим равенством $d(F) = \max d_C(F)$, где максимум берется по всем цепям C.

Теорема 1 [А. А. Марков, 1957–1963]. *Пусть* $k = 2$, $B_0 = M \cup \{\overline{x}\}$. *Тогда для любой конечной системы* $F \subset P_2$ *выполняется равенство*

$$I_{B_0}(F) = \lceil \log_2(d(F) + 1) \rceil .$$

Для формулировки обобщений этой теоремы потребуются дополнительные определения.

Для произвольной функции $f(x_1, \ldots, x_n) \in P_k$ и произвольной цепи C наборов из E_k^n введем величину $u_C(f)$ как наибольшую длину t подпоследовательности $\tilde{\beta}_1, \ldots, \tilde{\beta}_t$ последовательности C, удовлетворяющей условию $f(\tilde{\beta}_1) > f(\tilde{\beta}_2) > \ldots > f(\tilde{\beta}_t)$. Положим $u(f) = \max u_C(f)$, где максимум берется по всем цепям C наборов из E_k^n.

Теорема 2. *Для любого базиса B, имеющего вид $B = M \cup \{\omega_1, \ldots, \omega_s\}$, $\omega_i \in P_k \setminus M$, $i = 1, \ldots, s$, где все монотонные функции имеют нулевой вес, а функции $\omega_1, \ldots, \omega_s$ — положительные веса $p(\omega_1), \ldots, p(\omega_s)$„ найдется такая константа $c(B)$, что для любой конечной системы F функций из P_k верны неравенства*

$$p(\omega_j)\left\lceil \log_{u(\omega_j)}(d(F)+1)\right\rceil - c(B) \le I_B(F) \le p(\omega_j)\left\lceil \log_{u(\omega_j)}(d(F)+1)\right\rceil,$$

где функция $\omega_j \in B$ определяется из соотношения

$$u(\omega_j)^{1/p(\omega_j)} = \max\left\{u(\omega_1)^{1/p(\omega_1)}, \ldots, u(\omega_s)^{1/p(\omega_s)}\right\}.$$

Следующее утверждение устанавливает невозможность использования в теореме 2 вместо $c(B)$ абсолютной константы.

Теорема 3. *Для любого $k \ge 2$ и для любого заданного значения N найдутся функция $g_N \in P_k$ и базис $B_N \subset P_k$, все монотонные функции которого имеют нулевой вес, а немонотонные — единичный, такие что выполняется неравенство*

$$\left\lceil \log_{u(B_N)}(d(g_N)+1)\right\rceil - I_{B_N}(g_N) > N.$$

Для случая булевых функций теоремы 2 и 3 установлены в [3].

Далее рассматриваются такие базисы в P_k: $B_P = M \cup \{N_P(x)\}$ и $B_L = M \cup \{N_L(x)\}$, где $N_P(x)$ — отрицание Поста, т. е. функция $x+1 \pmod k$, а $N_L(x)$ — отрицание Лукасевича, т. е. функция $k-1-x$. В этих базисах веса немонотонных функций считаем единичными.

Теорема 4. *Для любой конечной системы F функций k-значной логики справедливы равенства*

$$I_{B_P}(F) = \lceil \log_2(d(F)+1)\rceil, \quad I_{B_L}(F) = \lceil \log_k(d(F)+1)\rceil.$$

Стандартным образом определим *функции Шеннона немонотонной сложности функций от n переменных и сложности систем из m функций от n переменных над базисом B*:

$$I_B(n) = \max_{f \in P_k(n)} I_B(f), \quad I_B(n,m) = \max_{F=\{f_1,\ldots,f_m\}:\, f_j \in P_k(n)} I_B(F).$$

Положим

$$T(k,n) = (k-1)n - \left\lfloor \frac{(k-1)n}{k} \right\rfloor + 1 = (k-2)n + \left\lceil \frac{n}{k} \right\rceil + 1.$$

Теорема 5. *Для любых n и m, $n \geq 1$, $m \geq 2$, верны равенства*

$$I_{B_P}(n) = \lceil \log_2 T(k,n) \rceil, \quad I_{B_P}(n,m) = \lceil \log_2((k-1)n+1) \rceil;$$

$$I_{B_L}(n) = \lceil \log_k T(k,n) \rceil, \quad I_{B_L}(n,m) = \lceil \log_k((k-1)n+1) \rceil.$$

В заключение перейдем к задаче об обычной сложности (когда под *сложностью $L_B(f)$ функции f* понимается минимально возможное число всех элементов при реализации функции f схемами над базисом B) функций из P_k в бесконечных базисах B_P и B_L.

Теорема 6. *Для любой функции $f \in P_k$ при $k \geq 2$ выполняется равенство*

$$L_{B_L}(f) = 2\log_k(d(f)+1) + O(1),$$

а при $k \geq 3$ — равенство

$$L_{B_P}(f) = 3\log_3(d(f)+1) + O(1).$$

Данное научное исследование (№ 14–01–0144) выполнено при поддержке Программы «Научный фонд НИУ ВШЭ» в 2014/2015 гг. Работа первого автора выполнена при частичной финансовой поддержке РФФИ, проект № 14–01–00598.

Список литературы

1. Марков А. А. Об инверсионной сложности систем функций // ДАН СССР. — 1957. — Т. 116, № 6. — С. 917–919.

2. Марков А. А. Об инверсионной сложности систем булевых функций // ДАН СССР. — 1963. — Т. 150, № 3. — С. 477–479.

3. Кочергин В. В., Михайлович А. В. О сложности схем в базисах, содержащих монотонные элементы с нулевыми весами // Прикладная дискретная математика. — 2015. — № 4 (30). — С. 24–31.

О НИЖНЕЙ ОЦЕНКЕ СЛОЖНОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ВСЕХ ЭЛЕМЕНТАРНЫХ ПЕРИОДИЧЕСКИХ СИММЕТРИЧЕСКИХ ФУНКЦИЙ В КЛАССЕ РАЗДЕЛИТЕЛЬНЫХ КОНТАКТНЫХ СХЕМ

Е. Г. Красулина (Москва)

В работе рассматривается задача о реализации системы всех элементарных периодических симметрических функций контактными

разделительными схемами. Определение контактной схемы можно найти в работе [1].

Контактную схему назовем $(1,k)$-*полюсником*, если в ней есть некоторый полюс, называемый входом, и k полюсов, называемых выходами. Обычно с $(1,k)$-полюсниками связывают систему из k функций, каждая из которых реализуется между входом и некоторым выходом. $(1,k)$-полюсник назовем *разделительным*, если проводимость между любыми двумя его выходами тождественно равна нулю.

Функция алгебры логики называется *симметрической*, если она не изменяется ни при какой перестановке своих переменных. Из этого определения следует, что симметрическая функция $f(x_1,\ldots,x_n)$, равная единице на наборе $\tilde{\alpha}=(\alpha_1,\ldots,\alpha_n)$, равна единице и на всяком наборе, имеющем столько же единиц, сколько их содержится в $\tilde{\alpha}$. Число a называется *рабочим числом* симметрической функции f, если f равна единице на (всяком) наборе, имеющем a единиц. Каждой симметрической функции $f(x_1,\ldots,x_n)$ поставим в соответствие последовательность $\tilde{\pi}_f=(\pi_0,\pi_1,\ldots,\pi_n)$ из нулей и единиц длины $n+1$ — *характеристическую* последовательность, определяемую следующим образом: $\pi_a=1$, если a является рабочим числом функции f, и $\pi_a=0$ в противном случае. Будем говорить, что симметрическая функция $f(x_1,\ldots,x_n)$ является *периодической* с периодом $\tilde{\tau}=(\tau_0,\tau_1,\ldots,\tau_{d-1})$ (или имеет период $\tilde{\tau}$), если для ее характеристической последовательности $\tilde{\pi}_f=(\pi_0,\pi_1,\ldots,\pi_n)$ выполнено условие: $\pi_{kd+i}=\tau_i$ $(k=0,1,\ldots,[n/d]\,,\ i=0,1,\ldots,d-1)$, то есть характеристическая последовательность $\tilde{\pi}_f$ является периодической с периодом $\tilde{\tau}$ (без предпериода). Число d называется длиной периода. Такую функцию будем обозначать символом $T_n^{\tilde{\tau}}$. Периодическую симметрическую функцию назовем *элементарной периодической*, если она представима в виде $T_n^{\tilde{\tau}}$ и ее период $\tilde{\tau}$ содержит ровно одну единицу. Для этой функции будем использовать также обозначение $T_n^{d,a}$.

Первые результаты о сложности реализации симметрических функций были получены Шенноном в работе [2]. В этой работе была построена контактная схема, реализующая систему всех элементарных симметрических функций, и число контактов в этой схеме не более $n(n+1)$.

О. Б. Лупанов в работе [3] показал, что совокупность d функций $T_n^{d,0},T_n^{d,1},\ldots,T_n^{d,d-1}$ от n переменных может быть реализована одним и тем же разделительным $(1,d)$-полюсником, имеющим не более $d(2n-d+1)$ контактов.

Будем рассматривать реализацию системы всех элементарных периодических симметрических функций в классе разделительных контактных схем. Вопрос разделительных контактных схем изучался в работе Мура [4], где была доказана минимальность разделительного контактного дерева.

Теорема. *Если контактная схема реализует все элементарные периодические симметрические функции* $T_n^{d,0}, T_n^{d,1}, \ldots, T_n^{d,d-1}$ *от* n *переменных с периодом* d *и является разделительным* $(1,d)$*-полюсником, то в этой схеме должно быть не меньше* $dn - \frac{d(d-3)}{2}$ *вершин и не меньше* $dn - \frac{(d-1)(d-2)}{2}$ *контактов.*

Список литературы

1. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматгиз, 1963. — С. 63–97.

2. Shannon C. E. The synthesis of two-terminal series parallel networks // Bell Syst. Techn. J. — 1949. — Vol. 28, №1. — P. 59–98. (Русский перевод в сб. Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ., 1963. — С. 59–101.)

3. Лупанов О. Б. К вопросу о реализации симметрических функций алгебры логики контактными схемами // Проблемы кибернетики. Вып. 15. — М.: Наука, 1965. — С. 85–99.

4. Edward F. Moore. Minimal complete relay decoding networks // IBM Journal. November 1960. — P. 525–531. (Русский перевод в сб. Кибернетический сборник (старая серия). — М.: ИЛ., 1963. — № 6. — С. 139–152.)

ТОЧНОЕ ЗНАЧЕНИЕ ФУНКЦИИ ШЕННОНА ДЛЯ СЛОЖНОСТИ КОНТАКТНЫХ СХЕМ ОТ ПЯТИ ПЕРЕМЕННЫХ

С. А. Ложкин, М. С. Шуплецов, В. А. Коноводов, Б. Р. Данилов, В. В. Жуков, Н. Ю. Багров (Москва)

Построение минимальных и близких к ним схем в заданной модели дискретных управляющих систем является актуальной задачей математической кибернетики. Каталоги или библиотеки таких схем находят свое применение в различных алгоритмах логического

синтеза цифровых схем (см., например, [1]). Первые каталоги минимальных контактных схем (КС), реализующих функции алгебры логики (ФАЛ) от малого числа переменных, появились еще в 1950-х гг. Так, например, в статье [2], в книге [3] и работе [4] приведены таблицы верхних оценок контактной сложности для всех типовых ФАЛ четырех переменных (всего 402 функции).

В [5] Г. Н. Поваровым с помощью построения схем было установлено, что одна ФАЛ из этих 402 требует не более 14 контактов, четыре ФАЛ — не более 13 контактов, а остальные — не более 12 контактов. Затем В. Л. ван дер Пуль [6] построил для первой из этих функций схему с 13 контактами. Ю. Л. Васильев [4], взяв за основу каталоги из работ Г. Н. Поварова [5], Игоннэ и Греа [7], указал минимальные значения всех функций от четырех переменных. Три ФАЛ имели сложность 12, и две — 13. Позднее в работе В. Ю. Сусова [8] каталог Ю. Л. Васильева был уточнен, и было доказано, что сложность 13 имеет только одна функция от четырех переменных.

В работе К. Шеннона [9] было доказано, что для реализации любой ФАЛ от 5 переменных в классе контактных схем достаточно 30 контактов. Позднее, Г. Н. Поваров [10] уточнил эту оценку до 28 контактов, используя метод каскадов и полученные ранее результаты для ФАЛ от четырех переменных. В. Ю. Сусовым [8] была найдена ФАЛ от 5 переменных, контактная сложность которой не меньше 19.

Пусть $X = \{x_1, \ldots, x_n, \ldots\}$ — счетный алфавит входных переменных, а $P_2(n)$ — множество всех ФАЛ от переменных $x_1, \ldots, x_n$. Обозначим через U^K класс (1,1)-КС от переменных из алфавита X. Сложностью $L(\Sigma)$ КС Σ, $\Sigma \in U^K$, называется общее число контактов в этой схеме, а сложностью $L(f)$ ФАЛ f, $f \in P_2(n)$, называется минимальная сложность КС Σ, реализующей ФАЛ f. Введем обычным образом функцию Шеннона $L(n)$ для сложности КС:

$$L(n) = \max_{f \in P_2(n)} L(f).$$

Основным результатом работы является следующая теорема.

Теорема. *Точное значение функции Шеннона для контактной сложности ФАЛ от* 5 *переменных равно* 19*:*

$$L(5) = 19.$$

Теорема была доказана в результате построения каталога минимальных и близких к ним КС [11], найденных в результате применения различных алгоритмов построения КС.

Стоит отметить, что при построения каталога все ФАЛ от пяти переменных были разбиты на классы эквивалентности относительно операций перестановки и инвертирования переменных, так как эти операции не меняют структуры КС, реализующей указанные ФАЛ и позволяют существенно сократить число рассматриваемых ФАЛ.

Работа выполнена при финансовой поддержке РФФИ, грант № 15-01-07474.

Список литературы

1. Mishchenko A., Chatterjee S., Brayton R. DAG-aware AIG rewriting: A fresh look at combinational logic synthesis // Proc. DAC'06. — P. 532–536.

2. Polya G. J. Sur les types des propositions composes // Symb. Logik. — 1940. — 5, № 3. — P. 98.

3. Синтез электронных вычислительных и управляющих систем. Пер. с англ. под ред. Шестакова В. И. — М.:, 1954.

4. Васильев Ю. Л. Минимальные контактные схемы для булевых функций четырёх переменных // ДАН СССР. — 1959. — Т. 127, вып. 2.

5. Поваров Г. Н. Исследование контактных схем с минимальным числом контактов. — Дисс., ИАТ АН СССР, 1954.

6. Van der Poel W. L. Engine bijzondere onderwerpen uit de schakelalgebra // De Ingenieur (Utrecht). —1955. — V. 67, Nr. 1, blz. E. 9.

7. Higonnet R., Gréa R. Etude logique des circuits électriques et des systémes binairs. — Paris: 1955.

8. Сусов В. Ю. Два алгоритма переборного типа для синтеза минимальных контактных схем и их реализация. — Дипломная работа. М.: ВМК МГУ, 1981.

9. Shannon C. E. The synthesis of two-terminal switching circuits // Bell System Techn. Journ. — 1949. — V. 28, № 1. — P. 59–98.

10. Поваров Г. Н. Математико-логическое исследование синтеза контактных схем с одним входом и k выходами // Сб. Логические исследования, ИАН СССР. — М.: Наука, 1959.

11. Ложкин С. А., Шуплецов М. С., Коноводов В. А., Данилов Б. Р. База данных "Значения функционалов сложности и известные оптимальные схемы из функциональных элементов и контактные схемы для булевых функций" (Электронный ресурс: `http://mks2.cmc.msu.ru/.`)

12. Поваров Г. Н. Метод синтеза вычислительных и управляющих контактных схем // Автоматика и телемеханика. — 1957. — Т. 18. № 2. — С. 145–162.

ОБ ОЦЕНКАХ ФУНКЦИЙ ШЕННОНА СЛОЖНОСТИ СХЕМ В НЕКОТОРЫХ БЕСКОНЕЧНЫХ БАЗИСАХ

О. В. Подольская (Москва)

В работе изучается сложность реализации булевых функций схемами из функциональных элементов в двух бесконечных полных базисах. Первый базис состоит из линейных и антицепных функций от любого числа переменных. В этом базисе установлена верхняя оценка сложности реализации произвольной булевой функции от n переменных порядка $\sqrt{n}\log_2 n$. Также в этом базисе доказана нижняя оценка порядка $\sqrt{n}$ наибольшей сложности булевых функций от n переменных. Второй базис состоит из функций голосования и антицепных функций от любого числа переменных. Доказано, что в этом базисе наибольшая сложность булевых функций от n переменных по порядку роста равна $\log_2 n$.

Базисом называется произвольное функционально полное множество булевых функций. Следуя [1], будем называть базис *бесконечным*, если он содержит функции, существенно зависящие от сколь угодно большого числа переменных.

Булева функция, принимающая значение 1 лишь на попарно несравнимых наборах, называется *антицепной*. Булева функция $l_n(x_1,\ldots,x_n) = x_1 + \ldots + x_n \pmod 2$ называется *линейной функцией*. Булева функция $m_n(x_1,\ldots,x_n)$, принимающая значение 1 лишь на тех наборах, в которых число единиц не меньше $n/2$, называется *функцией голосования*. Функция называется *симметрической*, если она не изменяется при любой перестановке своих переменных. *Слоем* булева куба называется множество всех наборов куба, содержащих одинаковое количество единичных компонент. Для симметрической булевой функции f через $k(f)$ обозначается количество слоев куба, на которых функция f равна 1.

Совокупность всех антицепных функций от любого числа переменных обозначается через AC. Множество AC образует полный базис, это следует, например, из полноты содержащейся в нем системы функций $\{\neg, \&\}$.

Сложностью схемы называется число элементов в этой схеме, *сложностью функции* — наименьшая сложность схемы, реализующей эту функцию (определение схемы и другие, используемые в работе понятия, см., например, в [4]). Для базиса B через $L_B(S)$ обозначается сложность схемы S в этом базисе, через $L_B(f)$ — сложность функции f. *Функцией Шеннона* называется функция $L_B(n) = \max L_B(f)$, где максимум берется по всем булевым функциям f от n переменных.

Пусть две действительнозначные функции $a(n)$ и $b(n)$ натурального аргумента при всех достаточно больших n принимают положительные значения. Следуя [3], будем говорить, что порядок роста функции $a(n)$ не больше $b(n)$ и обозначать это через $a(n) = O(b(n))$, если существует такая положительная константа c, что $a(n) \leqslant cb(n)$ при всех достаточно больших n. При этом будем говорить, что порядок роста функции $b(n)$ не меньше $a(n)$, и обозначать это через $b(n) = \Omega(a(n))$. Если одновременно $a(n) = \Omega(b(n))$ и $a(n) = O(b(n))$, то будем говорить, что порядки роста функций $a(n)$ и $b(n)$ равны, и обозначать это через $a(n) = \Theta(b(n))$.

В работах [1, 2, 5–7] изучались оценки сложности схем в базисе AC. В частности, опираясь на результаты работ [1, 2, 5], в [7] было получено точное значение сложности произвольной симметрической булевой функции f, зависящей от n переменных:

$$L_{AC}(f) = \min\left(k(f),\, n - k(f) + 2\right).$$

Тем самым в [7] были установлены точные значения сложности реализации линейной функции и функции голосования от n переменных: при всех $n \geqslant 2$ $L(l_n) = \lfloor \frac{n+1}{2} \rfloor$, $L(m_n) = \left\lfloor \frac{n}{2} \right\rfloor + 1$, а также соотношение $L_{AC}(n) = \Omega(n)$. В [1] была установлена верхняя оценка функции Шеннона $L_{AC}(n) \leqslant n+1$, которая затем была усилена: в [6] доказана оценка $L_{AC}(n) \leqslant n$. Указанные оценки функции Шеннона позволили установить ее порядок роста в базисе AC: $L_{AC}(n) = \Theta(n)$.

При дальнейшем исследовании возник вопрос: как изменяется функция Шеннона при расширении базиса AC, в частности, при добавлении к этому базису функций, имеющих в нем высокую сложность.

Рассмотрим два полных базиса: базис ACL получается из базиса AC добавлением линейных функций от любого числа переменных, базис ACM — добавлением функций голосования от любого числа переменных.

В [7] отмечено, что в базисе AC линейные функции и функции голосования обладают почти одинаковой и притом наибольшей по порядку роста сложностью. В данной работе показано, что в базисах ACL и ACM наблюдается существенное понижение порядка роста функции Шеннона по сравнению с базисом AC, при этом порядок роста функций Шеннона в этих базисах оказывается разным.

Установлены следующие оценки функции Шеннона в базисе ACL.

Теорема 1. *Выполнены соотношения:* $L_{ACL}(n) = O(\sqrt{n}\log_2 n)$, $L_{ACL}(n) = \Omega(\sqrt{n})$.

Нижняя оценка получается из доказанной в работе оценки сложности реализации функций голосования.

Теорема 2. *Выполнено соотношение:* $L_{ACL}(m_n) = \Omega(\sqrt{n})$.

Также установлен порядок роста функции Шеннона в базисе ACM.

Теорема 3. *Выполнено соотношение:* $L_{ACM}(n) = \Theta(\log_2 n)$.

Автор благодарит А. В. Кочергина за полезные замечания.

Работа выполнена при поддержке РФФИ, проект 14–01–00598.

Список литературы

1. Касим-Заде О. М. О сложности схем в одном бесконечном базисе // Вестн. Московск. ун-та. Сер. 1. Математика. Механика. — 1994. — № 6 — С. 40–44.

2. Касим-Заде О. М. О сложности реализации булевых функций схемами в одном бесконечном базисе // Дискретный анализ и исследование операций. — 1995. — Т. 2, вып. 1. — С. 7–20.

3. Касим-Заде О. М. О порядках роста функций Шеннона сложности схем над бесконечными базисами // Вестн. Московск. ун-та. Сер. 1. Математика. Механика. — 2013. — № 6 — С. 55–57.

4. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Моск. ун-та, 1984.

5. Подольская О. В. О нижних оценках сложности схем в базисе антицепных функций // Вестн. Московск. ун-та. Сер. 1. Математика. Механика. — 2013. — № 2. — С. 17–23.

6. Подольская О. В. Об оценках сложности схем в одном бесконечном базисе // Материалы IX Молодежной научной школы по дискретной математике и ее приложениям (16–23 сентября 2013 г.). — С. 97–100.

7. Подольская О. В. Сложность реализации симметрических булевых функций схемами в базисе антицепных функций // Дискретная математика. — 2015. — Т. 27, вып. 3. — С. 95–107.

О ЕДИНИЧНЫХ ДИАГНОСТИЧЕСКИХ ТЕСТАХ ДЛЯ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ В НЕКОТОРЫХ БАЗИСАХ

К. А. Попков (Москва)

Рассматриваются задачи синтеза легкотестируемых схем из функциональных элементов, реализующих заданные булевы функции. Логический подход к тестированию схем предложен С. В. Яблонским и И. А. Чегис в [1]. Пусть имеется схема S, реализующая функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \ldots, x_n)$. Под воздействием некоторого источника неисправностей один или несколько элементов схемы S могут перейти в неисправное состояние. В результате схема S вместо исходной функции $f(\tilde{x}^n)$ будет реализовывать некоторую функцию $g(\tilde{x}^n)$, вообще говоря, отличную от f. Все такие функции $g(\tilde{x}^n)$, получающиеся при всевозможных допустимых неисправностях элементов схемы S, называются *функциями неисправности* данной схемы.

Проверяющим (*диагностическим*) *тестом* для схемы S называется такое множество T входных наборов данной схемы, что по значениям схемы на этих наборах можно однозначно определить, реализует ли схема S «правильную» функцию f или же какую-то функцию неисправности, отличную от f (соответственно, какую именно функцию реализует схема S). Число наборов в T называется *длиной* теста. В качестве тривиального диагностического (и проверяющего) теста длины 2^n для схемы S всегда можно взять множество T, состоящее из всех двоичных наборов длины n. Тест называется *полным*, если в схеме могут быть неисправны сколько угодно элементов, и *единичным*, если в схеме может быть неисправен только один элемент. Единичные тесты обычно рассматривают для неизбыточных схем [2], в которых любая допустимая неисправность любого одного элемента приводит к функции неисправности, отличной от исходной функции, реализуемой данной схемой.

Пусть зафиксирован вид неисправностей элементов, B — произвольный функционально полный базис и T — единичный диагностический тест (ЕДТ) для некоторой схемы S. Введем следующие обозначения: $D^B(T)$ — длина теста T; $D^B(S) = \min D^B(T)$, где минимум берётся по всем ЕДТ T для схемы S; $D^B(f) = \min D^B(S)$, где минимум берётся по всем неизбыточным схемам S в базисе B, реализующим функцию f; $D^B(n) = \max D^B(f)$, где максимум берётся по всем функциям f от n переменных, для которых определено значение $D^B(f)$. Функция $D^B(n)$ называется *функцией Шеннона* длины ЕДТ.

Будем рассматривать схемы в базисах $B_0 = \{\&, \vee, \neg\}$, $B_1 = \{\&, \oplus, 1, 0\}$ и $B_1^* = \{\vee, \sim, 0, 1\}$, а в качестве неисправностей элементов — однотипные константные неисправности типа p на выходах элементов, при которых значение на выходе любого неисправного элемента становится равно заданной булевой константе p. Для удобства в качестве нижнего индекса у буквы D будем ставить символ «0» или «1» в случаях $p = 0$, $p = 1$ соответственно.

С использованием идей С. В. Яблонского по аналогии с доказательством [2, т. 9, с. 113] можно показать, что $D_p^B(n) \lesssim \frac{2^n}{n}$ для $p = 0, 1$ и любого функционально полного конечного базиса B. Н. П. Редькиным в [3] были получены оценки $D_p^{B_0}(n) \leqslant 2n + 1$, $p = 0, 1$.

Рассмотрим классический базис B_0. Выделим два возможных представления функции f:

$$f(\tilde{x}^n) = x_i, \qquad (a)$$

где $i \in \{1, \ldots, n\}$;

$$f(\tilde{x}^n) = K_1 \vee \ldots \vee K_m, \qquad (b)$$

где $m \geqslant 1$ и каждое слагаемое K_j, $j = 1, \ldots, m$, имеет вид либо x_{i_j}, либо $\overline{x_{i_j}}$, либо $x_{i_j} x_{i'_j}$ для некоторых $i_j, i'_j \in \{1, \ldots, n\}$, $i_j \neq i'_j$.

Теорема 1. *Для любой функции $f(\tilde{x}^n)$, отличной от тождественной единицы, справедливо равенство*

$$D_1^{B_0}(f) = \begin{cases} 0, & \text{если } f \text{ представима в виде } (a), \\ 1, & \text{если } f \text{ представима в виде } (b), \text{ но не в виде } (a), \\ 2, & \text{если } f \text{ не представима в виде } (b). \end{cases}$$

Если же $f \equiv 1$, то значение $D_1^{B_0}(f)$ не определено.

Следствие 1. *Справедливо равенство $D_1^{B_0}(n) = 2$.*

По принципу двойственности из теоремы 1 и следствия 1 нетрудно получить двойственные им результаты для случая $p = 0$, в частности,

Следствие 2. *Справедливо равенство $D_0^{B_0}(n) = 2$.*

Доказательства теоремы 1, следствия 1 и двойственных им результатов даны в [4]. Следствия 1 и 2 уточняют оценки $D_p^{B_0}(n) \leqslant 2n + 1$ для $p = 0, 1$ из [3].

Рассмотрим теперь базис Жегалкина B_1. Будем считать, что константы 0 и 1, содержащиеся в этом базисе, подаются со входов схемы,

не являются элементами и, соответственно, не могут быть неисправны. Выделим ещё два возможных представления функции f:

$$f(\tilde{x}^n) = 0,\ 1 \text{ или } x_i, \qquad (c)$$

где $i \in \{1, \ldots, n\}$;

$$f(\tilde{x}^n) = L_1 \& \ldots \& L_m, \qquad (d)$$

где $m \geqslant 1$ и каждый множитель L_j, $j = 1, \ldots, m$, имеет вид либо x_{i_j}, либо $\overline{x_{i_j}}$, либо $x_{i_j} \oplus x_{i'_j}$ для некоторых $i_j, i'_j \in \{1, \ldots, n\}$, $i_j \neq i'_j$.

Теорема 2. *Для любой функции $f(\tilde{x}^n)$ справедливо равенство*

$$D_0^{B_1}(f) = \begin{cases} 0, & \text{если } f \text{ представима в виде } (c), \\ 1, & \text{если } f \text{ представима в виде } (d), \text{ но не в виде } (c), \\ 2, & \text{если } f \text{ не представима ни в одном из видов } (c), (d). \end{cases}$$

Следствие 3. *При $n \geqslant 2$ справедливо равенство $D_0^{B_1}(n) = 2$.*

По принципу двойственности из теоремы 2 и следствия 3 нетрудно получить двойственные им результаты для случая $p = 1$ и базиса B_1^*, в частности,

Следствие 4. *При $n \geqslant 2$ справедливо равенство $D_1^{B_1^*}(n) = 2$.*

Список литературы

1. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Труды МИАН. — 1958. — Т. 51. — С. 270–360.

2. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

3. Редькин Н. П. О единичных диагностических тестах для однотипных константных неисправностей на выходах функциональных элементов // Вестник Московского университета. Серия 1. Математика. Механика. — 1992. — № 5. — С. 43–46.

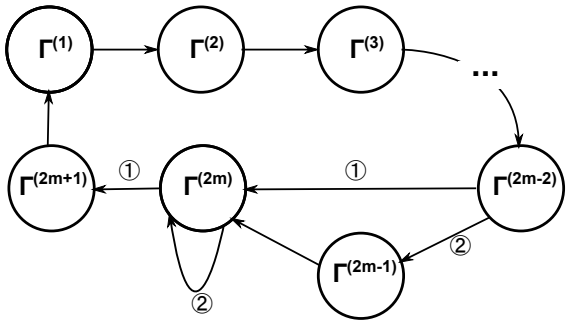
4. Попков К. А. О точном значении длины минимального единичного диагностического теста для одного класса схем // Препринты ИПМ им. М.В.Келдыша. — 2015. —№ 74. — 21 с. Электронный адрес: http://library.keldysh.ru/preprint.asp?id=2015-74

ПОСТРОЕНИЕ МОДЕЛИ И АНАЛИЗ УПРАВЛЯЮЩИХ СИСТЕМ ОБСЛУЖИВАНИЯ

М. А. Рачинская, М. А. Федоткин (Н. Новгород)

Объект исследования работы — система управления $m \geq 2$ потоками Π_j, $j = 1, 2, \ldots, m$ случайных заявок. Предполагается, что поступление заявок в систему по потоку Π_j (здесь и далее полагаем $j \in \{1, 2, \ldots, m\}$, если не указано иное) происходит группами (пачками). При этом интенсивность пуассоновского поступления пачек — параметр λ_j, а произвольная пачка может состоять из одной, двух или трех заявок с вероятностями p_j, q_j и s_j соответственно ($p_j + q_j + s_j = 1$). Такие неординарные пуассоновские потоки были подробно изучены в [1]. В работе изучается случай, когда поступление заявок по различным потокам происходит независимым образом и, кроме того, различные потоки имеют различный приоритет и интенсивность. Так, поток Π_1 — низкоинтенсивный поток с высоким приоритетом, $\Pi_2, \ldots, \Pi_{m-1}$ — низкоинтенсивные потоки с низким приоритетом, а Π_m — высокоинтенсивный поток с низким приоритетом.

Изучаемая система, помимо функции управления потоками, несет функцию обслуживания заявок этих потоков. Рассматривается так называемые конфликтные потоки: обслуживание заявок различных потоков должно происходить в непересекающиеся интервалы времени. Кроме того, системе необходимо время на осуществление переналадочных работ при переходе от обслуживания заявок одного потока к обслуживанию заявок другого. В связи с этим и с учетом особенностей различных потоков, в устройстве, осуществляющем обслуживание заявок, выделено $2m+1$ состояние. В состоянии вида $\Gamma^{(2j-1)}$, $j \in \{1, 2, \ldots, m-1\}$, с интенсивностью μ_j происходит обслуживание только заявок потока Π_j; в состоянии переналадки обслуживающего устройства (ОУ) вида $\Gamma^{(2j)}$, $j \in \{1, 2, \ldots, m-1\}$, только завершается обслуживание заявок потока Π_j, новое обслуживание не начинается. Обслуживание заявок высокоинтенсивного потока Π_m (и только его) происходит в состояниях $\Gamma^{(2m-1)}$ и $\Gamma^{(2m)}$ с интенсивностями μ_m и μ'_m соответственно. В свою очередь, завершение обслуживания заявок потока Π_m и переналадка ОУ происходит в состоянии $\Gamma^{(2m+1)}$. Предполагается, что в любом состоянии $\Gamma^{(k)}$, $k \in \{1, 2, \ldots, 2m+1\}$, ОУ находится в течение времени T_k, а затем происходит переключение состояния согласно алгоритму со следующим графом переходов:



Здесь переходы вида ① совершаются в случае, если количество заявок в очереди ожидания по потоку Π_1 достигло фиксированной величины H_1, в противном случае осуществляется переход типа ②.

Для того, чтобы построить адекватную модель такой управляющей системы, рассмотрим ее с точки зрения кибернетического подхода Ляпунова-Яблонского. Согласно такому подходу схема любой управляющей кибернетической системы может быть описана с помощью нескольких структурных блоков. Во-первых, это *входные полюса*. В нашей системе входные полюса представлены потоками Π_j $(1 \leq j \leq m)$. Выделяется также *внешняя память*, в качестве которой в системе выступают накопители O_j $(1 \leq j \leq m)$ заявок соответствующих потоков, поступивших в систему и вынужденных ожидать обслуживания. Накопители функционируют согласно дисциплине FIFO. *Устройство по переработке информации внешней памяти* представлено в изучаемой системе экстремальной стратегией обслуживания: в состоянии обслуживания потока Π_j из очереди O_j выбирается на обслуживание как можно большее количество имеющихся заявок, но не превышающее величины $l_j = [\mu_j T_{2j-1}]$ $(1 \leq j \leq m)$ или $l'_m = [\mu'_j T_{2m}]$ — пропускной способности устройства в соответствующем состоянии. Устройство обслуживания представляет блок *внутренней памяти*, а алгоритм смены его состояний — *устройство по переработке информации внутренней памяти*. Последним блоком являются *выходные полюса* — потоки Π'_j $(1 \leq j \leq m)$ обслуженных заявок. По аналогии с работой [2] в изучаемой управляющей системе выделяется информация, координаты и функция.

Задав основные свойства исследуемой системы, можем перейти к кодированию информации о системе и нелокальному описанию структурных блоков. При этом существенную роль играет фундаментальный принцип кибернетического подхода — принцип дискретности актов функционирования системы. Итак, вводятся следующие

основные случайные величины: τ_i, $i = 0, 1, \ldots$, — случайный момент переключения состояния ОУ; $\Gamma_i \in \Gamma = \{\Gamma^{(k)}; 1 \le k \le 2m+1\}$ — состояние ОУ на промежутке $[\tau_i, \tau_{i+1})$; $\eta_{j,i}$ — число заявок, поступивших в систему по потоку Π_j в промежутке $[\tau_i, \tau_{i+1})$; $æ_{j,i} \in \{0, 1, \ldots\}$ — число заявок, находящихся в очереди по потоку Π_j в момент времени τ_i; $\xi'_{j,i}$ — число обслуженных в промежутке $[\tau_i, \tau_{i+1})$ заявок потока Π_j. В терминах введенных величин можно формализовать условия переходов по представленному выше графу: ① выражается неравенством $æ_{1,i} + \eta_{1,i} \ge H_1$, а ② — неравенством $æ_{1,i} + \eta_{1,i} < H_1$. Наибольший интерес представляет динамика изменения количества заявок в очереди ожидания, а также количество обслуженных заявок по потокам Π_1 и Π_m. Применение кибернетического подхода позволило доказать теорему, открывающую возможности для применения в дальнейшем исследовании аппарата теории цепей Маркова.

Теорема. *Последовательность*

$$\{(\Gamma_i, æ_{1,i}, æ_{m,i}, \xi'_{1,i-1}, \xi'_{m,i-1}); i = 0, 1, \ldots\},$$

с начальным распределением вектора $(\Gamma_0, æ_{1,0}, æ_{m,0}, \xi'_{1,-1}, \xi'_{m,-1})$ *является однородной цепью Маркова.*

Работа выполнена в ННГУ при финансовой поддержке госбюджетной темы 01201456585 "Математическое моделирование и анализ стохастических эволюционных систем и процессов принятия решений" и государственной программы "Поддержка ведущих университетов РФ в целях повышения их конкурентоспособности среди ведущих мировых научно-образовательных центров".

Список литературы

1. Fedotkin M., Rachinskaya M. Parameters estimator of the probabilistic model of moving batches traffic flow // Distributed Computer and Communication Networks. Ser. Communications in Computer and Information Science. 2014. — V. 279. — P. 154–168.

2. Рачинская М. А., Федоткин М. А. Подход Ляпунова—Яблонского при построении и исследовании модели управляющих систем обслуживания конфликтных потоков // Материалы XVII международной конференции "Проблемы теоретической кибернетики"(16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 280–282.

ОБ ОЦЕНКАХ ФУНКЦИЙ ШЕННОНА ДЛИНЫ ТЕСТА ОТНОСИТЕЛЬНО КОНСТАНТНЫХ НЕИСПРАВНОСТЕЙ

Д. С. Романов, Е. Ю. Романова (Москва)

Под длиной минимального проверяющего (диагностического) теста для булевой функции или системы функций f, реализованной с помощью СФЭ в базисе B, относительно источника неисправностей U понимается величина $L_B^{\mathrm{detect}}(U,f)$ (соответственно, $L_B^{\mathrm{diagn}}(U,f)$), равная минимуму по всем неизбыточным реализующим f СФЭ S в базисе B минимума длины теста T по всем проверяющим (соответственно диагностическим) тестам T для S относительно U. Пусть $\hat{P}_2(n)$ — множество всех булевых функций, существенно зависящих от всех своих n переменных. *Функцией Шеннона* длины проверяющего (диагностического) теста для реализованной с помощью СФЭ в базисе B булевой функции f относительно источника неисправностей U называется величина $L_B^{\mathrm{detect}}(U,n) = \max\limits_{f\in\hat{P}_2(n)} L_B^{\mathrm{detect}}(U,f)$ (соответственно, величина $L_B^{\mathrm{diagn}}(U,n) = \max\limits_{f\in\hat{P}_2(n)} L_B^{\mathrm{diagn}}(U,f)$) (см. [1]). Обозначение для источника неисправностей будет иметь вид X_z^{y}, где X — это одна или несколько заглавных латинских букв, указывающих на место возможной неисправности (P — неисправности на входах схем, I — неисправности на входах функциональных элементов (ФЭ), O — неисправности на выходах ФЭ), y — это название типа неисправности (const, 0, 1 — константные неисправности: произвольные, типа 0 и типа 1 соответственно, inv — инверсные неисправности), z указывает на максимальное число возможных неисправностей (нижний индекс отсутствует, если ограничений нет). Приведем краткий обзор работ, в которых получены невысокие верхние оценки функций Шеннона длин тестов для СФЭ без введения дополнительных входов и выходов (n всюду далее по умолчанию произвольное натуральное). В работе [2] фактически было доказано, что в базисе Жегалкина $B_1 = \{x\,\&\,y, x\oplus y, 1\}$ имеют место неравенства: $L_{B_1}^{\mathrm{detect}}(IO_1^{\mathrm{const}},n) \le n+3$, $L_{B_1}^{\mathrm{detect}}(PIO_1^{\mathrm{const}},n) \le 3n+3$. Было установлено, что $L_{B_0}^{\mathrm{diagn}}(O_1^0,n) = L_{B_0}^{\mathrm{diagn}}(O_1^1,n) \le 2n+1$ [3], при $B_0^\infty = \{\bar{x}\}\cup\bigcup\limits_{i\ge 2}\{x_1\&\cdots\&x_i, x_1\vee\cdots\vee x_i\}$ имеет место: $L_{B_0^\infty}^{\mathrm{diagn}}(O_1^0,n) = L_{B_0^\infty}^{\mathrm{detect}}(O_1^1,n) \le 2\lceil\log_2 n+1\rceil+1$ [4]. Доказано, что в произвольном полном базисе B: $L_B^{\mathrm{detect}}(O_1^{\mathrm{inv}},n)\le 3$ [5], $L_B^{\mathrm{detect}}(O_1^{\mathrm{const}},n)\le n+3$ [6–

7], $2 \le L_B^{\mathrm{detect}}(O_1^{\mathrm{const}}, n) \le 4$ [15]. В базисе B_1: $L_{B_1}^{\mathrm{detect}}(O_1^{\mathrm{inv}}, n) = 1$ [8], $L_{B_1}^{\mathrm{detect}}(O_1^1, n) = 1$ [9], $L_{B_1}^{\mathrm{detect}}(O^0, n) = 1$ [10]. В базисе $B_0 = \{x\&y,\, x \vee y,\, \bar{x}\}$: $L_{B_0}^{\mathrm{detect}}(O^0, n) = L_{B_0}^{\mathrm{detect}}(O^1, n) = 2$ при $n > 1$ [11]. Отметим, что $L_{\{x|y\}}^{\mathrm{detect}}(O^1, n) \ge n + 1$ [12]. Найдены [13, 14] примеры полных конечных базисов $\check{B}'$, $\check{B}''$ таких, что $L_{\check{B}'}^{\mathrm{detect}}(O^{\mathrm{const}}, n) \le 4$, $L_{\check{B}''}^{\mathrm{detect}}(O^{\mathrm{inv}}, n) \le 4$. В работе [16] установлено, что $L_{B_0}^{\mathrm{diagn}}(O_1^0, n) = L_{B_0}^{\mathrm{diagn}}(O_1^1, n) = 2$, причем для каждой булевой функции указана длина минимального теста. Независимо один из авторов установил [17], что $L_{B_1}^{\mathrm{diagn}}(O_1^{\mathrm{inv}}, n) = 1$. Имеют место следующие утверждения.

Теорема 1. $\forall n,\, n \in \mathbb{N}$: $L_{B_1}^{\mathrm{detect}}(IO_1^{\mathrm{const}}, n) \le 80$.

Следствие. $\forall n,\, n \in \mathbb{N}$: $L_{B_1}^{\mathrm{detect}}(PIO_1^{\mathrm{const}}, n) = 2n - 2\log_2 n + O(1)$.

Теорема 2. $\forall n,\, n \in \mathbb{N}$: $L_{B_1}^{\mathrm{diagn}}(O_1^{\mathrm{const}}, n) \le 130$.

Следствие. $\forall n,\, n \in \mathbb{N}$: $L_{B_1}^{\mathrm{diagn}}(PO_1^{\mathrm{const}}, n) = 2n + O(1)$.

Работа выполнена в рамках проектов РФФИ № 15-01-07474-а и № 16-01-00593-а и государственного задания Министерства образования и науки РФ № 2014/601 (код проекта 3106).

Список литературы

1. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

2. Reddy S. M. Easily testable realization for logic functions // IEEE Trans. Comput. — 1972. — Vol. 21, Iss. 1. — P. 124–141.

3. Редькин Н. П. О единичных диагностических тестах для однотипных константных неисправностей на выходах функциональных элементов // Вестник Моск. ун-та. Серия 1. Матем. Механика. — 1992. — № 5. — С. 43–46.

4. Редькин Н. П. О синтезе легкотестируемых схем в одном бесконечном базисе // Вестник Моск. ун-та. Серия 1. Матем. Механика. — 2007. — № 3. — С. 29–33.

5. Редькин Н. П. Единичные проверяющие тесты для схем при инверсных неисправностях элементов // Математические вопросы кибернетики. Вып. 12. — М.: Физматлит, 2003. — С. 217–230.

6. Коляда С. С. Единичные проверяющие тесты для схем из функциональных элементов в базисах из элементов, имеющих не более двух входов // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 2. — С. 58–74.

7. Коляда С. С. Единичные проверяющие тесты для схем из функциональных элементов // Вестн. Моск. ун-та. Сер. 1. Матем.

Мех. — 2013. — № 4. — С. 32–34.

8. Коваценко С. В. Синтез легкотестируемых схем в базисе Жегалкина для инверсных неисправностей // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2000. — № 2. — С. 45–47.

9. Бородина Ю. В. О схемах, допускающих единичные тесты длины 1 при константных неисправностях на выходах элементов // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2008. — № 5. — С. 49–52.

10. Бородина Ю. В., Бородин П. А. Синтез легкотестируемых схем в базисе Жегалкина при константных неисправностях типа “0” на выходах элементов // Дискретная математика. — 2010. — Т. 22, вып. 3. — С. 127–133.

11. Бородина Ю. В. О синтезе легкотестируемых схем в случае однотипных константных неисправностей на выходах элементов // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2008. — № 1. — С. 40–44.

12. Бородина Ю. В. Нижняя оценка длины полного теста в базисе $\{x|y\}$ // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2015. — Т. 70, № 4. — С. 49–51.

13. Романов Д. С. О синтезе схем, допускающих полные проверяющие тесты константной длины относительно произвольных константных неисправностей на выходах элементов // Дискретная математика. — 2013. — Т. 25, вып. 2. — С. 104–120.

14. Романов Д. С. О синтезе схем, допускающих полные проверяющие тесты константной длины относительно инверсных неисправностей на выходах элементов // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2015. — № 1. — С. 30–37.

15. Романов Д. С. Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. — 2014. — Т. 26, вып. 2. — С. 100–130.

16. Попков К. А. О точном значении длины минимального единичного диагностического теста для одного класса схем. — М.: Издательство ИПМ им. М.В. Келдыша РАН, 2015. 20 с.

17. Романов Д. С. Метод синтеза неизбыточных схем в базисе Жегалкина, допускающих единичные диагностические тесты длины один // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 4. — С. 38–54.

АСИМПТОТИКА ДЛИНЫ ПОЛИНОМИАЛЬНЫХ ФУНКЦИЙ ПО СОСТАВНОМУ МОДУЛЮ

С. Н. Селезнева (Москва)

В работе получена асимптотика длины полиномиальных функций k-значной логики при составных k.

Пусть $k \geq 2$ — натуральное число, $E_k = \{0, 1, \ldots, k-1\}$, и $P_k = \{f^{(n)} : E_k^n \to E_k \mid n = 0, 1, \ldots\}$ — множество всех функций k-значной логики. Функция k-значной логики называется *полиномиальной*, если ее можно представить каким-то полиномом по модулю k. Равенство $P_k = Pol_k$, где Pol_k обозначает множество всех полиномиальных функций k-значной логики, справедливо тогда и только тогда, когда k — простое число [1].

Если k — простое число, то каждая функция k-значной логики задается однозначным полиномом по модулю k, в котором степень каждой переменной не превосходит $k-1$ [1]. При составных k однозначные виды полиномов одноместных полиномиальных функций k-значной логики получены в работах [2–4]. В [5] при составных k предложен однозначный вид полиномиальных функций k-значной логики, зависящих от произвольного числа переменных. Рассмотрим этот канонический вид.

Сначала пусть $k = p^m$, где p — простое число, $m \geq 1$. Определим *составную характеристику* $\mathrm{c}_{p,m}(x^s)$ степени переменной x^s, $s \geq 0$, как наибольшее число t из чисел $0, 1, \ldots, m-1, m$, такое, что найдется полином $g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_1 x = 0 (\mathrm{mod}\ p^t)$ с коэффициентами $c_1, \ldots, c_{s-1} \in E_{p^m}$ (по определению полагаем, что $x^s = 0 (\mathrm{mod}\ p^0)$). Из результатов работ [2, 4] следует, что $\mathrm{c}_{p,m}(x^s) = t$, где t — наибольшее число из чисел $0, 1, \ldots, m-1, m$, такое, что факториал $s!$ числа s делится нацело на число p^t. *Составной характеристикой* $\mathrm{c}_{p,m}(K)$ монома $K = \prod\limits_{i=1}^{n} x_i^{s_i}$, где x^s — степени, т.е. $x^s = 1$ при $s = 0$, $x^s = \underbrace{x \cdot \ldots \cdot x}_{s}$ при $s \geq 1$, назовем величину $\min(m, \sum\limits_{i=1}^{n} \mathrm{c}_{p,m}(x_i^{s_i}))$.

Теорема 1 [5]. *Если $k = p^m$, где p — простое число, $m \geq 1$, то каждая функция $f(x_1, \ldots, x_n) \in Pol_k$ задается однозначным полиномом по модулю k вида $P(f) = \sum\limits_{j=1}^{l} c_j \cdot K_j$, где K_j — мономы, $\mathrm{c}_{p,m}(K_j) < m$, $c_j \in E_k$ и $c_j < p^{m - \mathrm{c}_{p,m}(K_j)}$, $j = 1, \ldots, l$.*

Теперь пусть $k = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$, где $p_1, \ldots, p_r$ — попарно различные простые числа, $m_1, \ldots, m_r \geq 1$, $r \geq 1$. В силу необходимого условия полиномиальности из [6, 7] каждой функции $f \in Pol_k$ поставим в соответствие однозначный набор функций $(f_1, \ldots, f_r)$, где $f_i \in Pol_{p_i^{m_i}}$, $i = 1, \ldots, r$. Тогда каждая функция $f \in Pol_k$ задается однозначным полиномом по модулю k вида $P(f) = \sum\limits_{j=1}^{l} c_j K_j$, в котором K_j — мономы, $c_j \in E_k$ является однозначным (по китайской теореме об остатках) решением системы сравнений $c = c_j^{(i)} (\mathrm{mod}\ p_i^{m_i})$, где $c_j^{(i)} \in E_{p_i^{m_i}}$ — коэффициент, с которым моном K_j входит в полином $P(f_i)$, $i = 1, \ldots, r$, $j = 1, \ldots, l$ [8].

Длиной функции $f \in Pol_k$ назовем число попарно различных слагаемых с ненулевыми коэффициентами в ее полиноме $P(f)$. Введем *функцию Шеннона* $L_k(n)$ длины полиномиальных функций k-значной логики как наибольшую длину среди всех полиномиальных функций, зависящих от n переменных. Если k — простое число, то $L_k(n) = k^n$ [1].

Теорема 2. *Если $k = p^m$, где p — простое число, $m \geq 2$, то*

$$L_k(n) = \tfrac{1}{(m-1)!} \cdot n^{m-1} p^n + \Theta(n^{m-2} p^n) \text{ при } n \to \infty.$$

Теорема 3. *Если k — составное число, $k = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$, где $p_1, \ldots, p_r$ — попарно различные простые числа, $m_1, \ldots, m_r \geq 1$, $r \geq 2$, и $p_{i_0} = \max\limits_{1 \leq i \leq r} p_i$, $p = p_{i_0}$, $m = m_{i_0}$, то*

$$L_k(n) \sim \tfrac{1}{(m-1)!} \cdot n^{m-1} \cdot p^n \text{ при } n \to \infty.$$

Работа поддержана РФФИ, грант 16-01-00593-а.

Список литературы

1. Яблонский С. В. Функциональные построения в k-значной логике // Труды Математического института им. В.А. Стеклова АН СССР. — 1958. — Т. 51. — С. 5–142.

2. Niven I., Warren L. J. A generalization of Fermat's theorem // Proc. Amer. Math. Soc. — 1957. — V. 8. — P. 306–313.

3. Айзенберг Н. Н., Семйон И. В., Циткин А. И. Мощность класса функций k-значной логики от n переменных, представимых полиномами по модулю k // В кн. Многоустойчивые элементы и их применение. — М.: Сов. радио, 1971. — С. 79–83.

4. Singmaster D. On polynomial functions (mod m) // J. Number Theory. — 1974. — V. 6, is. 5. — P. 345–352.

5. Селезнева С. Н. Быстрый алгоритм построения для k-значных функций полиномов по модулю k при составных k // Дискретная математика. — 2011. — Т. 23, вып. 3. — С. 3–22.

6. Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k-значной логики полиномами по модулю k // В кн. Многоустойчивые элементы и их применение. — М.: Сов. радио, 1971. — С. 84–88.

7. Мещанинов Д. Г. Метод построения полиномов для функций k-значной логики // Дискретная математика. — 1995. — Т. 7, вып. 3. — С. 48–60.

8. Селезнева С. Н. Линейная оценка схемной сложности распознавания полиномиальности функций над кольцом вычетов по составному модулю // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2013. — № 1. — С. 27–31.

О ДЛИНЕ СИММЕТРИЧЕСКИХ ПЕРИОДИЧЕСКИХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ В КЛАССЕ ПОЛЯРИЗОВАННЫХ ПОЛИНОМИАЛЬНЫХ ФОРМ

С. Н. Селезнева, М. М. Гордеев (Москва)

В работе получены необходимые и достаточные условия того, что длина последовательности симметрических периодических функций с одним и тем же периодом в классе поляризованных полиномиальных форм равна по порядку функции Шеннона в этом классе.

Пусть $E_k = \{0, 1, \dots, k-1\}$, где $k \geq 2$ — натуральное число, $P_k = \{f^{(n)} : E_k^n \to E_k \mid n = 0, 1, 2, \dots\}$ — множество всех функций k-значной логики. *Поляризованной полиномиальной формой* (ППФ) по *вектору поляризации* $\delta = (d_1, \dots, d_n) \in E_k^n$ назовем выражение $\sum\limits_{j=1}^{l} c_j (x_1 + d_1)^{m_{j1}} \cdot \ldots \cdot (x_n + d_n)^{m_{jn}}$, где $c_j \in E_k$ — коэффициенты, $m_{j1}, \dots, m_{jn} \in E_k$ — степени, сложение и умножение рассматриваются по модулю k. *Длиной* $l(P)$ ППФ P называется число ее попарно различных слагаемых с ненулевыми коэффициентами.

Если k — простое число, то каждая функция $f(x_1,\ldots,x_n) \in P_k$ представима однозначной ППФ $P^{\delta}(f)$ по каждому вектору поляризации $\delta \in E_k^n$. Далее считаем, что k — простое число. *Длиной* $l(f)$ функции $f \in P_k$ в классе ППФ называется наименьшая длина среди всех ППФ, представляющих эту функцию. Рассматривается *функция Шеннона* $L_k^{\text{ППФ}}(n)$ длины функций k-значной логики в классе ППФ как наибольшая длина в классе ППФ среди всех функций, зависящих от n переменных.

В [1] получено точное значение функции Шеннона для функций алгебры логики: $L_2^{\text{ППФ}}(n) = \lfloor \frac{2}{3} \cdot 2^n \rfloor$. В [2] найдена верхняя оценка функции Шеннона при $k \geq 3$: $L_k^{\text{ППФ}}(n) \leq \frac{k(k-1)}{k(k-1)+1} \cdot k^n$, которая в [3] усилена: $L_k^{\text{ППФ}}(n) \leq \frac{k(k-1)-1}{k(k-1)} \cdot k^n$. В [4] получена нижняя оценка функции Шеннона: $\frac{k-1}{k} \cdot k^n \lesssim L_k^{\text{ППФ}}(n)$. В [1] построены последовательности таких функций $f_n(x_1,\ldots,x_n) \in P_2$, что $l(f_n) \geq \lfloor \frac{2}{3} \cdot 2^n \rfloor$, в [5, 6] получены последовательности таких функций $f_n(x_1,\ldots,x_n) \in P_3$, что $l(f_n) \geq \lfloor \frac{3}{4} \cdot 3^n \rfloor$. Отметим, что в [1, 6] указанные последовательности составлены из симметрических периодических функций с одним и тем же периодом.

Периодической функцией k-значной логики $f_\tau^{(n)}(x_1,\ldots,x_n)$ с периодом $\tau = (\tau_0, \tau_1, \ldots, \tau_{T-1}) \in E_k^T$ длины $T \geq 1$ назовем следующую функцию: для набора $\alpha = (a_1,\ldots,a_n) \in E_k^n$ верно $f_\tau^{(n)}(\alpha) = \tau_s$, если $\sum\limits_{i=1}^{n} a_i = s \pmod T$. Периодические функции являются *симметрическими*, т.е. не меняются при любой перестановке их переменных. Отметим, что период $\tau \in E_k^T$ задает последовательность периодических функций $\{f_\tau^{(n)}\}$, $(n = 1, 2, \ldots)$. Период $\tau \in E_k^T$ называется *сложным*, если найдутся такое натуральное число $n_0 \geq 1$ и такое действительное число $C > 0$, что $l(f_\tau^{(n)}) \geq C \cdot k^n$ при $n \geq n_0$, и называется *вырожденным*, если $l(f_\tau^{(n)}) = o(k^n)$ при $n \to \infty$.

Рассмотрим матрицы $A_d \in E_k[k \times k]$, $d \in E_k$ из [7]: $A_d[0,-d] = 1$, $A_d[0,j] = 0$ при $j \neq -d$, $A_d[i,j] = -(j+d)^{k-1-i}$ при $i = 1,\ldots,k-1$ (считаем, что $0^0 = 1$). Построим матрицы $B_{d,s}^{(T)} \in E_k[T \times T]$, $d, s \in E_k$, $T \geq k$: выберем строку с номером s в матрице A_d и дополним ее справа нулями до T столбцов, в результате получим строку $b_{d,s}^{(T)}$, которая является первой строкой матрицы $B_{d,s}^{(T)}$, а каждая следующая стро-

ка этой матрицы получается из предыдущей сдвигом вправо на один элемент.

Если $\tau \in E_k^T$, то положим $B_0(\tau) = \{\tau\}$, $B_{t+1}(\tau) = \{B_{d,s}^{(T)}\sigma \mid \sigma \in B_t, d, s \in E_k\}$, $t \geq 1$, и $B(\tau) = \bigcup\limits_{t\geq 0} B_t(\tau)$. Периоды из множества $B(\tau)$ назовем *порожденными* периодами для периода τ.

Теорема 1. *Пусть k — простое число.*

1. *Период $\tau \in E_k^T$ является сложным в том и только в том случае, когда $\tilde{0} \notin B(\tau)$, где $\tilde{0} = (0, \ldots, 0) \in E_k^T$ — нулевой период длины T, при этом $l(f_\tau^{(n)}) \geq \frac{1}{kT} \cdot k^n$ для всех n, начиная с некоторого n_0.*

2. *Период $\tau \in E_k^T$ является вырожденным в том и только в том случае, когда $\tilde{0} \in B(\tau)$, где $\tilde{0} = (0, \ldots, 0) \in E_k^T$ — нулевой период длины T.*

Следствие 1. *Если k — простое число, то для произвольного периода $\tau \in E_k^T$ верно, что либо он сложный, либо он вырожденный.*

Следствие 2. *Если k — простое число, то задача выяснения по заданному периоду $\tau \in E_k^T$, он сложный или вырожденный, является алгоритмически разрешимой.*

Теорема 2. *Если k — простое число и T взаимно просто с k, то все ненулевые периоды $\tau \in E_k^T$ с нулевой суммой компонент являются сложными в том и только в том случае, когда все однородные системы уравнений с матрицами $B_{d,s}^{(T)}$, $d, s \in E_k$, не имеют других решений, кроме $(c, \ldots, c) \in E_k^T$, $c \in E_k$.*

Следствие 3. *Если k — простое число, то задача выяснения по заданному числу T, взаимно простому с k, все ли ненулевые периоды $\tau \in E_k^T$ с нулевой суммой компонет сложные, является алгоритмически разрешимой.*

Работа частично поддержана РФФИ, грант 16–01–00593-а.

Список литературы

1. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, вып. 3. — С. 323–326.

2. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.

3. Балюк А. С., Янушковский Г. В. Верхние оценки функций над конечными полями в некоторых классах кронекеровых форм // Из-

вестия Иркутского государственного университета. Серия: Математика. — 2015. — Т. 14. — С. 3–17.

4. Алексеев В. Б., Вороненко А. А., Селезнева С. Н. О сложности реализации функций k-значной логики поляризованными полиномами // Сб. Труды V Международной конференции «Дискретные модели в теории управляющих систем» (Ратмино, 26–29 мая 2003 г.). — М.: МАКС Пресс, 2003. — С. 8–9.

5. Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — № 3. — С. 40–45.

6. Селезнева С. Н. Сложность систем функций алгебры логики и систем функций трехзначной логики в классах поляризованных полиномиальных форм // Дискретная математика. — 2015. — Т. 27, вып. 1. — С. 111–122.

7. Селезнева С. Н., Маркелов Н. К. Быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k-значных функций // Ученые записки Казанского университета. Серия Физико-математические науки. — 2009. — Т. 151, книга 2. — С. 151–147.

NP-ПОЛНОТА ЗАДАЧ ПРОВЕРКИ РАЗРЕШИМОСТИ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ И СОВМЕСТНОСТИ ИХ СИСТЕМ

М. Р. Старчак, Н. К. Косовский(Санкт-Петербург)

Для задач, NP-полнота которых доказана, неизвестен эффективный (полиномиальный по числу шагов машины Тьюринга) алгоритм решения. В некоторых случаях фиксированное значение одного из параметров задачи позволяет построить полиномиальный алгоритм, с другой стороны, важно понимать, ограничения на какие параметры оставляют задачу NP-полной.

Многие естественные задачи, встречающиеся в математических исследованиях, допускают переформулировку в виде линейных диофантовых уравнений, а также в виде их систем.

NP-полнота задачи проверки совместности в неотрицательных целых числах систем линейных уравнений с коэффициентами из $\{0, 1\}$ *при переменных.* Обозначим $L(x_1, ..., x_n)$ линейное выражение

вида $a_1x_1 + ...a_kx_k + b$. Линейное уравнение будем записывать в виде $L(x_1, ..., x_n) = 0$. Докажем следующее усиление следствия 18.1a теоремы 18.1 [1].

Теорема 1. *NP-полна задача проверки совместности в неотрицательных целых числах систем линейных уравнений с коэффициентами из* $\{0, 1\}$ *и свободными членами, равными* -1*. При этом в каждом уравнении не более трех коэффициентов при переменных, отличных от нуля.*

Доказательство. Принадлежность задачи классу NP следует из следствия 18.1a [1]. Задача о 3-выполнимости при одном истинном литерале (далее 3-ВПОИЛ) [2] полиномиально сводится к рассматриваемой задаче. Константы истина и ложь кодируются соответственно 1 и 0. Пропозициональные переменные соответствуют переменным для неотрицательных целых чисел. Литералы с отрицанием кодируются дополнительными переменными со штрихом и дополнительными уравнениями вида $x + x' - 1 = 0$. Элементарный дизъюнкт вида $x \vee y \vee z$ кодируется уравнением $x + y + z - 1 = 0$. Совместность в неотрицательных целых числах полученной системы эквивалентна разрешимости 3-ВПОИЛ.

Аналогично доказывается следующее по существу усиление следствия 18.1b [1].

Теорема 2. *NP-полна задача проверки совместности в* $\{0, 1\}$ *числах систем линейных уравнений с коэффициентами из* $\{0, 1\}$ *и свободными членами, равными* -1*. При этом в каждом уравнении не более трех коэффициентов при переменных, отличных от нуля.*

В то же время, несложно показать, что в приведенных теоремах нельзя заменить словосочетание "не более трех" на "не более двух". Имеет место следующее

Утверждение 1. *Принадлежит классу P проверка совместности в неотрицательных целых числах системы линейных уравнений, елси в каждом уравнении не более двух коэффициентов при переменных, отличных от нуля.*

Фиксирование числа переменных, как следует из результата Ленстры (следствие 18.7a [1]), даёт полиномиальный алгоритм решения задачи. В то же время, для любого фиксированного числа, большего 2, ненулевых коэффициентов в каждом уравнении, задача остаётся NP-полной. Как видим, количество ненулевых коэффициентов в уравнениях системы не есть параметр задачи, позволяющий строить при его фиксации полиномиальные по времени алгоритмы.

NP-полнота задачи разрешимости линейных диофантовых уравнений на отрезке. Докажем NP-полноту следующего обобщения задачи СУММА РАЗМЕРОВ [2] и следствия 18.1c из [1].

Теорема 3. *Для любого невырожденного отрезка $[m, m_1 - 1]$ целых чисел NP-полна задача разрешимости в целых числах из этого отрезка линейных уравнений с целыми коэффициентами и отрицательными свободными членами.*

Доказательство. Принадлежность задачи классу NP очевидна, поскольку каждая переменная принимает значения из указанного отрезка. Воспользуемся доказательством Теоремы 1 и аналогично ему осуществим полиномиальное сведение задачи 3-ВПОИЛ к системе линейных уравнений с только тремя ненулевыми коэффициентами. Обозначив $L_i(x_{i,1}, x_{i,2}, x_{i,3}) = x_{i,1} + x_{i,2} + x_{i,3}$, запишем:

$$\begin{cases} L_1 - 3m - 1 = 0 \\ L_2 - 3m - 1 = 0 \\ \vdots \\ L_M - 3m - 1 = 0 \end{cases}.$$

Совместность этой системы в целых числах из отрезка $[m, m_1 - 1]$ равносильна разрешимости на этом отрезке уравнения $(L_1 - 3m - 1) + 3m_1(L_2 - 3m - 1) + ... + (3m_1)^{i-1}(L_M - 3m - 1) = 0$. Таким образом, линейное уравнение вида $\sum_{i=1}^{M}(3m_1)^{i-1}L_i = \dfrac{(3m+1)(3m_1^M - 1)}{3m_1 - 1}$ разрешимо на $[m, m_1 - 1]$ тогда и только тогда, когда задача 3-ВПОИЛ имеет решение. Поскольку M не превосходит размера входных данных, длина записи числа m_1^M не превосходит полинома от длины входных данных.

Заключение. Результаты первой части сообщения указывает на то, что произвольное фиксированное число ненулевых коэффициентов при переменных в системе диофантовых уравнений не даёт в настоящее время существенного уменьшения вычислительной сложности задачи.

Доказательство NP-полноты задачи разрешимости линейного диофантова уравнения на произвольном невырожденном отрезке показывает, что при использовании компьютерного типа *integer* для переменных, на данный момент не известен полиномиальный по времени алгоритм решения этой задачи.

Список литературы

1. Схрейвер А. Теория линейного и целочисленного программирования. Т.2. — М.: Мир, 1991.

2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

АЛГЕБРАИЗАЦИЯ И ОБОБЩЕНИЕ КОНТАКТНЫХ СХЕМ

Ю. Г. Таразевич (Минск)

Предлагается алгебраизация класса контактных схем [1–3], представляющая матрицы инциденций [4] контактных схем как подкласс специального класса *расширенных матриц* (РМ) над кольцом полиномов Жегалкина [2] (ПЖ) и позволяющая:
1) полностью отойти от традиционного «наглядно-геометрического» подхода к задачам эквивалентных преобразований, анализа и синтеза контактных схем и формулировать и решать такие задачи на алгебраическом языке;
2) в рамках класса РМ над кольцом ПЖ естественным образом расширить класс контактных схем (т.е. «контактных графов») до нового нетривиального класса *контактных гиперграфов* (интерпретируемых как неориентированные двумерные «контактные полиэдры»), в котором можно получать, в частности, новые нетривиальные оценки сложности реализации булевых функций.

1. *Расширенные полиномиальные матрицы.* Пусть $P_2^{(n)}$ и $\text{ПЖ}^{(n)}$ — изоморфные кольца булевых функций и полиномов Жегалкина, зависящих от набора переменных $\tilde{x} = (x_1, \ldots, x_n)$.

Определение. *Расширенной матрицей* (РМ-*матрицей*) будем называть произвольную непустую прямоугольную матрицу с одним выделенным *источниковым столбцом*, элементами которой являются произвольные полиномы Жегалкина. Класс всех РМ-матриц (любых размеров) над кольцом $\text{ПЖ}^{(n)}$ обозначим $\text{РМ}^{(n)}$. Подматрицу (возможно пустую), состоящую из неисточниковых столбцов РМ-матрицы, будем называть ее *основной матрицей*.

Определим функционирование РМ-матриц. Любой матрице $A(\tilde{x}) \in \text{РМ}^{(n)}$ и любому булевому набору $\tilde{\alpha} \in \{0,1\}^n$ естественным образом сопоставляется двоичная РМ-матрица $A(\tilde{\alpha}) \in \text{РМ}^{(0)}$, которую можно рассматривать как расширенную матрицу (над полем $\{0,1\}$) системы линейных алгебраических уравнений (СЛАУ) [5]. Через $\Delta_A(\tilde{\alpha})$ обозначим разницу рангов расширенной и основной матрицы этой СЛАУ (в случае пустой основной матрицы ее ранг считается равным нулю). Будем говорить, что *матрица* $A(\tilde{x}) \in \text{РМ}^{(n)}$ *реализует функцию* $f(\tilde{x}) \in P_2^{(n)}$, если для любого набора $\tilde{\alpha} \in \{0,1\}^n$:

$$f(\tilde{\alpha}) = \neg\Delta_A(\tilde{\alpha}) = 1 - \Delta_A(\tilde{\alpha}) \qquad (1)$$

(иначе говоря, $f(\tilde{\alpha}) = 1$, если СЛАУ с матрицей $A(\tilde{\alpha})$ — совместна).

Замечание. Класс $\mathrm{PM}^{(n)}$ можно определить как счетно порожденный модуль [5] над кольцом $\mathrm{ПЖ}^{(n)}$. Кроме того, в классе $\mathrm{PM}^{(n)}$ имеется полная система эквивалентных преобразований [3] (сохраняющих функцию (1)), обобщающая известную систему элементарных преобразований строк и столбцов обычных многочленных матриц [5] и позволяющая любую РМ-матрицу приводить к однозначно определяемому одноэлементному каноническому виду (аналог диагонализации).

2. *Алгебраизация контактных схем.* Покажем, что класс $\mathrm{KC}^{(n)}$ всех двухполюсных контактных схем, построенных из контактов переменных из набора $\tilde{x} = (x_1, \ldots, x_n)$, является, по существу, подклассом класса $\mathrm{PM}^{(n)}$.

Рассмотрим произвольную двухполюсную схему $S(\tilde{x}) \in \mathrm{KC}^{(n)}$, дополненную («расширенную») *источниковым ребром*, соединяющим полюса. Любой такой «расширенной» схеме (т.е. неориентированному графу без петель [4] с одним ребром — источником и остальными ребрами — контактами) естественным образом сопоставляется расширенная двоичная матрица инциденций [4] $A(\tilde{x})$ (по две единицы в каждом столбце), каждый столбец которой, кроме одного (источникового), помечен символом замыкающего (x_i) или размыкающего ($\bar{x}_j$) контакта некоторой переменной. Неисточниковые столбцы матрицы $A(\tilde{x})$ будем называть *контактными столбцами*.

Метки x_i и $\bar{x}_j = x_j \oplus 1$ контактных столбцов матрицы инциденций контактной схемы естественным образом рассматриваются как полиномиальные множители своих столбцов. Тогда, умножив контактные столбцы матрицы инциденций $A(\tilde{x})$ на свои метки (полиномы Жегалкина x_i или $x_j \oplus 1$), получим ту же матрицу инциденций, записанную в собственно *полиномиальном виде*, т.е. $\mathrm{PM}^{(n)}$-матрицу, содержащую по два одинаковых полинома $x_i \oplus \sigma$ в каждом контактном столбце и две единицы в источниковом столбце.

Следующий факт очевиден.

Утверждение. *Имеет место взаимно-однозначное соответствие между цепями контактов, соединяющими полюса в произвольной двухполюсной контактной схеме, дополненной источниковым ребром, и одномерными циклами* [4], *содержащими источниковое ребро этой схемы, такое, что соответствующий цикл объединяет соответствующую цепь и источниковое ребро.*

Так как всякий цикл суть эйлеров подграф [4] (с четными сте-

пенями всех вершин), то легко видеть, что функция, реализуемая двухполюсной схемой $S(\tilde{x})$, совпадает с функцией (1), реализуемой $\text{РМ}^{(n)}$-матрицей, представляющей собой (записанную в полиномиальном виде) матрицу инциденций $A(\tilde{x})$ схемы $S(\tilde{x})$, дополненной источниковым ребром. Таким образом (с учетом замечания), мы имеем алгебраизацию класса $\text{КС}^{(n)}$ как подкласса класса $\text{РМ}^{(n)}$.

3. *Обобщение контактных схем.* Если в двоичных матрицах инциденций контактных схем (т.е. «контактных графов») снять обязательное для графов ограничение — не более двух единиц в столбце, — то получим более широкий (по сравнению с $\text{КС}^{(n)}$) подкласс класса $\text{РМ}^{(n)}$ — *контактные гиперграфы* ($\text{КГ}^{(n)}$) — с существенно более низкой, но все же экспоненциальной функцией Шеннона [1–3] (по порядку $2^{n/2}$ в классе $\text{КГ}^{(n)}$ против $2^n/n$ в классе $\text{КС}^{(n)}$), а также с более низкой, но все же нелинейной нижней оценкой сложности функции Нечипорука [2] ($n^{3/2-o(1)}$ в классе $\text{КГ}^{(n)}$ против $n^{2-o(1)}$ для $\text{КС}^{(n)}$ и формул в конечном базисе).

В итоге получаем цепочку включений $\text{КС}^{(n)} \subset \text{КГ}^{(n)} \subset \text{РМ}^{(n)}$, в которой $\text{РМ}^{(n)}$ — это «максимальный» алгебраический класс (модуль над кольцом $\text{ПЖ}^{(n)}$, с полной системой эквивалентных преобразований), а $\text{КГ}^{(n)}$ — нетривиальный «промежуточный» класс (с новыми оценками сложности реализации булевых функций).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991.

3. Яблонский С. В. Элементы математической кибернетики. — М.: Высш. школа, 2007.

4. Басакер Р., Саати Т. Конечные графы и сети. — М.: Наука, 1974.

5. Мальцев А. И. Основы линейной алгебры. — М.: Наука, 1970.

ОБ ОДНОМ СВОЙСТВЕ СООТНОШЕНИЯ ГЛУБИНЫ И СЛОЖНОСТИ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Тарасов П. Б. (Москва)

В работе рассматривается задача о реализации функций k-значной логики из замкнутых классов формулами в конечных базисах, состоящих из функций, принадлежащих этим же классам. Все необходимые определения можно найти в работах [1–3].

Обозначим через P_k множество всех функций k-значной логики, а через $P_{k,s}$ — множество всех функции k-значной логики, принимающих значения из множества $E_s = \{0, 1, \ldots, s-1\}$, $k \geq s \geq 2$. Пусть A — конечная система функций из P_k. Через $[A]$ обозначим замкнутый класс, порожденный системой A. Пусть Φ — формула над A. Обозначим через $L(\Phi)$ (сложность формулы Φ) число символов переменных, входящих в Φ, а через $D(\Phi)$ — глубину формулы Φ. Пусть $f \in [A]$. Положим $D_A(f) = \min D(\Phi)$, $L_A(f) = \min L(\Phi)$, где минимум берется по всем формулам Φ над A, реализующим f. Конечную систему функций A будем называть равномерной, если существуют такие константы c и d (зависящие только от A), что для любой функции $f \in [A]$ выполнено неравенство

$$D_A(f) \leq c \log_2 L_A(f) + d.$$

В работах [4, 5] доказана равномерность всех конечных полных систем булевых функций (см. также [6]). В [7] установлена равномерность всех конечных систем, порождающих класс M всех монотонных булевых функций. В работах [8, 9] доказана равномерность всех конечных систем булевых функций (см. также [3]).

Ряд публикаций посвящен задаче о соотношении глубины и сложности формул над конечными системами функций многозначной логики [10, 11].

Еще одной очень важной задачей теории управляющих систем является задача сравнения базисов. Конечные системы функций A и B такие, что $[A] = [B]$, называются полиномиально эквивалентными, если существуют такие константы c_1 и c_2, что для любой функции $f \in [A]$ выполнены неравенства

$$(L_A(f))^{c_1} \leq L_B(f) \leq (L_A(f))^{c_2}.$$

В работах [3, 9] доказано, что все конечные системы функций P_2, порождающие один и тот же замкнутый класс, полиномиально эквивалентны. В той же работе приведен пример систем функций из

P_4, порождающих один и тот же замкнутый класс и не являющихся полиномиально эквивалентными. Примеров не полиномиально эквивалентных систем функций из P_3 до настоящего времени не приводилось. Кроме того, не было известно примеров систем, порождающих один и тот же замкнутый класс, часть из которых равномерна, а часть — нет.

Обозначим через $d_3(x_1, x_2, x_3)$ функцию $x_1x_2 \vee x_2x_3 \vee x_1x_3$ из P_2.

Определим функцию $f(x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, z_1, z_2, z_3)$ из $P_{3,2}$ следующим образом. Пусть $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \beta_1, \beta_2, \gamma_1, \gamma_2, \gamma_3) \in E_k^{11}$ — набор значений переменных функции f. Пусть $X = \{(2,2,2,2,1,1), (2,2,1,1,2,2), (2,2,1,1,1,1)\}$, $Y = \{(1,1,2,2,2,2)\}$. Тогда

$$f(\widetilde{\alpha}, \widetilde{\beta}, \widetilde{\gamma}) = \begin{cases} \beta_1 \& \beta_2 \& d_3(\gamma_1, \gamma_2, \gamma_3), & \text{если } \widetilde{\alpha} \in X \text{ и } \beta_i, \gamma_j \in E_2; \\ \beta_1 \vee \beta_2 \vee d_3(\gamma_1, \gamma_2, \gamma_3), & \text{если } \widetilde{\alpha} \in Y \text{ и } \beta_i, \gamma_j \in E_2; \\ 0, & \text{в остальных случаях.} \end{cases}$$

Положим

$$f_2(x_1, x_2, x_3, y, z_1, z_2, z_3) = f(x_1, x_1, x_2, x_2, x_3, x_3, y, y, z_1, z_2, z_3),$$

$$A = \{f\}, \quad A' = \{f, f_2\}.$$

Очевидно, что $[A] = [A']$.

Теорема. *Справедливы следующие утверждения:*

1) *система A равномерна,*
2) *система A' не является равномерной,*
3) *системы A и A' не являются полиномиально эквивалентными.*

Равномерность системы A нетрудно получить, обобщив теорему 1 из работы [11]. Факт, что система A' не является равномерной, следует из теоремы 1 работы [12]. То, что системы A и A' не являются полиномиально эквивалентными, следует из двух предыдущих утверждений и определения полиномиальной эквивалентности.

Автор благодарен Р. М. Колпакову и О. С. Дудаковой за обсуждение результатов работы и ряд ценных замечаний.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

2. Lau D, Function Algebras on Finite Sets. — Springer-Verlag Berlin Heidelberg, 2006

3. Угольников А. Б. О глубине и полиномиальной эквивалентности формул для замкнутых классов двузначной логики // Математические заметки. — 1987. — Т. 42, вып. 4. — С. 603–612.

4. Яблонский С. В., Козырев В. П. Математические вопросы кибернетики. // Информационные материалы / М.: Научный совет по комплексной проблеме «Кибернетика» АН СССР, 1978. — Вып. 32 — С. 76–94.

5. Spira P. M. On time-hardware complexity tradeoffs for Boolean functions // Proc. 4th Hawai Symposium on System Sciences, North Hollywood, 1971. — P. 525–527.

6. Храпченко В.М. О соотношении между сложностью и глубиной формул // Методы дискретного анализа в синтезе управляющих систем. — 1978. — Вып. 32. — С. 76–94.

7. Wegener I. Relating Monotone Formula Size and Monotone Depth of Boolean Functions // Information Processing Letters. — 1983. — 16. — P. 41–42.

8. Угольников А. Б. О соотношении между глубиной и сложностью формул для замкнутых классов двузначной логики // IV Всесоюзная конференция "Применение методов математической логики": тезисы докладов. Таллин. 1986. — С. 184.

9. Ragaz M. E. Parallelizable algebras // Archiv fur mathematische Logik und Grundlagenforschung. — 1986. — 26(7) — P. 77–99.

10. Сафин Р. Ф. О глубине и сложности формул в некоторых классах k-значной логики // Вестн. Моск. ун-та. Сер. 1, Математика. Механика. — 2000. — № 6. — С. 65–68.

11. Тарасов П. Б. О некоторых достаточных условиях равномерности систем функций многозначной логики // Вестн. Моск. ун-та. Сер 1. Математика. Механика. — 2013. — № 5. — С. 41–46.

12. Тарасов П. Б. Некоторые условия равномерности функций k-значной логики, принимающих значения 0 и 1 // Ученые записки Казанского университета. — 2014. — № 3. — С. 123–129.

СИНТЕЗ РАСПИСАНИЙ В ДИСКРЕТНОЙ МОДЕЛИ ОБСЛУЖИВАНИЯ МУЛЬТПОТОКА ПАКЕТОВ ОБЪЕКТОВ

М. А. Трухина (Нижний Новгород), Д. И. Коган (Москва), Ю. С. Федосенко, А. В. Шеянов (Нижний Новгород)

Рассматривается модель обслуживания стационарным процессором конечного мультипотока объектов [1, 2], поступающих в составе

пакетов [3]; ставятся и исследуются оптимизационные задачи оценки качества расписаний обслуживания. Модель обслуживания адекватно описывает процессы подачи к терминалу грузовой обработки многосекционных судовых составов [4].

Процессор P должен выполнить обслуживание мультипотока M объектов, прибывающих в составе пакетов $O(s)$, $s = \overline{1,h}$. В принимаемых далее обозначениях первый индекс каждого объекта из M совпадает с номером пакета, которому объект принадлежит; второй индекс объекта через порядковый номер идентифицирует его внутри пакета. Количество объектов в пакете $O(s)$ обозначим $n(s)$, $n(s) \geq 1$. Таким образом, каждый пакет $O(s)$ состоит из объектов $o_{s,1}, o_{s,2}, \ldots, o_{s,n(s)}$, подлежащих однократному без прерываний обслуживанию, $s = \overline{1,h}$, а общее количество n таких объектов в мультипотоке M определяется суммой $\sum_{s=1}^{h} n(s)$. Для каждого пакета $O(s)$ считается известным момент t_s, $s = \overline{1,h}$, его поступления в очередь для обслуживания процессором P. Не ограничивая общности рассмотрения, полагаем $0 = t_1 \leq \ldots t_s \ldots \leq t_h$. В начальный момент времени $t = 0$ процессор считается свободным, находясь в состоянии готовности к выполнению обслуживания объектов подпотока $M_{g_0} \in M$. Обслуживание объектов процессором P может выполняться в произвольном порядке, т.е. без учета принадлежности их тому или иному пакету. Длительность обслуживания объекта $o_{s,l}$ определяется значением параметра $\tau_{s,l}$, $s = \overline{1,h}$, $l = \overline{1,n(s)}$.

Каждый объект $o_{s,l}$ характеризуется величиной g — признаком принадлежности объекта к подпотоку M_g, $g = \overline{1,m}$. Если в момент постановки на обслуживание объекта, принадлежащего подпотоку M_j, $j = \overline{1,m}$, процессор P настроен на обслуживание объектов подпотока M_q, $q = \overline{1,m}$, $j \neq q$, то выполняется процедура переналадки процессора. Длительности переналадки с режима обслуживания объекта из подпотока M_j на режим обслуживания объекта из подпотока M_q определены квадратной матрицей $H(h(j,q))$, в которой $h(j,q) > 0$ при $j \neq q$ и $h(j,q) = 0$ при $j = q$ и $j,q = \overline{1,m}$. Обслуживание объекта реализуется процессором без прерываний; в каждый момент времени он может обслуживать только один объект; по завершению обслуживания объект немедленно освобождает процессор; немотивированные простои процессора и объектов запрещены.

Пакет объектов $O(s)$ считается обслуженным, если завершены обслуживанием все входящие в его состав объекты $o_{s,l}$, $l = \overline{1,n(s)}$, $s = \overline{1,h}$.

Стратегия обслуживания записывается как произвольная перестановка $S = ((\alpha_1, \beta_1,), (\alpha_2, \beta_2), \ldots, (\alpha_i, \beta_i), \ldots, (\alpha_n, \beta_n))$ двойных индексов всех объектов, т.е. элементов мультипотока M. При известной стратегии S для каждого объекта $o_{s,l}$ моменты $t^b_{s,l}(S)$ и $t^f_{s,l}(S)$ соответственно начала и завершения обслуживания вычисляются очевидным образом арифметически; обозначаемый через $t^f_s(S)$ момент завершения обслуживания пакета $O(s)$ оказывается равным $\max(t^f_{s,1}(S), t^f_{s,2}(S), \ldots, t^f_{s,n(s)}(S))$.

За время от момента прибытия до момента завершения обслуживания по пакету $O(s)$ налагается штраф $F_s(\Delta) = \alpha_s\Delta$, $\Delta = t^f_s - t_s$, $s = \overline{1,h}$, α_s — величина штрафа за единицу времени пребывания пакета в системе обслуживания. Функция $F_s(\Delta)$ именуется функцией индивидуального штрафа по пакету $O(s)$, $s = \overline{1,h}$.

Рассматриваемые задачи записываются в виде.

1. *Построить расписание обслуживания объектов мультипотока M, минимизирующее суммарный штраф по всем пакетам, т.е.*

$$\min_S \sum_{s=1}^{h} F_s(t^f_s(S) - t_s). \tag{1}$$

2. *Построить расписание обслуживания объектов мультипотока M, минимизирующее значение максимального из индивидуальных штрафов по всем пакетам, т.е.*

$$\min_S \left(\max_{s=\overline{1,h}} F_s(t^f_s(S) - t_s) \right). \tag{2}$$

Для решения задач (1) и (2) в докладе предлагаются алгоритмы, сконструированные на основе схем динамического программирования и ветвей и границ; приводятся результаты вычислительных экспериментов по оценке быстродействия алгоритмов для практически значимых значений параметров модели обслуживания и размерности мультипотока M.

Работа выполнена при финансовой поддержке РФФИ (проект 15–07–03141).

Список литературы

1. Коган Д. И., Трухина М. А., Федосенко Ю. С., Шеянов А. В. Модель и алгоритм синтеза стратерий обслуживания мультипотока объектов мобильным процессором // Системы управления и информационные технологии. — 2015. — № 2. — С. 40–44.

2. Трухина М. А., Федосенко Ю. С., Шеянов А. В. Управление обслуживанием мультипотока объектов мобильным процессором // Труды IX Международной конференции “Дискретные модели в теории управляющих систем” (20–22 мая 2015 г.). — М.: МАКС Пресс, 2015. — С. 242–244.

3. Коган Д. И., Федосенко Ю. С. Однопроцессорное обслуживание потока пакетов объектов: модели и синтез оптимальных стратегий // Вестник МГТУ МИРЭА — М.: Изд-во МГТУ МИРЭА. — 2015. — Т. II, № 3. — С. 108–117.

4. Федосенко Ю. С., Трухина М. А. Каноническая модель и задача синтеза стратегий однопроцессорного обслуживания потока пакетов объектов // Материалы IV Международной научно-практической конференции “Информационные управляющие системы и технологии” (22–24 сентября 2015 г.). — Одесса: Изд-во Одесского национального морского университета, 2015. — С. 83–85.

КОНВЕЙЕРНОЕ ГЕНИРИРОВАНИЕ ДИСКРЕТНЫХ МАРКОВСКИХ ПРОЦЕССОВ НА ОСНОВЕ РАЗЛОЖЕНИЯ СТОХАСТИЧЕСКИХ МАТРИЦ

С. В. Шалагин (Казань)

Предложен метод конвейерного генерирования дискретных марковских процессов (ДМП), заданных стохастическими матрицами (СМ). Метод не предполагает каких-либо ограничений ни на структуру СМ, ни на вид ее элементов.

Известна задача синтеза конечных цепей Маркова и их стохастических функций, задаваемых СМ. Примерно с 70-х годов XX века известен метод разложения СМ на имплицирующий вектор и стохастические булевы матрицы [1–3]. Были предложены различные модификации указанного метода, которые имеют ограничения в зависимости как от вида элементов СМ [4], так и от структуры самой СМ [5, 6]. Предложенный в [7] и развиваемый в данной работе метод разложения СМ не предполагает каких-либо ограничений ни на ее структуру, ни на вид ее элементов.

Для СМ размерности l на n имеет место выражение [3]:

$$P_{l\times n} = \sum_{b=1}^{B} a_b \cdot A_b, \tag{1}$$

где $B \le (n-1)\cdot l+1$, (a_b) — имплицирующий вектор (ИВ), $(A_b)_{l\times n}$ — система стохастических булевых матриц, $b = \overline{1,B}$. Является актуальной задача снижения верхней границы для значения B, имеющего порядок $O(n \cdot l)$.

СМ $P_{l\times n}$ представима согласно выражению:

$$P_{l\times n} = \left(\hat{P}^{(i)}_{1\times d} \cdot P_{d\times n}(i)\right), i = \overline{1,l}, \tag{2}$$

где $\hat{p}^{(i)}_{1\times d} = \left(\hat{p}^{(i)}_1 ... \hat{p}^{(i)}_d\right)$, $P_{d\times n}(i) = \left(M^{(i)}_1 ... M^{(i)}_d\right)\cdot S_d$, $\hat{p}^{(i)}_k = \sum_{j\in D_k} p_{ij}$, $M^{(i)}_k = \left(p_{ij}/\hat{p}^{(i)}_k\right)_{1\times q}$, $j \in D_k$, $k = \overline{1,d}$, $q =]n/d[$, S_k — $(d\times n)$-матрица, в которой k-я строка содержит значения «1», а остальные элементы — значения «0», $i = \overline{1,l}$. Справедлива [7]

Лемма. *Любая стохастическая матрица $P_{l\times n}$ представима согласно* (2).

Лемма обосновывает метод конвейерного генерирования ДМП, включающий два этапа (две ступени конвейера):

1) получение дискретной случайной величины $\hat{X} \in [1,d]$, распределенной в соответствии со СМ $\hat{P}_{l\times d} = \left(\hat{P}^{(i)}_{1\times d}\right)_{l\times 1} = \left(\hat{p}^{(i)}_k\right)_{l\times d}$, при заданном значении i (начальном состоянии ДМП): $i = \overline{1,l}$, $k = \overline{1,d}$;

2) генерирование значения ДМП в соответствии с одной из d СМ $P_{l\times q}\left(\hat{X}\right) = \left(M^{(i)}_{\hat{X}}\right)$, $k = \overline{1,l}$, при заданном значении $\hat{X}$, $\hat{X} = \overline{1,d}$.

Замечание 1. *Если $s = n \mod d \neq 0$, то столбцы $P_{l\times q}\left(\hat{X}\right)$ под номерами $\overline{1+s,q}$ – нулевые.*

СМ вида $\hat{P}_{l\times d}$ представима на основе разложения вида (1): $\hat{P}_{l\times d} = \sum_{f=1}^{\hat{B}} \hat{a}_f \cdot \hat{A}_f$, где $\hat{B} \le (d-1)\cdot l + 1$.

Верхняя оценка для $\hat{B}$ имеет порядок $O(d \cdot l)$. Множество СМ

мощности d вида $\left\{P_{l\times q}\left(\hat{X}\right)\right\}$, $\hat{X}=\overline{1,d}$, представимо согласно (1):

$$P_{l\times q}\left(\hat{X}\right)=\sum_{h=1}^{B}a_h\left(\hat{X}\right)\cdot A_h,$$

где $B\le(q-1)\cdot l+1$. Варьируя ИВ $\left(a_h\left(\hat{X}\right)\right)$, $h=\overline{1,B}$, получаем различные СМ из множества $\left\{P_{l\times q}\left(\hat{X}\right)\right\}$, $\hat{X}=\overline{1,d}$. Верхняя оценка B имеет порядок $\mathrm{O}(n\cdot l/d)$. Значения $\left(M_{\hat{X}}^{(i)}\right)$, $i=\overline{1,l}$, $\hat{X}=\overline{1,d}$, получены согласно (2). На основе леммы справедлива

Теорема. *Для $d<n$ СМ $P_{l\times n}$ представима согласно* (2) *на основе разложений вида (1): $\hat{P}_{l\times d}=\sum_{f=1}^{B}\hat{a}_f\cdot\hat{A}_f$ и $P_{l\times q}\left(\hat{X}\right)=\sum_{h=1}^{B}a_h\left(\hat{X}\right)\cdot A_h$, $\hat{X}=\overline{1,d}$, причем $\hat{B}\le(d-1)\cdot l+1$, $B\le(q-1)\cdot l+1$.*

Согласно теореме, для $d=]\sqrt{n}[$, порядок верхних оценок для величин $\hat{B}$ и B составляет $\mathrm{O}(l\cdot\sqrt{n})$.

Замечание 2. *Возможно рекурсивное применение предложенного метода к стохастическим матрицам $\hat{P}_{l\times d}$ и $P_{l\times q}\left(\hat{X}\right)$, $d=]\sqrt{n}[$, полученным согласно* (2) *на основе исходной СМ $P_{l\times n}$.*

В случае t-кратного рекурсивного применения предложенного метода, $t=1,2,...$, значение $d=]n^{2^{-t}}[$, порядок верхних оценок для величин $\hat{B}$ и B каждом из разложений будет равен $\mathrm{O}\left(l\cdot n^{2^{-t}}\right)$.

Список литературы

1. Поспелов Д. А. Вероятностные автоматы — М.: Энергия, 1970.
2. Ченцов В. М. Об одном методе синтеза автономного стохастического автомата // Кибернетика. — 1968. — № 3. — С. 32–35.
3. Лоренц А. А. Синтез надежных вероятностных автоматов. — Рига: Зинатне, 1975.
4. Захаров В. М. Анализ алгоритмов разложения двоичнорациональных стохастических матриц на комбинации булевых матриц // Информационные технологии. — 2008. — № 3. — С. 54–59.
5. Кузнецов С. Е., Нурмеев Н. Н., Салимов Ф. И. Задача о минимальном имплицирующем векторе // Математические вопросы кибернетики. Вып. 3. — 1991. — С. 199–216.
6. Альпин Ю. А., Захаров В. М., Моделирование случайных последовательностей автономными автоматными схемами // Вероят-

ностные автоматы и их приложения. — Казань: Изд-во КГУ, 1986. — С. 22–29.

7. Шалагин С. В. Метод разложения стохастических матриц для синтеза конвейерных генераторов дискретных марковских процессов // Вестник технологического университета. — 2015. — Т. 18, Вып. 10. — С. 160–162.

Секция «Функциональные системы»

О ВЫРАЗИМОСТИ АВТОМАТОВ ОТНОСИТЕЛЬНО СУПЕРПОЗИЦИИ ПРИ НАЛИЧИИ В БАЗИСЕ БУЛЕВЫХ ФУНКЦИЙ И ЗАДЕРЖКИ

Д. Н. Бабин, А. А. Летуновский (Москва)

Известно, что в общем случае работа со схемами автоматов наталкивается на существенные трудности [1]. Так в работе [2] установлена континуальность множества предполных классов для систем автоматных функций, а в работе М. И. Кратко [3] установлена алгоритмическая неразрешимость задачи полноты относительно суперпозиции для конечных систем автоматных функций.

Ограничение арности (числа входов) систем автоматов не важно, так как системы, состоящие из автоматов с двумя входами уже образуют полную систему [4].

Альтернативным подходом к полноте автоматов относительно суперпозиции является теорема Крона—Роудза [5], в которой рассматривается частный случай: автоматы с полной системой переходов и максимально возможным числом состояний. Соотношение теоремы Крона—Роудза и общего случая суперпозиции автоматов описано в [6].

Ранее в задачах полноты относительно суперпозиции и обратной связи хорошо зарекомендовал себя метод использования систем функций, содержащих фиксированную добавку [7, 8]. Такой же метод применяется нами для выразимости автоматов относительно одной только суперпозиции.

Авторы вводят понятие *расширенной* суперпозиции, как суперпозиции с обязательным наличием в системе "задержки" и функции Шеффера. Для расширенной суперпозиции авторам удалось доказать алгоритмическую разрешимость задачи выразимости для широкого класса автоматных функций: константных автоматных функций [9], групповых автоматных функций Медведева [10], а также линейных автоматных функций, что в случае обычной суперпозиции было алгоритмически неразрешимо. Выразимость линейных автоматных функций была расмотрена в работе [11].

Класс всех автоматных функций обозначим через P. Константной автоматной функцией назовем автоматную функцию, выдающую одно и тоже периодическое сверхслово на всех входных сверхсловах. Класс константных автоматных функций обозначим через K.

Автомат $A = (E_2^k, Q, E_2^l, \phi, \psi, q_0), Q \subset E_2^n$, называется *групповым,* если для любого $a \in E_2^k$ отображение $\phi_a : Q \to Q$ — биекция. Здесь $\phi_a : (q) = \phi(q, a)$. Автомат называется *автоматом Медведева,* если $B = Q$ и $\psi(q, a) = q$. Класс всех линейных автоматных функций обозначим через L. Будем обозначать замыкание системы автоматов M относительно расширенной суперпозиции через $< M >$.

Результат М. И. Кратко [3] об алгоритмической неразрешимости выразимости константных автоматов можно в наших обозначениях представить так.

Теорема 1 [3]. *Не существует алгоритма, проверяющего выразимость константой автоматной функции суперпозициями элементов конечной системы автоматных функций.*

Теорема 2 [7]. *Пусть $M \in P$, $|M| < \infty$, $K_1 \in K$. Тогда задача $K_1 \in< M >$ алгоритмически разрешима.*

Теорема 3 [8]. *Пусть $M \in P$, $|M| < \infty$, G_1 - групповой автомат Медведева. Тогда задача $G_1 \in< M >$ алгоритмически разрешима.*

Теорема 4. *Пусть $M \in P$, $|M| < \infty$, $L_1 \in L$. Тогда задача $L_1 \in< M >$ алгоритмически разрешима.*

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов — М.: Наука, 1985.

2. Кудрявцев В. Б. О мощности множеств предполных классов некоторых функциональных систем, связанных с автоматами // Проблемы кибернетики, вып.13. — 1965. — С. 45–74.

3. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, вып. 1. — С. 35–37.

4. Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная матетматика. — 1989. — Т. 1, вып. 4. — С. 423–431.

5. Арбиб М. А. Алгебраическая теория автоматов, полугрупп и языков. — М.: Наука, 1975.

6. Алешин. С. В. Об одном следствии теоремы Крона—Роудза // Дискретная математика — 1999. — Т. 11, вып. 4 — С. 101–109.

7. Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для о.д.-функций // Математические заметки. —

1972. — Т. 12, вып. 6. — С. 687–697.

8. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. — 1992. — Т. 4, вып. 4 — С. 41–56.

9. Летуновский А. А. О выразимости константных автоматов суперпозициями // Интеллектуальные системы. — 2009. — Т. 13, вып. 1–4. — С. 397–406.

10. Летуновский А. А. О выразимости суперпозициями групповых автоматов Медведева // Интеллектуальные системы. — 2011. — Т. 15, вып. 1–4. — С. 402–412.

11. Летуновский А. А. Выразимость линейных автоматов относительно расширенной суперпозиции // Интеллектуальные системы. — 2015. — Т. 19, вып. 1. — С. 161–170.

ГИСТОГРАММНАЯ ФУНКЦИЯ АВТОМАТА

Д. Н. Бабин, Д. В. Пархоменко (Москва)

Автоматная функция при подаче всех входных слов в общем случае некоторые выходные слова не выдает, а некоторые из них выдает неоднократно. Такая автоматная функция и автомат, ее порождающий, в компактном виде кодируют частоту встречаемости своих выходных слов. Если сопоставить слову число его появлений на выходе автомата, то данное соответствие определяется функцей, названной авторами гистограммной функцией автомата.

Под конечным детерминированным инициальным автоматом, согласно [1] , будем понимать шестерку

$$V = (A, Q, B, \phi, \psi, q_0),$$

где A — входной алфавит, Q — множество состояний, B — выходной алфавит, все три множества конечны, q_0 начальное состояние. Функционирование автомата происходит по тактам времени, согласно каноническим уравнениям, здесь ϕ и ψ функции переходов и выходов, соответственно, q_0 — начальное состояние. Обозначим через $K(A, B)$ множество конечных автоматов с входным алфавитом A и выходным алфавитом B.

Гистограммной автоматной функцией автомата V [2] назовем функцию $\varkappa_V : B^* \to \mathbf{N}^0$, где

$$\varkappa_V(\beta) = |\{\alpha|\overline{\psi}(q_0, \alpha) = \beta\}|.$$

Для натурального p и автомата V, p-языком, порожденным автоматом V назовем множество:

$$L_p(V) = \{\beta|\varkappa_V(\beta) \geq p\}.$$

Назовем классом p-языков множество

$$\mathbf{L}_p = \{L_p(V)|V \in K(A, B)\}.$$

Имеет место

Теорема 1 [3]. *Для всех V и p множество L_p регулярный язык.*

Теорема 2 [4]. *Для натуральных $s \neq p$ выполнено $\mathbf{L}_s \not\supseteq \mathbf{L}_p$.*

Теорема 3 [4]. *Существует алгоритм, который для любого регулярного языка L, определяет все те p, для которых $L \in \mathbf{L}_p$.*

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Бабин. Д. Н. Частотные регулярные языки // Интеллектуальные системы. — 2014. — Т. 18, вып. 1. — С. 205–210.

3. Пархомнеко Д. В. Вторая автоматная функция и с нею связанные классы регулярных языков // Интеллектуальные системы. — 2013. — Т. 17, вып. 1–4.

4. Пархоменко Д. В. Порожденные автоматами p-языки // Дискретная математика. — 2014. — Т. 26, вып. 1. — С. 96–102.

О МАКСИМАЛЬНЫХ КЛОНАХ ЧАСТИЧНЫХ УЛЬТРАФУНКЦИЙ

С. А. Бадмаев, И. К. Шаранхаев (Улан-Удэ)

Пусть $A = \{0, 1\}$ и $F = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$. Определим следующие множества функций:

$$P^{\overline{*}}_{2,n} = \{f|f : A^n \to F\},\ P^{\overline{*}}_2 = \bigcup_n P^{\overline{*}}_{2,n},$$

$P_{2,n} = \{f | f \in P_{2,n}^{\overline{*}}$ и $|f(\tilde{\alpha})| = 1$ для всех $\tilde{\alpha} \in A^n\}$, $P_2 = \bigcup\limits_n P_{2,n}$.

Функции из P_2 называют булевыми функциями, из $P_2^{\overline{*}}$ – мультифункциями на A.

Для того, чтобы суперпозиция

$$f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)),$$

где $f, f_1, \ldots, f_n \in P_2^{\overline{*}}$, определяла мультифункцию $g(x_1, \ldots, x_m)$, следуя [1, 2], определим значения мультифункции g на наборах из подмножеств множества A следующим образом: если $(\alpha_1, \ldots, \alpha_m) \in A^m$, то

$$g(\alpha_1, \ldots, \alpha_m) = \begin{cases} \bigcap\limits_{\beta_i \in f_i(\alpha_1, \ldots, \alpha_m)} f(\beta_1, \ldots, \beta_n), & \text{если не пусто;} \\ \bigcup\limits_{\beta_i \in f_i(\alpha_1, \ldots, \alpha_m)} f(\beta_1, \ldots, \beta_n), & \text{в противном случае.} \end{cases}$$

На наборах, содержащих $\varnothing$, мультифункция принимает значение $\varnothing$. Это определение позволяет вычислить значение $f(x_1, \ldots, x_n)$ на любом наборе $(\sigma_1, \ldots, \sigma_n) \in F^n$.

Если мультифункции на A рассматриваются с данной суперпозицией, то их называют частичными ультрафункциями на A.

Клоном называется множество функций, замкнутое относительно суперпозиции, добавления и удаления несущественных переменных, содержащее все проекции.

Клон K называется максимальным, если не существует клона K_1 такого, что $K \subset K_1 \subset P_2^{\overline{*}}$.

Для упрощения записи используется следующая кодировка: $\varnothing \leftrightarrow *$, $\{0\} \leftrightarrow 0$, $\{1\} \leftrightarrow 1$, $\{0, 1\} \leftrightarrow 2$.

Обозначим через $Pol(R)$ класс функций, сохраняющих предикат R.

Теорема. *Класс $Pol(R)$ является максимальным клоном частичных ультрафункций на A, где*

$$R = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 0 & 1 & 2 & * & * & * & * & * & * & * \\ 0 & 1 & 0 & 1 & 1 & 1 & 2 & 1 & 2 & * & * & * & 0 & 1 & 2 & * & * & * & * \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & * & * & * & * & * & * & 0 & 1 & 2 & * \end{pmatrix}$$

или

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 2 & * & * & * & * & * & * & * \\ 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 2 & * & * & * & 1 & 0 & 2 & * & * & * & * \\ 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 2 & * & * & * & * & * & * & 1 & 0 & 2 & * \end{pmatrix}.$$

Список литературы

1. Бадмаев С. А., Шаранхаев И. К. Минимальные частичные ультраклоны на двухэлементном множестве // Известия Иркутского гос. университета. Серия Математика. — 2014. — Т. 9. — С. 3–9.

2. Пантелеев В. И. О двух максимальных мультиклонах и частичных ультраклонах // Известия Иркутского гос. университета. Серия Математика. — 2012. — Т. 5, № 4. — С. 46–53.

РЕШЕТКА ЗАМКНУТЫХ КЛАССОВ ТРЕХЗНАЧНОЙ ЛОГИКИ, СОДЕРЖАЩИХ ФУНКЦИЮ МАКСИМУМА ДЛЯ НЕЛИНЕЙНОГО ЧАСТИЧНОГО ПОРЯДКА

Г. В. Боков (Москва)

Центральной задачей для функциональных систем конечнозначных функций является изучение и описание структуры замкнутых классов. Основополагающую роль в изучении данной структуры для двузначной логики играет результат Поста [1]. Описание решетки замкнутых классов k-значных функций уже при $k \geq 3$ натолкнулось на принципиальные трудности, связанные с континуальным обилием замкнутых классов, обнаруженных Яновым и Мучником [2], вследствие чего исследование этой решетки стало иметь лишь фрагментарный характер [3]. Новый взгляд на соответствие Галуа между замкнутыми классами функций и предикатов позволил продвинуться в решении данных проблем. Так, например, недавно Жук [4] в терминах данного соответствия описал структуру континуальной решетки замкнутых классов самодвойственных функций трехзначной логики.

В данной работе, используя соответствия Галуа между функциями, и предикатами описана структура решетки замкнутых классов

функций трехзначной логики, содержащих функцию максимума для частичного порядка $\{(0,2),(1,2)\}$:

$$f(x,y)=\begin{cases}2, & x=2\vee y=2;\\ 1, & x=0\vee y=0;\\ 0, & \text{иначе.}\end{cases}$$

Пусть $E_k=\{0,1,\ldots,k-1\}$ и

$$P_k^{(n)}=\{f\mid f\colon E_k^n\to E_k\},\quad P_k=\bigcup_{n\geq 1}P_k^{(n)},$$
$$R_k^{(m)}=\{\rho\mid \rho\subseteq E_k^m\},\qquad R_k=\bigcup_{m\geq 1}R_k^{(m)}.$$

Для $Q\subseteq P_k$ и $S\subseteq R_k$ определим $[Q]$ — замыкание относительно суперпозиции и $[S]$ — замыкание относительно позитивных формул первого порядка [3]. Предполагаем, что $[Q]$ содержит селекторы и $[S]$ содержит предикаты $\{\emptyset,=\}$.

Функция $f\in P_k^{(n)}$ *сохраняет* предикат $\rho\in R_k$, если для любых $\alpha_1,\ldots,\alpha_n\in\rho$ выполнено $f(\alpha_1,\ldots,\alpha_n)\in\rho$. Положим

$$\mathrm{Pol}(\rho)=\{f\in P_k\mid f\text{ сохраняет }\rho\},\quad \mathrm{Pol}(S)=\bigcap_{\rho\in S}\mathrm{Pol}\rho,$$
$$\mathrm{Inv}(f)=\{\rho\in R_k\mid f\text{ сохраняет }\rho\},\quad \mathrm{Inv}(Q)=\bigcap_{f\in Q}\mathrm{Inv}f.$$

Тогда $Q=\mathrm{Pol}(\mathrm{Inv}(Q))$ для любого $Q=[Q]\subseteq P_k$ и $S=\mathrm{Inv}(\mathrm{Pol}(S))$ для любого $S=[S]\subseteq R_k$.

При $n\geq 1$, $1\leq m\leq 3$ и $l\geq 2$ введем следующие обозначения:

$$\begin{aligned}
\rho_{\vee,n}(x_1,x_2,\ldots,x_n)=1 &\;\Leftrightarrow\; x_1=2\vee x_2=2\vee\ldots\vee x_n=2,\\
\rho_{\to,m}(x_1,x_2,\ldots,x_m)=1 &\;\Leftrightarrow\; x_1\neq 2\vee x_2=2\vee\ldots\vee x_m=2,\\
\rho_{=,l}(x_1,x_2,\ldots,x_l)=1 &\;\Leftrightarrow\; x_1=x_2\vee x_3=2\vee\ldots\vee x_l=2,\\
\rho_{\sim}(x_1,x_2)=1 &\;\Leftrightarrow\; \rho_{\to,2}(x_1,x_2)\wedge\rho_{\to,2}(x_2,x_1),\\
\rho_{\simeq}(x_1,x_2,x_3)=1 &\;\Leftrightarrow\; \rho_{\sim}(x_1,x_2)\wedge\rho_{=,3}(x_1,x_2,x_3),\\
\rho_{\bar{\wedge}}(x_1,x_2,x_3)=1 &\;\Leftrightarrow\; \rho_{\to,1}(x_1)\wedge\rho_{\to,1}(x_2)\wedge\rho_{=,3}(x_1,x_2,x_3),
\end{aligned}$$

$$P_3=\mathrm{Pol}(\emptyset),\quad T_n=\mathrm{Pol}(\rho_{\vee,n}),\quad F_m=\mathrm{Pol}(\rho_{\to,m}),\quad E_l=\mathrm{Pol}(\rho_{=,l}),$$
$$M=\mathrm{Pol}(\rho_{\sim}),\quad S=\mathrm{Pol}(\rho_{\simeq}),\quad I=\mathrm{Pol}(\rho_{\bar{\wedge}}).$$

Определим счетное семейство Θ замкнутых классов, являющихся пересечением конечного числа классов из P_3, T_n, F_m, E_l, M, S, I.

Пусть $\mathcal{B}_n$ — множество всех подмножеств в $\{1,\dots,n\}$, $\mathcal{E}_n$ — множество отношений эквивалентностей на $\{1,\dots,n\}$ и $\mathcal{E}_n^* = \mathcal{E}_n \cup \{\bot, \top\}$, причем $\bot \subseteq A$ и $A \subseteq \top$ для всех $A \in \mathcal{E}_n$. Отображение $\xi\colon \mathcal{B}_n \to \mathcal{E}_n^*$ назовем *характеристическим*, если $\xi(\{1,\dots,n\}) \neq \bot$, $\xi(\emptyset) \neq \top$, $M_1 \subseteq M_2 \;\Rightarrow\; \xi(M_1) \subseteq \xi(M_2)$, $\xi(M_1), \xi(M_2) \neq \bot \;\Rightarrow\; \xi(M_1 \cap M_2) \neq \bot$ и $\xi(M) \in \mathcal{E}_n$ для некоторого $M \in \mathcal{B}_n$. Множество всех таких отображений обозначим через $\mathcal{X}_n$. Пусть $\mathcal{X} = \bigcup\limits_{n\geq 2} \mathcal{X}_n$. Определим на $\mathcal{X}$ оператор замыкания $[\,]$, порожденный следующими операциями:
1) $\mathrm{tr}\colon \mathcal{X}_m \to \mathcal{X}_n$. Если $\zeta = \mathrm{tr}(\xi)$, то $\zeta(M)$ — минимальный элемент, для которого $\sigma\xi\sigma^{-1}(M) \subseteq \zeta(M)$, где $\sigma\colon \{1,\dots,m\} \to \{1,\dots,n\}$;
2) $\mathrm{pr}\colon \mathcal{X}_{n+m} \to \mathcal{X}_n$. Если $\zeta = \mathrm{pr}(\xi)$, то $\zeta(M)$ — минимальный элемент, для которого $\xi(M) \cap \{1,\dots,n\} \times \{1,\dots,n\} \subseteq \zeta(M)$;
3) $\wedge\colon \mathcal{X}_n \times \mathcal{X}_n \to \mathcal{X}_n$. Если $\zeta = \xi \wedge \eta$, то $\zeta(M)$ — минимальный элемент, для которого $\xi(M) \subseteq \zeta(M)$ и $\eta(M) \subseteq \zeta(M)$.
Подмножество $X = [X] \subseteq \mathcal{X}$ будем называть *замкнутым*.

Пусть $M_\alpha = \{i \mid \alpha(i) \neq 2\}$ для $\alpha \in E_3^n$, где $\alpha(i)$ — элемент с номером i в α. Каждое $\xi \in \mathcal{X}_n$ задает n-местный предикат $\rho_\xi \in R_k^{(n)}$:

$$\rho_\xi(\alpha) = 1 \;\Leftrightarrow\; \xi(M_\alpha) \in \mathcal{E}_n \text{ и } \forall i,j \in \xi(M_\alpha)\colon \alpha(i) = \alpha(j).$$

Положим $R_X = \{\rho_\xi \mid \xi \in X\}$ для $X \subseteq \mathcal{X}$ и определим континуальное семейство замкнутых классов $\Xi = \{\mathrm{Pol}(X) \mid X = [X] \subseteq \mathcal{X}\}$.

Теорема. *Если $Q = [Q] \subseteq P_3$, то $f \in Q \;\Leftrightarrow\; Q \in \Theta \cup \Xi$.*

Для семейства Θ полностью описана решетка по включению. Попарная вложенность классов из семейства Ξ определяется условием

$$R_{[X]} = [R_X], \quad R_{[X]} \subseteq R_{[Y]} \;\Leftrightarrow\; [X] \subseteq [Y]$$

для всех $X, Y \subseteq \mathcal{X}$. Попарная вложенность клонов из семейств Θ и Ξ между собой полностью определяется из того факта, что $\Theta \cap \Xi \neq \emptyset$.

Теорема. *Все классы из $\Theta \cup \Xi$ имеют базис.*

Кроме того, показано, что все классы из Θ имеют конечный базис, состоящий из не более чем 4 элементов. Так как семейство Ξ континуальное, то в Ξ существуют замкнутые классы с бесконечным базисом.

Список литературы

1. Post E. Two-valued iterative systems of mathematical logic. — Princeton: Princeton Univ. Press, 1941.

2. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — Т. 127, № 1 — 1959. — С. 44–46.

3. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Berlin: Springer, 2006.

4. Жук Д. Н. Решетка замкнутых классов самодвойственных функций трехзначной логики. — М.: Издательство МГУ, 2011.

О ПРОВЕРКЕ k-ЗНАЧНОСТИ КОНЕЧНЫХ АВТОМАТОВ-ПРЕОБРАЗОВАТЕЛЕЙ НАД ПОЛУГРУППАМИ

З. А. Джусупекова, В. А. Захаров (Москва)

Автоматы-преобразователи в качестве модели последовательных реагирующих программы используются в системном программировании, в компьютерной лингвистике, в криптографии, при проектировании микроэлектронных схем и др. Преобразователь принимает на входе последовательность сигналов и выполняет некоторую последовательность действий, преобразуя тем самым конечные слова входного алфавита в полугрупповые выражения, значения которых и являются результатами вычислений.

Пусть задана некоторая конечно порожденная полугруппа S. *Конечным автоматом-преобразователем* над полугруппой S называется система $\pi = \langle \Sigma, S, Q, q_{in}, F, T \rangle$, в которой Σ — конечный алфавит, Q — конечное множество состояний, q_{in} — начальное состояние, F — подмножество финальных состояний, $T \subseteq Q \times \Sigma \times S \times Q$ — конечное отношение переходов. *Вычислением* преобразователя π на входном слове $w = a_1 a_2 \dots a_n$ называется последовательность переходов $q_0 \overset{a_1/s_1}{\longrightarrow} q_1 \overset{a_2/s_2}{\longrightarrow} \cdots \overset{a_n/s_n}{\longrightarrow} q_n$, где $q_0 = q_{in}, q_n \in F$. Элемент полугруппы $s_1 s_2 \cdots s_n$ считается *результатом* данного вычисления. Преобразователь π называется *k-значным*, если для любого входного слова количество различных результатов всех возможных вычислений преобразователя на этом слове не превосходит некоторого k.

Далее мы будем рассматривать автоматы-преобразователи над произвольной полугруппой S, которая вложима в некоторую конечно порожденную группу с разрешимой проблемой тождества. В статье [1] было установлено, что задача проверки k-значности конечных автоматов-преобразователей над свободными моноидами разрешима. Затем в статье [2] было показано, что эту задачу можно решить за время, полиномиальное относительно размера преобразователей. Более общий метод анализа поведения автоматов преобразователей над полугруппами, вложимыми в разрешимые группы, был предложен в статье [3]. Однако в этой статье применение этого метода было обосновано только для решения задачи проверки 2-значности автоматов-преобразователей. Цель данной работы — показать, что при помощи метода из [3] можно для любого $k, k \geq 1$, за полиномиальное время проверять свойство k-значности конечных автоматов-преобразователей, работающих над полугруппой, вложимой в конечно порожденные разрешимые группы.

Рассмотрим произвольный преобразователь $\pi = \langle \Sigma, S, Q, q_{in}, F, T \rangle$, и пусть G — разрешимая группа, в которую вложима полугруппа S. Запись $M_\pi[q_0]$ будет обозначать конечный автомат $\langle \Sigma, Q, q_{in}, F, \varphi_\pi \rangle$, в котором отношение переходов задается множеством $\varphi_\pi = \{(q, a, q') : \exists s : q \xrightarrow{a/s} q' \in T\}$. Для проверки свойства k-значности преобразователя π введем систему переходов (LTS) $\Gamma_\pi^k = \langle Q \times (Q \times G)^k, \longrightarrow \rangle$. Отношение переходов $\longrightarrow$ определяется следующим образом: для пары вершин $v_1 = (q_0, (q_1, g_1), \ldots, (q_k, g_k))$ и $v_2 = (q'_0, (q'_1, g'_1), \ldots, (q'_k, g'_k))$ LTS Γ_π^k и произвольной буквы $a, a \in \Sigma$, отношение $v_1 \xrightarrow{a} v_2$ выполняется тогда и только тогда, когда $q_i \xrightarrow{a/s_i} q'_i$, $0 \leq i \leq k$, где $g'_j = (s_0)^{-} g_j s_j$, $1 \leq j \leq k$ и $\bigcap\limits_{i=0}^{k} L(M_\pi[q'_i]) \neq \varnothing$. Вершину $v_{in} = (q_{in}, (q_{in}, e), (q_{in}, e), ..., (q_{in}, e))$, где e — единичный элемент группы G, назовем *стартовой вершиной* LTS Γ_π^k. Множество всех вершин достижимых из стартовой вершины обозначим записью V_π^k. Вершину $(q_0, (q_1, g_1), ..., (q_k, g_k))$ будем называть *опровергающей*, если она удовлетворяет условиям: 1) $q_i \in F$ и $g_i \neq e$ для всех $i = \overline{0, k}$, и 2) $g_i \neq g_j$ для всех пар i, j, $1 \leq i < j \leq k$. Множество всех опровергающих вершин LTS Γ_π^k обозначим записью R_π^k.

Справедливы следующие утверждения

Лемма 1. *Преобразователь π не является k-значным тогда и*

только тогда, когда $V_\pi^k \bigcap R_\pi^k \neq \varnothing$.

Лемма 2. *Пусть множество* V_π^k *содержит* $N = C_{k+1}^2$ *вершин* $v_i = (q^0, (q^1, g_i^1), (q^2, g_i^2), \ldots, (q^k, g_i^k))$, $1 \leq i \leq N$, *удовлетворяющих соотношениям:*
1) $g_i^m \neq g_j^m$ *для всех троек* (m, i, j), *где* $m = \overline{1, N}$, $1 \leq i < j \leq N$,
2) $g_i^m (g_i^n)^- \neq g_j^m (g_j^n)^-$ *для всех четверок* (m, n, i, j), *где* $1 \leq i < j \leq N$, $1 \leq m < n \leq N$.
Тогда $V_\pi^k \bigcap R_\pi^k = \varnothing$.

Лемма 3. *Предположим, что в* $LTS\, \Gamma_\pi^k$ *есть* $k{+}2$ *различных вершин* $v_i = (q^0, (q^1, g_i^1), (q^2, g_i^2), \ldots, (q^k, g_i^k))$, $1 \leq i \leq k+2$, *и пусть все эти вершины удовлетворяют одному из следующих наборов условий для всех пар* i, j *чисел из множества* $\overline{1, k+2}$*:*

$g_i^1 = g_j^1,\ g_i^2 = g_j^2,\ \ldots\ ,\ g_i^{k-2} = g_j^{k-2},\ g_i^{k-1} = g_j^{k-1},$
$g_i^1 = g_j^1,\ g_i^2 = g_j^2,\ \ldots\ ,\ g_i^{k-2} = g_j^{k-2},\ g_i^k = g_j^k,$
$\ldots$
$g_i^2 = g_j^2,\ g_i^3 = g_j^3,\ \ldots\ ,\ g_i^{k-1} = g_j^{k-1},\ g_i^k = g_j^k,$
$g_i^1 = g_j^1,\ g_i^2 = g_j^2,\ \ldots\ ,\ g_i^{k-2} = g_j^{k-2},\ (g_i^{k-1})^- g_i^k = (g_j^{k-1})^- g_j^k,$
$g_i^1 = g_j^1,\ g_i^2 = g_j^2,\ \ldots\ ,\ g_i^{k-3} = g_j^{k-3},\ (g_i^{k-2})^- g_i^{k-1} = (g_j^{k-2})^- g_j^{k-1},$
$\ldots$
$(g_i^1)^- g_i^2 = (g_j^1)^- g_j^2,\ (g_i^1)^- g_i^3 = (g_j^1)^- g_j^3,\ \ldots\ ,\ (g_i^1)^- g_i^k = (g_j^1)^- g_j^k.$

Тогда, если опровергающая вершина достижима из вершины v_{k+2}, *то некоторая опровергающая вершина также достижима из одной из других вершин* v_j, $1 \leq j \leq k+1$.

При помощи лемм 2 и 3 можно доказать следующую теорему.

Теорема 1. *Если полугруппа* S *вложима в конечно порожденную разрешимую группу* G, *то свойство* k*-значности конечных преобразователей над полугруппой* S *разрешимо. Кроме того, если проблема равенства слов в группе* G *разрешима за полиномиальное время, то и свойство* k*-значности конечных преобразователей над* S *разрешима за полиномиальное время.*

Теорема 2. *Свойство* k*-значности преобразователей над свободной полугруппой можно проверить за время* $2^{O(k^2)} \ell m^{k+1} n^{k+1}$, *где* n *— количество состояний,* m *— количество переходов, и* ℓ *— максимальная длина выхода на переходе.*

Работа выполнена при финансовой поддержке гранта РФФИ (проект 15-01-05742).

Список литературы

1. Weber A. Decomposing finite-valued transducers and deciding

their equivalence // SIAM Journal on Computing. — 1993. — V. 22. — P. 175–202.

2. Sakarovitch J., de Souza R. On the decidability of bounded valuedness for transducers // Proceedings of the 33rd International Symposium on Mathematical Foundations of Computer Science. — 2008. — P. 588–600.

3. Захаров В. А. Моделирование и анализ поведения последовательных реагирующих программ // Труды Института системного программирования РАН. — 2015. — Т. 27, вып. 2. — С. 221–250.

КРИТЕРИЙ КОНЕЧНОЙ ПОРОЖДЕННОСТИ КЛАССОВ ФУНКЦИЙ, МОНОТОННЫХ ОТНОСИТЕЛЬНО МНОЖЕСТВ ВЫСОТЫ 5 С НАИМЕНЬШИМ И НАИБОЛЬШИМ ЭЛЕМЕНТАМИ

О. С. Дудакова (Москва)

Известно, что при $k \leq 7$ все предполные классы в $\mathcal{P}_k$ являются конечно-порожденными [1], а начиная с $k = 8$, существуют предполные классы монотонных функций, не имеющие конечного базиса [2]; полного описания конечно-порожденных предполных классов монотонных функций к настоящему времени не получено. В ряде работ (см., например, [3, 4]) выделены некоторые семейства частично упорядоченных множеств, для которых получены критерии конечной порожденности соответствующих классов монотонных функций. В данной работе продолжены исследования в этом направлении.

Пусть $\preccurlyeq$ — частичный порядок на множестве $E_k = \{1, 2, \ldots, k\}$. Положим $\mathcal{P} = (E_k, \preccurlyeq)$. Всюду далее будем считать, что множество $\mathcal{P}$ имеет наименьший и наибольший элементы. Через $\mathcal{M}_\mathcal{P}$ будем обозначать класс всех монотонных функций над $\mathcal{P}$ (отметим, что для множеств с наименьшим и наибольшим элементами класс $\mathcal{M}_\mathcal{P}$ является предполным [5]).

Частично упорядоченные множества называются *изоморфными*, если существует взаимно-однозначное соответствие между их элементами, сохраняющее отношение порядка.

Пусть a_1 и a_2 — элементы множества $\mathcal{P}$, несравнимые относительно $\preccurlyeq$. Элемент $b \in \mathcal{P}$ называется *верхней гранью* элементов a_1 и a_2, если выполняется неравенство $a_1, a_2 \preccurlyeq b$. Верхняя грань b элементов a_1 и a_2 называется *минимальной верхней гранью* этих элементов, если не существует такой верхней грани c элементов a_1 и a_2, что $c \preccurlyeq b$ и $c \neq b$. Через $|\mathcal{P}|$ обозначается число элементов множества $\mathcal{P}$. Величину $\max |I|$, где максимум берется по всем цепям I множества $\mathcal{P}$, будем называть *высотой* множества $\mathcal{P}$ (обозначение $l(\mathcal{P})$).

Через $\mathcal{T}$ будем обозначать множество из 8 элементов, приведенное в работе [2].

Пусть $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathcal{P}$. Будем говорить, что эти элементы *обладают свойством* (Т6), если элементы a_1 и a_2 несравнимы, элементы b_1, b_2 являются минимальными верхними гранями элементов a_1, a_2, а элементы c_1, c_2 являются минимальными верхними гранями элементов b_1, b_2. Заметим, что если множество $\mathcal{P}$ (с наименьшим и наибольшим элементами) содержит шестерку элементов, обладающих свойством (Т6), то $l(\mathcal{P}) \geq 5$.

Основным результатом работы является следующее утверждение:

Теорема 1. *Пусть $l(\mathcal{P}) \leq 5$. Класс $\mathcal{M}_\mathcal{P}$ является конечно-порожденным тогда и только тогда, когда $\mathcal{P}$ не содержит шестерку элементов, обладающих свойством* (Т6).

Доказательство теоремы опирается на следующие леммы.

Лемма 1. *Пусть $l(\mathcal{P}) = 5$, $\mathcal{P}$ содержит шестерку элементов, обладающих свойством* (Т6). *Тогда класс $\mathcal{M}_\mathcal{P}$ не имеет конечного базиса.*

Доказательство этой леммы получается обобщением доказательства основного утверждения из работы [2].

Лемма 2. *Пусть $l(\mathcal{P}) \leq 5$, $\mathcal{P}$ не содержит шестерку элементов, обладающих свойством* (Т6). *Тогда в классе $\mathcal{M}_\mathcal{P}$ существует мажоритарная функция.*

Функция $\mu(x_1, \ldots, x_n)$, $n \geq 3$, называется *мажоритарной*, если для любых $a, b \in \mathcal{P}$ выполняется

$$\mu(a, b, \ldots, b) = \mu(b, a, b, \ldots, b) = \ldots = \mu(b, \ldots, b, a) = b.$$

Известно [6], что если в замкнутом классе содержится мажоритарная функция, то класс имеет конечный базис.

Далее переформулируем теорему 1 в других терминах.

Пусть $\mathcal{Q} \subseteq \mathcal{P}$, $\mathcal{Q} \neq \emptyset$. Будем говорить, что множество $\mathcal{P}$ *стягивается* к множеству $\mathcal{Q}$, если если существует монотонное отображение $\varphi : \mathcal{P} \to \mathcal{Q}$, такое, что $\varphi(x) = x$ для всех $x \in \mathcal{Q}$.

Нетрудно доказать следующее утверждение:

Утверждение 1. *Пусть* $l(\mathcal{P}) \leq 5$. *Множество* $\mathcal{P}$ *содержит шестерку элементов, обладающих свойством* (Т6) *тогда и только тогда, когда* $\mathcal{P}$ *стягивается к множеству, изоморфному множеству* $\mathcal{T}$.

Теорема 2. *Пусть* $l(\mathcal{P}) \leq 5$. *Следующие условия эквивалентны:*
(1) *класс* $\mathcal{M}_{\mathcal{P}}$ *имеет конечный базис,*
(2) *в* $\mathcal{P}$ *нет шестерки элементов, обладающих свойством* (Т6),
(3) $\mathcal{P}$ *не стягивается к множеству, изоморфному* $\mathcal{T}$,
(4) *в классе* $\mathcal{M}_{\mathcal{P}}$ *содержится мажоритарная функция.*

Доказательство. Импликация (1) $\Rightarrow$ (2) следует из леммы 1. Импликация (2) $\Rightarrow$ (4) следует из леммы 2. Импликация (4) $\Rightarrow$ (1) следует из результата работы [6]. Эквивалентность (2) $\Leftrightarrow$ (3) следует из утверждения 1.

Работа выполнена при финансовой поддержке РФФИ, проект № 14-01-00598.

Список литературы

1. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — 24. — S. 79–96.

2. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — 3. — P. 211–218.

3. Zádori L. Series parallel posets with nonfinitely generated clones // Order. — 1993. — 10. — 305–316.

4. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестн. Моск. ун-та. Серия 1. Математика. Механика. — 2008. — № 1. — С. 31–37.

5. Мартынюк В. В. Исследование некоторых классов в многозначных логиках // Проблемы кибернетики. — М.: Наука. — 1960. — Т. 3. — С. 49–60.

6. Baker K., Pixley A. Polynomial interpolation and the Chinese remainder theorem for algebraic systems // Math. Z. — 1975. — 143. — 165–174.

О ПРОБЛЕМЕ ЛОГИКО-ТЕРМАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ НЕДЕТЕРМИНИРОВАННЫХ СТАНДАРИТНЫХ СХЕМ ПРОГРАММ

В. А. Захаров, У. В. Попеско (Москва)

Стандартные схемы программ были введены в статье [1] для разработки математических методов решения задач трансляции, оптимизации и верификации последовательных операторных программ. Эта модель вычислений определяется следующим образом.

Пусть заданы конечные множества переменных $\mathcal{X}$, функциональных символов $\mathcal{F}$ и предикатных символов $\mathcal{P}$. Над этими множествами обычным образом определяются множества термов $Term(\mathcal{F}, \mathcal{X})$ и атомарных формул (атомов) $Atom(\mathcal{P}, \mathcal{F}, \mathcal{X})$. *Подстановкой* назовем всякое отображение $\theta : \mathcal{X} \to Term(\mathcal{F}, \mathcal{X})$. Множество всех подстановок условимся обозначать записью $Subst(\mathcal{F}, \mathcal{X})$. Результатом применения подстановки θ к выражению (терму или атому) E является выражение $E\theta$, получающийся одновременной заменой в E каждой переменной x термом $\theta(x)$. Композиция $\theta\eta$ подстановок θ, η — это подстановка, которая определяется равенством $\theta\eta(x) = (x\theta)\eta$ для каждой переменной x.

Стандартная (детерминированная) *схема программ* — это конечный размеченный ориентированный граф π, удовлетворяющий следующим условиям.

1. Каждой вершине v графа π, приписана атомарная формула A_v из множества $Atom(\mathcal{P}, \mathcal{F}, \mathcal{X})$.
2. Из каждой вершины исходят две дуги, одна из которых помечена символом 0, а другая — символом 1.
3. Каждой дуге, ведущей в графе π из вершины u в вершину v, приписана подстановка θ_{uv} из множества $Subst(\mathcal{F}, \mathcal{X})$.
4. Одна из вершин v_{in} графа π особо выделена в качестве входа, а другая вершина v_{out} играет роль выхода; вершине выхода приписан особая атомарная формула $Out(x_{i_1}, \ldots, x_{i_k})$.

Трассой в схеме программ π называется всякий маршрут из ее входа $v_{in} = v_0$ в выход $v_{out} = v_n$

$$tr = v_0 \xrightarrow{\theta_1,\sigma_1} v_1 \xrightarrow{\theta_2,\sigma_2} \cdots \xrightarrow{\theta_n,\sigma_n} v_n. \qquad (*)$$

Отношение эквивалентности на множестве схем программ можно ввести двояко. *Функциональная эквивалентность* [1] определяется на множестве эрбрановских интерпретаций. Каждая эрбрановская интерпретация — это отображение $I : Atom(\mathcal{P}, \mathcal{F}, \mathcal{X}) \to \{0, 1\}$. Трасса $(*)$ реализуема в интерпретации I, если для любого $i, 1 \leq i \leq n$,

выполняется равенство $I(A_i\theta_i \cdots \theta_1) = \sigma_i$. Каждая схема программ π вычисляет частичное отображение F_π множества эрбрановских интерпретаций в множество атомарных формул: для каждой эрбрановской интерпретации I значение $F_\pi(I)$ определено и равно $Out(t_1, \ldots t_k)$ в том и только том случае, если в схеме π существует трасса $(*)$, реализуемая в интерпретации I и удовлетворяющая равенству $Out(t_1, \ldots t_k) = A_{v_n}\theta_n \cdots \theta_1$. Для детерминированной схемы программ π функция F_π определена однозначно. Схемы программ π_1 и π_2 *функционально эквивалентны*, если $F_{\pi_1}(I) = F_{\pi_2}(I)$ для любой эрбрановской интерпретации I. Стандартные схемы программ с отношением функциональной эквивалентностью адекватно моделируют поведение последовательных императивных программ. Главный недостаток этой разновидности моделей программ состоит в том, что отношение функциональной эквивалентности неразрешимо.

Для преодоления этого недостатка в статье [2] было введено более строгое отношение эквивалентности схем программ — логико-термальная эквивалентность. *Логико-термальной историей* трассы $(*)$ называется последовательность пар

$$lth(tr) = (A_{v_1}\eta_1, \sigma_1), (A_{v_2}\eta_2, \sigma_2), \ldots, (A_{v_n}\eta_n, 0),$$

в которой $\eta_i = \theta_i\theta_{i-1} \cdots \theta_1$ для каждого $i, 1 \leq i \leq n$. Схемы программ π_1 и π_2 *логико-термально эквивалентны*, если множества их логико-термальных историй совпадают. Как было показано в [2], логико-термальная эквивалентность аппроксимирует функциональную эквивалентность стандартных схем программ. Другое достоинство логико-термальной эквивалентности состоит в том что это отношение разрешимо за полиномиальное время [3, 4]. Возникает вопрос: можно уточнить отношение логико-термальной эквивалентности, сохранив при этом ее полиномиальную разрешимость?

Покажем, что достичь этой цели, по меньшей мере, затруднительно. Для этого рассмотрим недетерминированный вариант стандартных схем программ, который отличается от детерминированного варианта тем, что требование п. 2 приведенного выше определения ослаблено: из каждой вершины недетермированной схемы может исходить произвольное конечное множество дуг помеченных одним и тем же символом $\sigma, \sigma \in \{0, 1\}$.

Теорема. *Проблема логико-термальной эквивалентности для недетерминированных стандартных схем программ алгоритмически неразрешима.*

Доказательство этого утверждения опирается на следующие два факта.

1. Как показано в статье [5], проблема эквивалентности конечных недетерминированных автоматов-преобразователей алгоритмически неразрешима.
2. Существует такая эффективная трансляция Tr конечных автоматов-преобразователей в недетерминированные стандартные схемы программ, что для любой пары автоматов-преобразователей M_1 и M_2 эти автоматы эквивалентны тогда и только тогда, когда соответствующие им стандартные схемы программ $Tr(M_1)$ и $Tr(M_2)$ логико-термально эквивалентны.

Работа выполнена при финансовой поддержке гранта РФФИ (проект 15-01-05742).

Список литературы

1. Luckham D. C., Park D. M., Paterson M. S. On formalized computer programs // Journal of Computer and System Science. — 1970. — V. 4, iss. 3. — P. 220–249.

2. Иткин В. Э. Логико-термальная эквивалентность схем программ // Кибернетика. — 1972. — № 1. — С. 5–27.

3. Сабельфельд В. К. Полиномиальная оценка сложности распознавания логико-термальной эквивалентности // ДАН СССР. — 1979. — Т. 249, № 4. — С. 793–796.

4. Захаров В. А., Новикова Т. А.. Полиномиальный по времени алгоритм проверки логико-термальной эквивалентности программ // Труды Института системного программирования РАН. — 2012. — Т. 22 — С. 435–455.

5. Griffiths T. The unsolvability of the equivalence problem for ε-free nondeterministic generalized machines // Journal of the ACM. — 1968. — V. 15. — P. 409–413.

О ПЕРИОДАХ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ АВТОМАТОВ С МАГАЗИННОЙ ПАМЯТЬЮ БЕЗ ВХОДА

И. И. Иванов (Москва)

Автомат с магазинной памятью возник в математике в связи с развитием теории формальных языков. Он является распознавателем для контекстно-свободных грамматик. Важность магазинов (известных также под названием стеков) в процессах обработки языков была осознана в начале 1950-х годов. Эттингер [1] и Шютценберже

[2] первыми формализовали понятие автомата с магазинной памятью. Эквиваленность автоматов с магазинной памятью и контекстно-свободных грамматик была показана Хомским [3] и Эви [4].

Очень скоро стало понятно, что класс контектно-свободных языков устроен сложнее класса регулярных. В работах [5, 6] появились следующие примеры алгоритмически неразрешимых проблем.
1. Не существует алгоритма, позволяющего установить равенство двух контестно-свободных языков.
2. Не существует алгоритма проверки, что один контектно-свободный язык лежит в другом.
3. Не существует алгоритма проверки, что пересечение двух контекстно-свободных языков является пустым.
4. Не существует алгоритма проверки контекстно-свободного языка на регулярность.

Заметим, что все эти проблемы разрешимы в классе регулярных языков. Исследования их свойств довольно скоро сформировали теорию автоматов как отдельное направление дискретной математики. Возникли уже самостоятельные задачи описания автоматов как функциональных систем. Были доказаны такие фундаментальные свойства автоматов как преобразователей, как сохранение периодических последовательностей и как следствие отсутствие конечных полных систем (относительно суперпозиции) [7]. Д. Н. Бабиным было доказано, что что арность множества автоматных функций равна двум (аналог 13-й проблемы Гильберта для автоматных функций) [8].

Оказалось, что многие техники работы с конечными автоматами и регулярными языками для автоматов с магазинной памятью не работают. В частности, было показано, что класс языков, разпознаваемых детерминированными автоматами с магазинной памятью, не равен классу всех контекстно-свободных языков, а является его собственным подмножеством [2, 9].

В данной работе будет рассмотрен автономная версия автомата. Инициальным детерминированным автоматом с магазиной памятью без входа будем называть "восьмерку"$P = \{Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0\}$, где Q — конечное множество состояний, B — выходной алфавит, Γ — алфавит памяти (алфавит ленты магазина), $\varphi : Q \times (\Gamma \cup \lambda) \to Q$ — функция переходов, $\psi : Q \times (\Gamma \cup \lambda) \to B$ — функция выхода, $\eta : Q \times (\Gamma \cup \lambda) \to \Gamma^*$ — функция памяти, $q_0 \in Q$ — начальное состояние, $\gamma_0 \in \Gamma^*$ — начальная запись в магазине.

Функционирование P можно определить с помощью системы канонических уравнений, которые задают в каждый момент времени t состояние автомата $q(t)$, записанное в магазине слово $\gamma(t)$, и выход

автомата $b(t)$:

$$\begin{cases} q(0) = q_0, \\ \gamma(0) = \gamma_0, \\ z(t) = LS(\gamma(t)), \\ q(t+1) = \varphi(q(t), z(t)), \\ \gamma(t+1) = S(\gamma(t))\eta(q(t), z(t)), \\ b(t) = \psi(q(t), z(t)). \end{cases}$$

где $LS : \Gamma^* \to \Gamma \cup \{\lambda\}$ возвращает последний символ при подаче непустого слова и $LS(\lambda) = \lambda$, а $S : \Gamma^* \to \Gamma^*$ — стирает последний символ входного слова и $S(\lambda) = \lambda$.

Теорема 1. *Автономный автомат с магазинной памятью $P = \{Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0\}$ генерирует периодическую выходную последовательность.*

Обозначим $n = |Q|$, $m = |\Gamma|$, $k = \max\limits_{(q,z)\in Q\times\Gamma\cup\{\lambda\}} |\eta(q, z)|$ и будем говорить, что $P \in \mathcal{M}_0(n, m, k)$.

Для автомата с магазинной памятью без входа обозначим $L(P)$ минимальную длину периода периодической последовательности, которую он генерирует. Нас будет интересовать максимальная длина периода в классе автоматов $L(n, m, k) = \max\limits_{P\in\mathcal{M}_0(n,m,k)} L(P)$.

Теорема 2. *При $k > 1$ и $n \to \infty$*

$$L(n, 1, k) = \frac{k(k-1)}{4k-2} n^2(1 + o(1)).$$

Теорема 3. *При $k > 1$ выполнено, $L(n, m, k) \le \frac{n(k^{nm+1}-1)}{k-1}$.*

Теорема 4. *При $m > 1$, $k > 1$ и $n \to \infty$*

$$L(n, m, k) \gtrsim \begin{cases} 12 \cdot 2^{\frac{2n}{9}}, \ m = 2, \ k = 2, \\ (\frac{k-1}{k})^n k^{n(m-1)} \end{cases}$$

Список литературы

1. Oettinger A. Automatic syntatic analysis and the pushdown store // Structure of Language and its Mathematical Concepts, Proc. 12th Symposium on Applied Mathematics. — 1961. — P. 104–129.

2. Schutzenberger M. P. On contex-free languages and pushdown automata // Information and Control. — 1963. — 6:3. — P. 246–264.

3. Chomsky N. Context-free gtammars and pushdown storage. Quarlerly Progress Report, № 65, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambrig, Mass. — 1962.

4. Evey R.J. Applications of pushdown-store machines // Proc. AFIPS Fall Joint Computer Conference, 24, 1963. — P. 215–227.

5. Bar-Hillel Y., Perles M., Shamir E. On formal properties of simple phrase structure grammars // Z. Phonctik, Sprachwissensch. Kommunikationsforsch. — 1961. — 14. — P. 143–172.

6. Ginsburg S., Rose G.F. Some recursively unsolvable problems in ALGOL-like languages // J. Assoc. Computing Machinety. — 1963. — 10. — P. 175–195.

7. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

8. Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная математика. — 1989. — Т. 1, вып. 4. — С. 423–431.

9. Ginsburg S., Greibach S. Deterministic context free languages // Information and Control. — 1966. — V. 9, is. 6 — P. 620–648.

ИНЪЕКТИВНОСТЬ И ПРОЕКТИВНОСТЬ ПОЛИГОНОВ НАД ВПОЛНЕ ПРОСТЫМИ ПОЛУГРУППАМИ

И. Б. Кожухов, А. О. Петриков (Москва)

Важную роль в общей алгебре играют инъективные и проективные объекты. Теория инъективности и проективности развивалась под большим влиянием теории колец и модулей, где понятия инъективности и проективности занимают одно из ведущих мест. В монографии [1] приведены многие результаты этой теории в случае унитарных полигонов над моноидоами. Аналогично модулям над кольцом могут быть определены инъективная оболочка полигона — наименьший инъективный полигон, содержащий данный, и проективное накрытие полигона — наименьший проективный полигон, имеющий сюръективный гомоморфизм на данный. Как и в случае колец и модулей, инъективная оболочка существует у всякого полигона, а проективное накрытие не у всякого. Целью данной работы является

описание инъективных и проективных полигонов над вполне простыми полугруппами.

Полигоном над полугруппой S называется множество X, на котором действует полугруппа S, то есть определено отображение $X \times S \to X$, $(x, s) \mapsto xs$ такое, что $x(st) = (xs)t$ при всех $x \in X$, $s, t \in S$. Полигон является унарной алгеброй — элементы полугруппы S задают унарные операции на X. Кроме того, полигон является алгебраической моделью автомата [2]. Полигон X называется *проективным*, если для любого сюръективного гомоморфизма $\alpha : A \to B$ полигонов и любого гомоморфизма $\varphi : X \to B$ существует гомоморфизм $\psi : X \to A$ такой, что $\psi\alpha = \varphi$. Полигон X называется *инъективным*, если для любого инъективного гомоморфизма $\alpha : A \to B$ полигонов и любого гомоморфизма $\varphi : A \to X$ существует гомоморфизм $\psi : B \to X$ такой, что $\alpha\psi = \varphi$.

Если полигон X является объединением попарно не пересекающихся подполигонов X_i $(i \in I)$, то X называется копроизведением и обозначается $\coprod_{i \in I} X_i$.

Пусть G — группа, H — её подгруппа (не обязательно нормальная) и пусть G/H — множество правых смежных классов Hg. Тогда G/H — полигон над G относительно умножения $Hg \cdot g' = Hgg'$.

Вполне простой полугруппой называется полугруппа, не имеющая нетривиальных идеалов и содержащая примитивный идемпотент (то есть минимальный относительно естественного порядка $e \leq f \Leftrightarrow ef = fe = f$). Согласно теореме Сушкевича—Риса [3, §3.2] вполне простые полугруппы — это в точности рисовские матричные полугруппы $\mathcal{M}(G, I, \Lambda, P)$ (обозначения см. в [3]). Полигоны над такими полугруппами были описаны в [4] следующим образом. Пусть X — множество, G — группа, $Q = \coprod_{\gamma \in \Gamma} G/H_\gamma$ — полигон, $\pi_i : X \to Q$ $(i \in I)$, $\kappa_\lambda : Q \to X$ $(\lambda \in \Lambda)$ — отображения и $q\kappa_\lambda\pi_i = q \cdot p_{\lambda i}$ для всех $q \in Q$, $i \in I$, $\lambda \in \Lambda$; тогда множество X с умножением $x \cdot (g)_{i\lambda} = (x\pi_i \cdot g)\kappa_\lambda$ является полигоном над полугруппой $S = \mathcal{M}(G, I, \Lambda, P)$, и все S-полигоны имеют такой вид.

Следующие теоремы обобщают результаты, полученные в [5].

Теорема 1. *Полигон X над вполне простой полугруппой $S = \mathcal{M}(G, I, \Lambda, P)$ инъективен в том и только том случае, если (i) X содержит хотя бы один нуль и (ii) для любого отображения $\omega: I \to Q$ существует такое $x \in X$, что $x\pi_i = i\omega$ при всех $i \in I$.*

Теорема 2. *Пусть $S = \mathcal{M}(G, I, \Lambda, P)$ — вполне простая полугруппа, X — полигон над S. Если в X нет нуля, присоединим к X нуль z_0; если в X есть нули, зафиксируем какой-нибудь из них и обозначим его через z_0. При присоединении нуля z_0 внешним обра-*

зом множество Q пополнится элементом q_0. Далее, для каждого отображения $\omega : I \to Q$ (или $\omega : I \to Q \cup \{q_0\}$ в случае присоединения нуля), для которого не существует элемента $x \in X$ такого, что $x\pi_i = i\omega$ при всех $i \in I$, присоединим к X элемент b_ω и определим действие на нём элементов полугруппы S следующим образом: $b_\omega \cdot (g)_{i\lambda} = (i\omega \cdot g)\kappa_\lambda$. Тогда полученный после присоединения элементов полигон $\widetilde{X}$ является инъективной оболочкой полигона X.

Теорема 3. *Пусть X — полигон над вполне простой полугруппой $S = \mathcal{M}(G, I, \Lambda, P)$, XS — подполигон, $A = X \setminus XS$, $Z = XS \setminus AS$. Полигон X проективен в том и только том случае, когда выполнены условия (i) $as = bt \Rightarrow (a = b) \wedge (s = t)$ при $a, b \in A$, $s, t \in S$ и (ii) $z \cdot (g)_{i\lambda} = z \cdot (h)_{i\mu} \Rightarrow (g = h) \wedge (\lambda = \mu)$ при $z \in Z$, $i \in I$, $\lambda, \mu \in \Lambda$, $g, h \in G$.*

В полугруппе $S = \mathcal{M}(G, I, \Lambda, P)$ для $i \in I$ положим $R_i = \{(g)_{i\lambda} | g \in G, \lambda \in \Lambda\}$. Очевидно, R_i — правый идеал полугруппы S. Он является также $\mathcal{R}$-классом Грина этой полугруппы и $rS = R_i$ для любого $r \in R_i$ (имеет место даже более сильное утверждение: $rR_i = R_i$ при всех $r \in R_i$). Также ясно, что R_i являются подполигонами полигона S_S и $S_S = \coprod_{i \in I} R_i$.

Теорема 4. *Пусть $S = \mathcal{M}(G, I, \Lambda, P)$ — вполне простая полугруппа. Для $i \in I$ пусть $R_i = \{(g)_{i\lambda} | g \in G, \lambda \in \Lambda\}$. Полигон X над полугруппой S проективен в том и только том случае, если $X \cong \coprod_{\delta \in \Delta} Y_\delta \sqcup \coprod_{\varepsilon \in E} Z_\varepsilon$, где $Y_\delta \cong S^1, Z_\varepsilon \cong R_i$ для любых $\delta \in \Delta$, $\varepsilon \in E$. При этом возможно, что $\Delta = \emptyset$ или $E = \emptyset$.*

Теорема 5. *Пусть X — полигон над вполне простой полугруппой $S = \mathcal{M}(G, I, \Lambda, P)$. Представим X в виде $X = (A \cup AS) \sqcup \coprod_{\gamma \in \Gamma} z_\gamma S$. Пусть $F(A)$ — свободный S-полигон с множеством свободных образующих A, $R_i = \{(g)_{i\lambda} | g \in G, \lambda \in \Lambda\}$ — правый S-полигон ($i \in I$ фиксировано). Положим $P(X) = F(A) \sqcup \coprod_{\gamma \in \Gamma} R^{(\gamma)}$ ($R^{(\gamma)} \cong R_i$) и определим отображение $\beta : P(X) \to X$ по правилу $(as)\beta = as$ (для $a \in A$, $s \in S^1$), $(g)_{i\lambda}\beta = z_\gamma (g)_{i\lambda}$ (если $(g)_{i\lambda}$ рассматривается как элемент из $R^{(\gamma)}$). Тогда β — сюръективный гомоморфизм, а $P(X)$ — проективное накрытие полигона X.*

Список литературы

1. Kilp M., Knauer U., Mikhalev A. V. Monoids, acts and categories. — Berlin: W. de Gruyter, N.Y., 2000.

2. Плоткин Б. И., Гринглаз Л. Я., Гварамия А. А. Элементы алгебраической теории автоматов. — М.: Высш. шк., 1994.

3. Клиффорд А., Престон Г. Алгебраическая теория полугрупп. —

М. Мир, 1972.

4. Avdeyev A. Yu., Kozhukhov I. B. Acts over completely 0-simple semigroups // Acta Cybernetica. — 2000. — V. 14, № 4. — P. 523–531.

5. Кожухов И. Б., Халиуллина А. Р. Инъективность и проективность полигонов над сингулярными полугруппами // Электронные информационные системы. — 2014 . — № 2 (2). — С. 45–56.

ТЕМПОРАЛЬНАЯ ЛОГИКА ДЛЯ ВЕРИФИКАЦИИ АВТОМАТОВ-ПРЕОБРАЗОВАТЕЛЕЙ

Д. Г. Козлова, В. А. Захаров (Москва)

Верификация моделей программ — один из наиболее эффективных методов проверки правильности поведения реагирующих программ [1]. В качестве модели реагирующей программы обычно используются модели Крипке — размеченные системы переходов. Вычислениями модели являются бесконечные последовательности состояний, связанные отношением переходов. Для спецификации требований правильного поведения модели используются формулы темпоральных логик. Модель M удовлетворяет спецификации φ, если формула φ выполняется во всех начальных состояниях модели M.

Характерная особенность моделей Крипке и большинства темпоральных логик (PLTL, CTL, PDL, μ-исчисление и др.), используемых в качестве формальных языков спецификации, состоит в том, что элементарные свойства вычислений зависят только от состояний модели, но не от вычислений, которыми достигаются состояния. Однако для стороннего наблюдателя поведение реагирующей системы проявляется в соответствии между последовательностями стимулов (сигналов), которыми внешняя среда воздействует на систему, и откликов (действий), которые вырабатывает или исполняет система в ответ на внешние воздействия. Поэтому при верификации некоторых видов реагирующих систем элементарными свойствами становятся множества конечных последовательностей действий. Это обстоятельство должно быть также учтено при разработке формального языка спецификаций поведения таких систем.

В данной статье рассмотрена задача формальной верификации реагирующих систем, моделируемых конечными автоматами-преобразователями [2]. Для спецификации их поведения предложен новый вариант темпоральной логики линейного времени LTL-FL (LTL with Formal Languages). Формальные языки (множества конечных слов фиксированных алфавитов) в формулах LTL-FL используются для представления элементарных свойств вычислений, а также для параметризации темпоральных операторов. Установлено, что задача проверки выполнимости формул регулярного фрагмента FL-LTL на конечных автоматах преобразователях разрешима.

Пусть заданы конечные алфавита *событий* $\mathcal{C}$ и *действий* $\mathcal{A}$. Слова и ω-слова в алфавите $\mathcal{C}$ будем называть *потоками событий*. Действия из множества $\mathcal{A}$ являются образующими моноида $(S, \circ, e)$. Элементы моноида S будем называть *историями*. Бесконечную последовательность пар $\alpha = (c_1, s_1), (c_2, s_2), \ldots, (c_i, s_i), \ldots$, где $c_i \in \mathcal{C}, s_i \in S$ для всех $i, i \geq 0$, назовем *траекторией*. Запись $\alpha|^i$ используется для обозначения суффикса $(c_i, s_i), (c_{i+1}, s_{i+1}), \ldots$ траектории α.

Пусть выделены счетное семейство языков $\mathcal{L}, \mathcal{L} \subseteq \wp(\mathcal{C}^*)$, в алфавите событий и счетное множество одноместных предикатов $\mathcal{P}, \mathcal{P} \subseteq \wp(S)$ в моноиде S. Для конструктивного описания языков из $\mathcal{L}$ и предикатов из $\mathcal{P}$ могут быть использованы различные средства — формальные грамматики, автоматы, алгебраические выражения и др. Множество формул $\mathcal{LP}$-LTL строится из предикатов множества $\mathcal{P}$ при помощи булевых связок и параметризованных темпоральных операторов, причем параметрами являются языки из множества $\mathcal{L}$.

Формулы логики $\mathcal{LP}$-LTL — это выражения, устройство которых определяется следующими правилами:
1) если $P \in \mathcal{P}$, то P — атомарная формула;
2) если φ и ψ — формулы, $c \in \mathcal{C}$, и $L, L_1, L_2 \in \mathcal{L}$, то формулами являются выражения $\neg\varphi$, $\varphi \wedge \psi$, $\mathbf{X}[c]\varphi$, $\mathbf{Y}[c]\varphi$, $\mathbf{F}[L]\varphi$, $\mathbf{G}[L]\varphi$, $\varphi\mathbf{U}[L_1, L_2]\psi$ и $\varphi\mathbf{R}[L_1, L_2]\psi$.

Семантика формул $\mathcal{LP}$-LTL определяется отношением выполнимости на траекториях и историях. Пусть задана некоторая траектория $\alpha = (c_1, s_1), (c_2, s_2), \ldots, (c_i, s_i), \ldots$ и история $s, s \in S$. Тогда
- если $\varphi_0 = P$ — атомарная формула, то $\alpha, s \models \varphi_0 \;\Leftrightarrow\; s \in P$;
- $\alpha, s \models \neg\varphi \;\Leftrightarrow\; \alpha, s \not\models \varphi$;
- $\alpha, s \models \varphi \wedge \psi \;\Longleftrightarrow\; \alpha, s \models \varphi_1$ и $\alpha, s \models \varphi_2$;
- $\alpha, s \models \mathbf{X}[c]\varphi \;\Longleftrightarrow\; c = c_1$ и $\alpha|^2, ss_1 \models \varphi$;
- $\alpha, s \models \mathbf{Y}[c]\varphi \;\Longleftrightarrow\; c \neq c_1$ или $\alpha|^2, ss_1 \models \varphi$;
- $\alpha, s \models \mathbf{F}[L]\varphi \;\Longleftrightarrow\; \exists i : i \geq 0 :\; c_1 c_2 \ldots c_i \in L$ и $\alpha|^{i+1}, ss_1 s_2 \cdots s_i \models \varphi$;

- $\alpha, s \models \mathbf{G}[L]\varphi \Longleftrightarrow \forall i : i \geq 0 :\ c_1c_2 \ldots c_i \in L \Rightarrow \alpha|^{i+1}, ss_1s_2 \cdots s_i \models \varphi$;
- $\alpha, s \models \varphi \mathbf{U}[L_1, L_2]\psi \Longleftrightarrow \exists i : i \geq 0 : 1)\ c_1c_2 \ldots c_i \in L_2$ и $\alpha|^{i+1}, ss_1 \cdots s_i \models \psi$ и $2)\ \forall j : 0 \leq j < i :\ c_1c_2 \ldots c_j \in L_1 \Rightarrow \alpha|^{j+1}, ss_1s_2 \cdots s_j \models \varphi$;
- $\alpha, s \models \varphi \mathbf{R}[L_1, L_2]\psi \Longleftrightarrow 1)\ \forall i : i \geq 0 : c_1 \ldots c_i \in L_2 \Rightarrow \alpha|^{i+1}, ss_1 \cdots s_i \models \psi$ или $2)\ \exists i : i \geq 0 : c_1c_2 \ldots c_i \in L_2$ и $\alpha|^{i+1}, ss_1s_2 \cdots s_i \models \varphi$ и $\forall j : 0 \leq j \leq i :\ c_1c_2 \ldots c_j \in L_1 \Rightarrow \alpha|^{j+1}, ss_1s_2 \cdots s_j \models \psi$.

Формула φ выполнима на траектории α (обозначается $\alpha \models \varphi$), если $\alpha, e \models \varphi$.

Формулы $\mathcal{LP}$-LTL можно использовать в качестве формальных спецификаций для реагирующих систем. Вычисления системы порождают траектории. События из $\mathcal{A}$ играют роль воздействий внешней среды на систему. Действия из $\mathcal{A}$ — это реакция системы на воздействия среды, а истории — это результат выполнения действий. В качестве моделей реагирующих систем можно использовать автоматы-преобразователи над алфавитами $\mathcal{C}$ и $\mathcal{A}$.

Конечный *автомат-преобразователь* $\pi = \langle \mathcal{C}, \mathcal{A}, Q, Q_0, T \rangle$ — это система переходов, состоящая из множества *состояний* Q, подмножества *начальных состояний* Q_0 и *отношения переходов* $T \subseteq Q \times \mathcal{C} \to Q \times \mathcal{A}^*$. Отношение переходов T тотально, т.е. из любого состояния q в множестве T есть некоторый переход (q, c, q', h). *Вычислением* преобразователя π называется всякая бесконечная последовательность четверок
$(q_0, c_1, q_1, h_1), (q_1, c_2, q_1, h_2), \ldots, (q_{i-1}, c_i, q_i, h_i), (q_i, c_{i+1}, q_{i+1}, h_{i+1}), \ldots$
в которой $q_0 \in Q_0$ и $(q_{i-1}, c_i, q_i, h_i) \in T$ для любого $i, i \geq 1$. Последовательность $\alpha = (c_1, h_1), (c_2, h_2), \ldots, (c_i, h_i), \ldots$ называется траекторией данного вычисления. Множество траекторий всех вычислений преобразователя π обозначим записью $Tr(\pi)$.

Формула φ выполняется на преобразователе π, если отношение $\alpha \models \varphi$ выполняется для любой траектории α из $Tr(\pi)$.

Теорема. *Если $\mathcal{L}$ — семейство регулярных языков, S — свободный моноид, и $\mathcal{P}$ — множество всех регулярных предикатов, то задача проверки выполнимости формул $\mathcal{LP}$-LTL на конечных автоматах-преобразователях алгоритмически разрешима.*

Работа выполнена при финансовой поддержке гранта РФФИ (проект 15-01-05742).

Список литературы

1. Кларк Э. М., Грамберг О., Пелед Д. Верификация моделей программ. Model Checking. — М.: МЦНМО, 2002.

2. Захаров В. А. Моделирование и анализ поведения последовательных реагирующих программ // Труды Института системного программирования РАН. — 2015. — Т. 27, N 2. — С. 221–250.

ТРИ СЕМЕЙСТВА ЗАМКНУТЫХ КЛАССОВ В P_k, ОПРЕДЕЛЯЕМЫХ d-РАЗНОСТЯМИ

Д. Г. Мещанинов (Москва)

В [1, 2] анализировались замкнутые классы $R(d)$ и $L(d)$ функций из P_k, *сохраняющих* и, соответственно, *абсолютно сохраняющих* d-*разности*, $d|k$.

Теорема 1 [1, 2]. *Классы $R(d)$ и $L(d)$ обладают следующими свойствами.*

1. *Если $d \neq 1$ и $d \neq k$, то $L \subset L(d) \subset R(d) \subset C(d)$, где L — класс всех линейных по модулю k функций, $C(d)$ — класс функций сохраняющих сравнение по модулю d:*

$$\tilde{x} \equiv \tilde{y} \pmod{d} \Rightarrow f(\tilde{x}) \equiv f(\tilde{y}) \pmod{d}.$$

2. *Имеют место равенства*

$$L(1) = R(1) = L, \qquad L(k) = R(k) = C(k) = C(1) = P_k.$$

3. *Классы $R(d)$ при различных $d|k$ образуют решетку по включению, изоморфную решетке делителей числа k. Такую же решетку образуют классы $L(d)$.*

4. *Класс $L(d)$ является предполным в $R(d)$ в точности при $k = pd$, где число p простое. В точности при том же условии класс $R(d)$ является предполным в $C(d)$.*

Классы $C(d)$ при всех $d \neq 1$, $d \neq k$ являются предполными в P_k [3].

Эти свойства классов семейств $R(d)$ и $L(d)$ позволили построить решетку всех классов, содержащих L, при $k = p^2, k = p_1 \cdots p_m$, где $p_1, \ldots, p_m$ — различные простые числа. Свойства классов $R(d)$ и $L(d)$ позволяют также дать им следующую характеризацию.

Функция, удовлетворяющая условию

$$\tilde{x} \equiv \tilde{y} \pmod{d} \Rightarrow f(\tilde{x}) = f(\tilde{y}),$$

называется d-периодической.

Введем функции

$$g_d(\tilde{x}) = \begin{cases} 1, & \tilde{x} \equiv \tilde{0} \pmod{d}, \\ 0, & \tilde{x} \not\equiv \tilde{0} \pmod{d}, \end{cases} \qquad \chi_{d,j}(\tilde{x}) = x_j g_d(\tilde{x}),\ j = 1, \ldots, n.$$

Теорема 2. *Функция принадлежит классу $R(d)$ тогда и только тогда, когда ее можно представить в виде*

$$f(\tilde{x}) = l(\tilde{x}) + g(\tilde{x}) + h(\tilde{x}), \tag{1}$$

где $l(\tilde{x}) \in L$, $g(\tilde{x})$ — d-периодическая и $h(\tilde{x})$ — линейная комбинация функций $\chi_{d,j}(\tilde{x} - \tilde{\mu})$, j=1,... $n, \tilde{\mu} \in E_d$, причем функция $l(\tilde{x})$ имеет специальный вид и все слагаемые суммы (1) *определены однозначно.*

Теорема 3. *Функция принадлежит классу $L(d)$ тогда и только тогда, когда ее можно представить в виде*

$$f(\tilde{x}) = l(\tilde{x}) + g(\tilde{x}), \tag{2}$$

где $l(\tilde{x}) \in L$, $g(\tilde{x})$ — d-периодическая, причем функция $l(\tilde{x})$ имеет специальный вид и слагаемые суммы (2) *определены однозначно.*

В связи с этим рассмотрим функции, допускающие представление в виде

$$f(\tilde{x}) = l(\tilde{x}) + h(\tilde{x}), \tag{3}$$

где $l(\tilde{x}) \in L$, $h(\tilde{x})$ — линейная комбинация функций $\chi_{d,j}(\tilde{x} - \tilde{\mu})$, $j = 1, \ldots n$, $\tilde{\mu} \in E_d$.

Теорема 4. *Функции вида* (3) *образуют замкнутый подкласс в $R(d)$.*

Обозначим этот класс как $S(d)$. Тогда

$$[L(d) \cup S(d)] = R(d).$$

Теорема 5. *Если $k = p^2$, то класс $S(p)$ является предполным в $R(p)$.*

Такое свойство классов $S(p)$ позволило описать решетку всех классов, содержащих L, при $k = p^2$ [4]. В случае $k = 4$ эта решетка была построена ранее в [5].

Список литературы

1. Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Математические вопросы кибернетики. Вып. 7. — М.: Наука, 1998. — С. 265–280.

2. Мещанинов Д. Г. О замкнутых классах k-значных фунуций, сохраняющих первые d-разности // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 219–230.

3. Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН СССР. — 1958. — Т. 51. — С. 5–142.

4. Мещанинов Д. Г. О замкнутых классах полиномов над кольцом Z_k // Труды IX Междунар. конф. "Дискретные модели в теории управляющих систем" (20–22 мая 2015 г.) — М.: МАКС-Пресс, 2015. — С. 161–163.

5. Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов // Дискретная математика. — 1997. — Т. 9, вып. 2. — С. 24–39.

О БАЗИРУЕМОСТИ КЛАССОВ ФУНКЦИЙ ТРЁХЗНАЧНОЙ ЛОГИКИ, ПОРОЖДЁННЫХ ПЕРИОДИЧЕСКИМИ СИММЕТРИЧЕСКИМИ ФУНКЦИЯМИ

А. В. Михайлович (Москва)

Э. Пост [1] показал, что все замкнутые классы булевых функций имеют конечный базис. В k-значных логиках при $k \geq 3$ этот результат не сохраняется. В работе [2] установлено, что при всех $k \geq 3$ в множестве функций k-значной логики существуют как замкнутые классы со счетным базисом, так и классы, не имеющие базиса. Следует отметить, что порождающие системы замкнутых классов в этих примерах состоят из симметрических функций, которые принимают значения из множества $\{0, 1\}$, причем ненулевые значения принимаются на наборах, состоящих только из единиц и двоек. В работе [3] рассматривались периодические симметрические функции трёхзначной логики, принимающие только значения 0 и 1,

причем единичное значение — на таких наборах из единиц и двоек, в которых число единиц образует периодическую последовательность. Для классов, порождённых периодическими симметрическими функциями с ограниченным периодом, получен критерий базируемости и показано, что классы такого вида либо имеют конечный базис, либо не имеют базиса. В данной работе рассматриваются классы, у которых период является степенью некоторого простого числа. Для таких классов получены критерии базируемости и конечной порождённости.

Дадим некоторые определения. Все недостающие определения можно найти в [4].

Функции f и g называются *конгруэнтными*, если одна из них получается из другой переименованием переменных без отождествления.

Будем обозначать через N_f множество всех наборов, на которых функция f принимает значение 1.

Пусть $E = \{0, 1, 2\}$. Множество всех наборов из E^n, которые получаются друг из друга перестановкой компонент, будем называть *слоем*. Слой из E^n, содержащий e единиц и $n - e$ двоек, обозначим через $\mathcal{L}(e, n - e)$.

Обозначим через R множество всех функций трехзначной логики, принимающих значения только из множества $\{0, 1\}$ и равных нулю на всех наборах, содержащих хотя бы одну нулевую компоненту.

Пусть $t \in \mathbb{N}$. Функция $f(x_1, \ldots, x_n)$ из множества R называется *элементарной периодической симметрической функцией с периодом* t, если $N_f \neq \varnothing$ и для некоторых e и d, удовлетворяющих условиям $e + d = n$, $0 \leq d < t$, выполняется соотношение

$$N_f = \bigcup_{i=0}^{s} \mathcal{L}(e - it, d + it),$$

где $s = \lceil \frac{n-d}{t} \rceil$. Будем обозначать через t_f период функции f, а через e_f и d_f — число единиц и двоек соответственно в слое из N_f с наибольшим числом единиц. Множество всех элементарных периодических симметрических функций будем обозначать через PS, множество всех элементарных периодических симметрических функций с периодом t — через PS^t, а множество всех элементарных периодических симметрических функций, у которых период является степенью простого числа p — через $PS^{[p]}$. Множество функций PS^1 обозначим через I.

Доказательство основного результата опирается на следующий вспомогательный факт, при формулировке которого под записью (a, b) понимается наибольший общий делитель чисел a и b.

Лемма. *Пусть* $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m) \in PS$, $\{(1^m), (2^m)\} \not\subset N_g$, $t_f > 1$, $d_f + t_f \leq n$. *Тогда имеют место следующие утверждения:*

1. *Функция* f *содержится в классе* $[\{g\}]$ *тогда и только тогда, когда* d_g *кратно* $\frac{t_g}{t_f}(d_f, t_f)$ *и существуют такие* $s \in \mathbb{Z}^+$, $q \in \mathbb{N}$ *и* $k \in \mathbb{Z}^+$, *что выполняются условия:*
   - *a)* q *кратно* $\frac{t_g}{t_f}$,
   - *b)* $m = qn + st_g$,
   - *c)* $0 < q < t_g$,
   - *d)* $d_g + kt_g = qd_f$.

2. *Функция* f *содержится в классе* $[\{g\} \cup I]$ *тогда и только тогда, когда* d_g *кратно* $\frac{t_g}{t_f}(d_f, t_f)$ *и существуют такие* $q \in \mathbb{N}$ *и* $k \in \mathbb{Z}^+$, *что выполняются условия:*
   - *a)* q *кратно* $\frac{t_g}{t_f}$,
   - *b)* $m \geq qn$,
   - *c)* $0 < q < t_g$,
   - *d)* $d_g + kt_g = qd_f$.

Пусть $G \subset PS^{[p]}$. Положим

$$G_t = \left\{ f \in G \mid \frac{t_f}{(d_f, t_f)} = p^t \right\}.$$

Основным результатом данной работы является следующий критерий базируемости и конечной порождённости для классов, порождённых функциями из рассматриваемых семейств.

Теорема. *Пусть* G *— множество попарно неконгруэнтных функций из* $PS^{[p]}$, $F = [G]$. *Тогда справедливы следующие утверждения:*

1. *Класс* F *имеет базис тогда и только тогда, когда множество* $G \backslash I$ *конечно.*
2. *Класс* F *имеет счётный базис тогда и только тогда, когда множество* $G \backslash I$ *бесконечно и для любого* $t \in \mathbb{N}$ *множество* G_t *конечно.*
3. *Класс* F *не имеет базиса тогда и только тогда, когда множество* $G \backslash I$ *бесконечно и существует* $t \in \mathbb{N}$, *такое что множество* G_t *бесконечно.*

Отметим, что в отличие от классов, порождённых периодическими симметрическими функциями с ограниченным периодом, среди рассматриваемых классов существуют классы со счётным базисом.

Данное научное исследование (№ 14-01-0144) выполнено при поддержке Программы «Научный фонд НИУ ВШЭ» в 2014/2015 гг.

Список литературы

1. Post E. L. The two-valued iterative systems of mathematical logic // Annals of Math. Studies. — Princeton Univ. Press, 1941.

2. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — 127, № 1. — С. 44–46.

3. Михайлович А. В. О замкнутых классах функций в P_3, порожденных периодическими симметрическими функциями // Вест. Нижегор. ун-та им. Н. И. Лобачевского. — 2013. — № 1. — С. 208–212.

4. Михайлович А. В. О замкнутых классах функций многозначной логики, порожденных симметрическими функциями // Математические вопросы кибернетики. Вып. 18. — М.: Физматлит, 2013. — С. 123–212.

О ТРИВИАЛЬНЫХ ПЕРЕСЕЧЕНИЯХ ПРЕДПОЛНЫХ КЛАССОВ СЕМЕЙСТВА $C \setminus T$ В ЧЕТЫРЕХЗНАЧНОЙ ЛОГИКЕ

А. С. Нагорный (Москва)

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$. Обозначим через P_k множество всех конечноместных функций на E_k. Элементы множества P_k будем называть k-значными функциями или функциями k-значной логики. Определения основных понятий можно взять, например, из [1].

Предикат, заданный на E_k, назовем *центральным*, если он является вполне рефлексивным, вполне симметричным, отличен от тождественно истинного предиката, и существует такое непустое подмножество множества E_k (называемое *центром*), что предикат является истинным для любого набора, пересекающегося с центром. При любом $k \geq 2$ классы k-значных функций, сохраняющих центральные

предикаты, являются замкнутыми и предполными в P_k [2]. Обозначим через C семейство всех таких классов. Пусть также T есть множество тех классов из семейства C, которые сохраняют одноместные центральные предикаты.

Опишем все пересечения классов из семейства $C \setminus T$ в четырехзначной логике, которые являются *тривиальными*, т. е. содержат только константы и селекторные функции. Интерес к данному семейству обусловлен тем фактом, что с ростом k почти все предполные классы в P_k лежат в $C \setminus T$ [3].

Пусть π — произвольная перестановка на E_k, $f(\tilde{x}^n) \in P_k$. Функцию $f^*(\tilde{x}^n) = \pi^{-1}(f(\pi(x_1), \pi(x_2), \ldots, \pi(x_n)))$ назовем *двойственной к функции* f относительно перестановки π.

Класс функций Φ^* назовем *двойственным классу функций* Φ, если существует такая перестановка π, что Φ^* состоит из всех функций, двойственных функциям из Φ относительно π, и только из них.

Тривиальное пересечение замкнутых классов $K_{i_1} \cap K_{i_2} \cap \ldots \cap K_{i_s}$ назовем *неприводимым*, если после удаления любого K_{i_m} получается нетривиальное пересечение оставшихся классов.

В P_2 семейство $C \setminus T$ не содержит ни одного класса, в P_3 оно состоит из трех классов C_0, C_1 и C_2, отвечающих предикатам с центрами $\{0\}$, $\{1\}$ и $\{2\}$, соотвественно (при этом тривиальным является только пересечение всех трех этих классов). В четырехзначной логике семейство $C \setminus T$ состоит из 26 предполных классов. Это классы функций, сохраняющих двухместные центральные предикаты:

$$C_0 = Pol_4 \begin{pmatrix} 0123000123 \\ 0123123000 \end{pmatrix} \text{ и еще 3 двойственных класса,}$$

$$C_{01} = Pol_4 \begin{pmatrix} 012300012311 23 \\ 012312300023 11 \end{pmatrix} \text{ и еще 5 двойственных классов,}$$

$$C_{0\{12\}} = Pol_4 \begin{pmatrix} 012300012312 \\ 012312300021 \end{pmatrix} \text{ и еще 11 двойственных классов}$$

и трехместные центральные предикаты: $D_0 =$

$$= Pol_4((x_1 = x_2) \vee (x_1 = x_3) \vee (x_2 = x_3) \vee j_0(x_1) \vee j_0(x_2) \vee j_0(x_3))$$

и еще 3 двойственных класса.

Теорема. *В четырехзначной логике имеется ровно* 1315 *неприводимых тривиальных пересечений классов из семейства* $C \setminus T$*, среди которых ровно* 78 *попарно недвойственных* (*все они перечислены в нижеследующей таблице*). *Знак* $\cap$ *для краткости всюду опущен.*

№	Пересечение классов	№	Пересечение классов
1	$C_{0\{12\}}C_{1\{23\}}C_{3\{02\}}$	2	$C_0C_1C_2C_3$
3	$C_0C_1C_2C_{3\{01\}}$	4	$C_0C_1C_2D_3$
5	$C_0C_1C_{02}C_{3\{12\}}$	6	$C_0C_1C_{2\{30\}}C_{3\{01\}}$
7	$C_0C_1C_{2\{30\}}C_{3\{02\}}$	8	$C_0C_1C_{2\{30\}}C_{3\{12\}}$
9	$C_0C_1C_{2\{30\}}D_3$	10	$C_0C_{01}C_{2\{31\}}C_{3\{01\}}$
11	$C_0C_{01}C_{2\{31\}}C_{3\{12\}}$	12	$C_0C_{12}C_{13}C_{23}$
13	$C_0C_{12}C_{13}C_{2\{30\}}$	14	$C_0C_{12}C_{1\{23\}}C_{3\{02\}}$
15	$C_0C_{12}C_{1\{30\}}C_{3\{02\}}$	16	$C_0C_{12}C_{3\{01\}}C_{3\{02\}}$
17	$C_0C_{1\{23\}}C_{1\{20\}}C_{3\{02\}}$	18	$C_0C_{1\{23\}}C_{2\{30\}}C_{3\{01\}}$
19	$C_0C_{1\{23\}}C_{2\{30\}}C_{3\{02\}}$	20	$C_0C_{1\{23\}}C_{2\{30\}}C_{3\{12\}}$
21	$C_0C_{1\{23\}}C_{2\{30\}}D_3$	22	$C_0C_{1\{23\}}C_{2\{31\}}C_{3\{12\}}$
23	$C_0C_{1\{23\}}C_{2\{31\}}D_3$	24	$C_{01}C_{02}C_{1\{23\}}C_{3\{02\}}$
25	$C_{01}C_{0\{23\}}C_{2\{31\}}C_{3\{01\}}$	26	$C_{01}C_{0\{23\}}C_{2\{31\}}C_{3\{12\}}$
27	$C_{01}C_{2\{30\}}C_{2\{31\}}C_{3\{01\}}$	28	$C_{0\{12\}}C_{0\{13\}}C_{2\{31\}}C_{3\{12\}}$
29	$C_{0\{12\}}C_{1\{23\}}C_{2\{30\}}C_{3\{01\}}$	30	$C_0C_1C_2C_{03}C_{13}$
31	$C_0C_1C_{02}C_{13}C_{23}$	32	$C_0C_1C_{02}C_{23}C_{1\{30\}}$
33	$C_0C_1C_{02}C_{23}C_{3\{02\}}$	34	$C_0C_1C_{02}C_{23}D_3$
35	$C_0C_1C_{23}C_{0\{12\}}C_{1\{30\}}$	36	$C_0C_1C_{23}C_{0\{12\}}C_{3\{12\}}$
37	$C_0C_1C_{23}C_{0\{12\}}D_3$	38	$C_0C_1C_{23}C_{2\{01\}}C_{3\{01\}}$
39	$C_0C_1C_{23}C_{2\{01\}}D_3$	40	$C_0C_1C_{23}D_2D_3$
41	$C_0C_{01}C_{02}C_{12}C_{3\{12\}}$	42	$C_0C_{01}C_{12}C_{23}C_{3\{12\}}$
43	$C_0C_{01}C_{12}C_{2\{30\}}C_{3\{12\}}$	44	$C_0C_{01}C_{12}C_{3\{02\}}C_{3\{12\}}$
45	$C_0C_{01}C_{12}C_{3\{12\}}D_2$	46	$C_0C_{12}C_{13}C_{0\{23\}}C_{2\{31\}}$
47	$C_0C_{12}C_{13}C_{2\{31\}}C_{3\{12\}}$	48	$C_0C_{12}C_{13}C_{2\{31\}}D_3$
49	$C_0C_{12}C_{0\{13\}}C_{2\{31\}}C_{3\{12\}}$	50	$C_0C_{12}C_{0\{13\}}C_{3\{02\}}C_{3\{12\}}$
51	$C_0C_{12}C_{0\{13\}}C_{3\{12\}}D_2$	52	$C_0C_{12}C_{1\{30\}}C_{2\{30\}}C_{3\{12\}}$
53	$C_0C_{12}C_{1\{30\}}C_{2\{30\}}D_3$	54	$C_0C_{12}C_{1\{30\}}C_{3\{12\}}D_2$
55	$C_0C_{12}C_{3\{01\}}C_{3\{12\}}D_2$	56	$C_0C_{12}C_{3\{12\}}D_1D_2$
57	$C_0C_{1\{20\}}C_{1\{30\}}C_{2\{30\}}D_3$	58	$C_{01}C_{02}C_{03}C_{12}C_{3\{12\}}$
59	$C_{01}C_{02}C_{03}C_{1\{23\}}C_{2\{31\}}$	60	$C_{01}C_{02}C_{12}C_{3\{01\}}C_{3\{02\}}$
61	$C_{01}C_{02}C_{13}C_{2\{31\}}C_{3\{02\}}$	62	$C_{01}C_{02}C_{0\{13\}}C_{2\{31\}}C_{3\{12\}}$
63	$C_{01}C_{02}C_{1\{23\}}C_{3\{01\}}C_{3\{12\}}$	64	$C_{01}C_{02}C_{1\{20\}}C_{3\{02\}}C_{3\{12\}}$
65	$C_{01}C_{0\{12\}}C_{2\{31\}}C_{3\{02\}}C_{3\{12\}}$	66	$C_{01}C_{0\{23\}}C_{1\{23\}}C_{2\{30\}}C_{3\{12\}}$
67	$C_{01}C_{0\{23\}}C_{1\{23\}}C_{2\{30\}}D_3$	68	$C_{01}C_{2\{30\}}C_{2\{31\}}C_{3\{02\}}C_{3\{12\}}$
69	$C_{01}C_{2\{30\}}C_{2\{01\}}C_{3\{01\}}C_{3\{12\}}$	70	$C_{01}C_{2\{30\}}C_{2\{01\}}C_{3\{01\}}D_1$
71	$C_{0\{12\}}C_{0\{13\}}C_{1\{23\}}C_{2\{31\}}D_3$	72	$C_{0\{12\}}C_{0\{13\}}C_{1\{20\}}C_{3\{12\}}D_2$
73	$C_{01}C_{02}C_{03}C_{12}C_{13}C_{23}$	74	$C_{01}C_{02}C_{13}C_{23}C_{0\{13\}}C_{2\{31\}}$
75	$C_{01}C_{02}C_{13}C_{0\{13\}}C_{2\{31\}}D_3$	76	$C_{01}C_{23}C_{0\{23\}}C_{1\{23\}}C_{2\{01\}}C_{3\{01\}}$
77	$C_{01}C_{23}C_{0\{23\}}C_{1\{23\}}C_{2\{01\}}D_3$	78	$C_{01}C_{23}C_{0\{23\}}C_{1\{23\}}D_2D_3$

Отметим, что полученные результаты могут служить отправной точкой для построения решетки *основных замкнутых классов* (являющихся пересечениями предполных классов) четырехзначной логики. Кроме того, их удается обобщать на случай произвольного $k \geq 3$, формулируя и доказывая аналогичные утверждения.

Работа выполнена при финансовой поддержке РФФИ (проект 16-01-00593-а).

Список литературы

1. Марченков С. С. Функциональные системы с операцией суперпозиции. — М.: Физматлит, 2004.

2. Rosenberg I. G. Über die funktionale Vollständigkeit in den mehrwertigen Logiken // Rozpravy Československe Akad. Věd. N. 80. Praha: Řada Math. Přir. Věd., 1970. — P. 3–93.

3. Захарова Е. Ю., Кудрявцев В. Б., Яблонский С. В. О предполных классах в k-значных логиках // ДАН СССР. — 1969. — Т. 186. № 3. — С. 509–512.

РАЗБИЕНИЕ РЕШЕТОК КЛОНОВ (СУПЕРКЛОНОВ) НА ИНТЕРВАЛЫ

Н. А. Перязев (Санкт-Петербург), И. К. Шаранхаев (Улан-Удэ)

Пусть A — множество, $B(A)$ — множество всех подмножеств A. Тогда n-местная *операция над* A — это $f : A^n \to A$, а n-местная *мультиоперация над* A — это $f : A^n \to B(A)$. При этом операции можно рассматривать как частный случай мультиопераций, отождествляя элементы с одноэлементными множествами. Обозначим через P_A^n, P_A — множества всех n-местных и всех операций над A, а через M_A^n, M_A — множества всех n-местных и всех мультиопераций над A.

Мультиоперация f на множестве A называется *пустой*, *полной*, *проектирования по i аргументу*, если для любых $a_1, \ldots, a_n$ из A выполняется, соответственно:

$$f(a_1, ..., a_n) = \emptyset, \ f(a_1, ..., a_n) = A, \ f(a_1, ..., a_n) = \{a_i\}.$$

Определим *суперпозицию* мультиопераций $f, f_1, ..., f_n$:

$$f * (f_1, ..., f_n)(a_1, ..., a_m) = \bigcup_{b_i \in f_i(a_1,...,a_m)} f(b_1, ..., b_n);$$

разрешимость мультиоперации f по i-му аргументу:

$$\mu_i f(a_1, ...a_n) = \{a \mid a_i \in f(a_1, ..., , a_{i-1}, a, a_{i+1}, ..., a_n)\};$$

пересечение мультиопераций:

$$(f \cap g)(a_1, ..., a_n) = f(a_1, ..., a_n) \cap g(a_1, ..., a_n).$$

Клоном над множеством A называется любое подмножество $K \subseteq P_A$, содержащее все операции проектирования и замкнутое относительно суперпозиций. *Алгеброй n-местных операций* над A называется любое подмножество $K \subseteq P_A^n$, содержащее все n-местные операции проектирования и замкнутое относительно суперпозиций. В [1] такие алгебры называются m-замкнутыми классами.

Суперклоном над множеством A называется любое подмножество $R \subseteq M_A$, содержащее все полные и пустые мультиоперации проектирования и замкнутое относительно суперпозиций и разрешимостей [2]. *Алгеброй n-местных мультиопераций* над A называется любое подмножество $R \subseteq M_A^n$, содержащее все n-местные мультиоперации проектирования, пустую, полную мультиоперации и замкнутое относительно суперпозиций, разрешимостей и пересечений.

Мощность множества A называется *рангом* клона, суперклона или алгебры. Введем обозначения:
$[F]$ — клон над A, порожденный множеством $F \subseteq P_A$;
$St_n(F) = \{f | f_i^n \in F \Rightarrow f * (f_1^n, ..., f_m^n) \in F\}$;
$\langle\, R \,\rangle$ — суперклон над A, порожденный множеством $R \subseteq M_A^n$;
$St_n(R) = \{g | g_i^n \in R \Rightarrow g * (g_1^n, ..., g_m^n) \in R$ и $(\mu_i g) * (g_1^n, ..., g_m^n) \in R\}$;
$F^n = F \cap P_A^n$; $R^n = R \cap M_A^n$.

Теорема 1. *а) Для любого клона F ранга k выполняется $[F^n] \subseteq F \subseteq St_n(F^n)$. б) Для любого суперклона R ранга k выполняется $\langle\, R^n \,\rangle \subseteq R \subseteq St_n(R^n)$.*

Следствие. *а) Решетка клонов ранга k для любого n разбивается на конечное число интервалов вида $[[K], St_n(K)]$, где K — алгебра n-местных операций ранга k.*

б) Решетка суперклонов ранга 2 для любого n разбивается на конечное число интервалов вида $[\langle\, B \,\rangle, St_n(B)]$, где B — алгебра n-местных мультиопераций ранга 2.

В случае $n = 1$ получается хорошо известное разбиение решетки клонов на моноидальные интервалы [3]. Напомним, что решетки клонов и суперклонов одного ранга являются антиизоморфными, поэтому разбиение решетки клонов определяет некоторое разбиение решетки суперклонов, и наоборот.

Теорема 2. *а) Для любой алгебры K n-местных операций ранга k существует клон F ранга k такой, что $F^n = K$.*

б) Для любой алгебры B n-местных мультиопераций ранга 2 существует суперклон R ранга 2 такой, что $R^n = B$.

Мультиоперации $f \in M_A$, где $A = \{a_0, ..., a_{k-1}\}$ можно представлять как отображения $f : \{2^0, 2^1, ..., 2^{k-1}\}^n \to \{0, 1, ..., 2^k - 1\}$, получаемых из f при кодировке $\{a_{i_1}, ..., a_{i_s}\} \to 2^{i_1} + ... + 2^{i_s}$; $a_i \to 2^i$; $\emptyset \to 0$. Векторная форма $f = (\alpha_1, ..., \alpha_{k^n})$ для n-местной мультиоперации f, определяется следующим образом: $\alpha_i \in \{0, 1, ..., 2^k - 1\}$ и $\alpha_i = f(2^{i_1}, ..., 2^{i_n})$, где $(i_1, ..., i_n)$ есть представление $i - 1$ в системе исчисления по основанию k.

Алгебры унарных операций ранга 2 (всего — 6):
$[(12)], [(11)], [(22)], [(21)], [(11), (22)], [(11), (21)]$.

Алгебры бинарных операций ранга 2 (всего — 26):
$[(1212)], [(1111)], [(2222)], [(2121)], [(1112)], [(1222)], [(1221)],$
$[(2112)], [(1211)], [(2212)], [(2111)], [(1111), (2222)], [(1111), (1112)],$
$[(1111), (1222)], [(1112), (2222)], [(1222), (2222)], [(1111), (2121)],$
$[(1221), (2112)], [(1112), (1222)], [(1211), (1222)], [(1112), (2212)],$
$[(1112), (1111), (2222)], [(1222), (1111), (2222)], [(1112), (1222), (1111)],$
$[(1112), (1222), (2222)], [(1112), (1222), (1111), (2222)]$.

Алгебры унарных мультиопераций ранга 2 (всего — 19):
$\langle (12) \rangle$, $\langle (11) \rangle$, $\langle (22) \rangle$, $\langle (21) \rangle$, $\langle (31) \rangle$, $\langle (23) \rangle$, $\langle (11), (22) \rangle$,
$\langle (11), (23) \rangle, \langle (22), (31) \rangle, \langle (11), (21) \rangle, \langle (13) \rangle, \langle (11), (13) \rangle, \langle (22), (32) \rangle,$
$\langle (13), (31) \rangle$, $\langle (23), (32) \rangle$, $\langle (11), (23), (32) \rangle$, $\langle (22), (13), (31) \rangle$,
$\langle (11), (22), (13) \rangle$, $\langle (31), (23) \rangle$.

Алгебры бинарных мультиопераций ранга 2 (всего — 44):
$\langle (1212) \rangle$, $\langle (1111) \rangle$, $\langle (2222) \rangle$, $\langle (3131) \rangle$, $\langle (1111), (2222) \rangle$,
$\langle (1111), (1313) \rangle$, $\langle (2323) \rangle$, $\langle (1111), (2323) \rangle$, $\langle (2222), (3131) \rangle$,
$\langle (1111), (2121) \rangle$, $\langle (1313) \rangle$, $\langle (2121) \rangle$, $\langle (2222), (3232) \rangle$,
$\langle (1111), (2222), (1313) \rangle$, $\langle (1313), (3131) \rangle$, $\langle (2111) \rangle$,
$\langle (1111), (2323), (3232) \rangle, \langle (2222), (1313), (3131) \rangle, \langle (3331) \rangle, \langle (2333) \rangle,$
$\langle (2323), (3232) \rangle, \langle (3131), (2323) \rangle, \langle (1221) \rangle, \langle (2112) \rangle, \langle (1332) \rangle,$
$\langle (2222), (3331) \rangle, \langle (3331), (3322) \rangle, \langle (3332), (3331) \rangle, \langle (1111), (2333) \rangle,$
$\langle (2333), (1133) \rangle$, $\langle (3331), (2222), (3322) \rangle$, $\langle (2333), (1111), (1133) \rangle$,

$\langle\,(1221),(2112)\,\rangle$, $\langle\,(3332)\,\rangle$, $\langle\,(3332),(2222)\,\rangle$, $\langle\,(3332),(2222),(3331)\,\rangle$, $\langle\,(1333)\,\rangle$, $\langle\,(1333),(2333)\,\rangle$, $\langle\,(1333),(1111)\,\rangle$, $\langle\,(1333),(2333),(1111)\,\rangle$, $\langle\,(1333),(3332)\,\rangle$, $\langle\,(2333),(3332)\,\rangle$, $\langle\,(1333),(3331)\,\rangle$, $\langle\,(1332),(2211)\,\rangle$.

В книге [4] приведено перечисление всех 699 алгебр унарных операций (унарнопорожденных клонов, моноидов операций) ранга 3. В [5] дано описание всех 2079040 алгебр унарных мультиопераций ранга 3.

Список литературы

1. Черепов А. Н., Черепов В. А. Классы сохранения основания в многозначных логиках // Труды 4-й Международной конференции «Дискретные модели в теории управляющих систем» (19–25 июня 2000 г.). — М.: МАКС Пресс, 2000. — С. 135–136.

2. Перязев Н. А., Шаранхаев И. К. Теория Галуа для клонов и суперклонов // Дискретная математика. — 2015. — Т. 27, вып. 4. — С. 79–93.

3. Scendrei A. Clones in universal algebra. — Montreal: Les presses de l'universite de Montreal, 1986.

4. Lau D. Function algebras on finite sets. — Springer-Verlag Berlin YeideWater Resourses Research, 2006.

5. Казимиров А. С., Перязев Н. А. Алгебры унарных мультиопераций // Тезисы докладов Международной конференции «Мальцевские чтения» (11–15 ноября). — Новосибирск, 2013. — С. 156.

ЭКВИВАЛЕНТНЫЕ ПРЕОБРАЗОВАНИЯ В АЛГЕБРАИЧЕСКИХ МОДЕЛЯХ ПРОГРАММ С ПРОЦЕДУРАМИ

Р. И. Подловченко, А. Э. Молчанов (Москва)

Один из разделов теории схем программ посвящен алгебраическим моделям программ [1, 2]. Эти модели строятся для заданной формализации понятия программы и аппроксимируют классы формализованных программ. При формализации программы в [2] учтены все основные композиции базисных операторов и логических

условий, над которыми строятся реальные программы, включая аппарат процедур. Если этот аппарат не используется, то модель называется простой.. Для моделей программ исследуются проблемы эквивалентности и эквивалентных преобразований (э.п.) схем. Первая состоит в поиске алгоритма, который распознает эквивалентность схем в модели. Вторая проблема состоит в построении системы э.п. схем, обладающей свойством полноты: существует алгоритм, который для любых двух эквивалентных схем из данной модели строит конечную цепочку э.п., трансформирующих одну схему в другую. Обе проблемы решены для широкого класса простых алгебраических моделей программ, называемых далее избранными [3]. В данной статье полученные в [3] результаты использованы для решения обеих проблем в некотором классе моделей программ с процедурами.

Нами применялась разработанная в [4] методика α построения полной системы э.п. в модели вычислений, объектами которой являются конечные размеченные графы. Согласно ей вводится понятие фрагмента объекта модели, частным случаем которого является сам объект, и определяется отношение вхождения фрагмента в объект. Для двух фрагментов описывается операция подстановки вместо вхождения в объект одного из них вхождения другого, результатом которой является объект. Таким образом, парой фрагментов определяется преобразование исходного объекта модели в другой. Если независимо от выбора исходного объекта и вхождения в него какого-либо из этой пары фрагментов получаемый объект эквивалентен исходному, то фрагменты объявляются безусловно эквивалентными; в случае алгоритммического ограничения на вхождение — условно эквивалентными. Так вводится формальное исчисление, элементами которого служат фрагменты, единственным правилом вывода — операция подстановки, а аксиомой — множество пар эквивалентных фрагментов. Выбор в качестве аксиом рекурсивных множеств таких пар может индуцировать полную в модели систему э.п. Методика α применяется к модели с разрешимой проблемой эквивалентности и к такой, в каждом классе эквивалентности которой есть каноническая форма. Методика α требует, чтобы разрешающий алгоритм трансформировал эквивалентные схемы в каноническую форму. Анализом операций, выполняемых таким алгоритмом, создаются искомые аксиомы. Полнота индуцируемых ими э.п. обеспечена.

Объектами алгебраических моделей программ, введенных в [2], являются схемы программ, представляющие собой конечные орграфы. Их вершины размечены символами операторов, вызовов и возвратов из множеств Y, C, R соответственно, а дуги — элементами конечного множества X. Граф состоит из подграфов, один из которых

называется главным, а остальные — процедурными. Вход в схему и выход из нее — это вершины главного подграфа, каждый процедурный подграф тоже имеет вершину-вход и вершину-выход. Остальные вершины подразделяются на преобразователи, вызовы и возвраты. Дуга из вызова ведет во вход процедурного подграфа, а из выхода этого подграфа дуга ведет в парный ему возврат. Из каждой вершины типа вход, преобразователь, возврат исходят дуги, помеченные элементами из X. Вычисление схемы проводится на функции разметки, отображающей множество H цепочек символов из Y, C, R в множество X. Вычисление представляет собой обход ее графа, начинающийся во входе схемы при пустой цепочке и сопровождающийся приписыванием к ней символов, помечающих проходимые вершины. Обход завершается при достижении выхода схемы, и полученная цепочка объявляется результатом выполнения схемы на взятой функции разметки. Так схема реализует отображение множества функций разметки в множество H. Эквивалентность схем определяется множеством допустимых функций разметки, на которых выполняются схемы, и отношением эквивалентности в H, используемым при сравнении результатов их выполнения. Пара указанных параметров идентифицирует модель.

В множестве алгебраических моделей программ с процедурами нами отобраны т.н. перегородчатые алгебраические модели, параметры которых индуцируются параметрами ее простой подмодели [5]. В этих моделях выделены классы примитивных схем. В [6] доказано, что разрешимость эквивалентности в классе примитивных схем следует из разрешимости эквивалентности в индуцирующей его простой модели. Далее в качестве последней берется исключительно избранная модель. Важным обстоятельством является то, что для класса примитивных схем выполнены необходимые условия применимости методики α. Исчисление фрагментов примитивных схем строится как расширение такового для избранной модели, изложенное в [3]. В частности, определяется каноническая форма примитивной схемы и доказывается, что существует алгоритм, разрешающий эквивалентность примитивных схем путем их приведения в каноническую форму. Эти результаты, дающие решение проблемы э.п. для класса примитивных схем, индуцированных любой избранной моделью, получены в [7].

Работа выполнена при финансовой поддержке гранта РФФИ (проект 15-01-05742).

Список литературы

1. Подловченко Р. И. Иерархия моделей программ // Программирование. — 1981. — № 2. — С. 3–14.

2. Подловченко Р. И. Рекурсивные программы и иерархия их моделей // Программирование. — 1991. — № 6. — С. 44–51.

3. Подловченко Р. И. Об одном массовом решении проблемы эквивалентных преобразований схем программ // Программирование. — 2000. —№ 1. — С. 66–77; Программирование. — 2000. — № 2. — С. 3–11.

4. Подловченко Р. И. Эквивалентные преобразования в математических моделях вычислений. — М.: Издат. отдел факультета ВМК МГУ, МАКС-Пресс, 2011.

5. Подловченко Р. И., Молчанов А. Э. Разрешимость эквивалентности в перегородчатых моделях программ // Моделирование и анализ информационных систем. — 2014. — Т. 1, вып. 2. — С. 56–70.

6. Подловченко Р. И. Исследование примитивных схем программ с процедурами // Моделирование и анализ информационных систем. — 2014. — Т. 21, вып. 4. — С. 116–131.

7. Молчанов А. Э. Разрешимость проблемы эквивалентных преобразований в классе примитивных схем программ // Труды Института системного программирования РАН. — 2015. — Т. 27, вып. 2. — С. 173–188.

ПОЛНЫЕ СИСТЕМЫ В P-МНОЖЕСТВАХ

А. А. Родин (Москва)

Обозначим через P^2 множество всех ограниченно-детерминированных функций (автоматных отображений), входные и выходные переменные которых определены на множестве бесконечных последовательностей, составленных из нулей и единиц.

Будем считать, что на множестве P^2 определена операция суперпозиции [1]. Пусть $M \subseteq P^2$. Замыкание множества M относительно суперпозиции обозначим через $[M]$.

Пусть D — произвольный замкнутый класс Поста [2]. Введем понятие P-множества, порожденного классом D, — это множество всех ограниченно-детерминированных (о.-д.) функций, в каждом состоянии которых реализуется функция алгебры-логики, принадлежащая D. Будем обозначать такое множество через P_D. Несложно

видеть, что любое P-множество является замкнутым множеством автоматных функций.

В работах [3, 4] рассмотрены особенности P-множеств. Приведем некоторые из них.

Свойство 1. *Пусть класс Поста D содержит тождественную функцию алгебры логики. Тогда существует такая о.-д. функция u, что*

$$[P_D \cup \{u\}] = P^2.$$

Свойство 2. *Пусть несобственный класс Поста D содержит тождественную функцию алгебры логики. Тогда в P^2 существует континуум предполных классов, содержащих P_D.*

Свойство 3. *Пусть несобственный класс Поста D содержит тождественную функцию алгебры логики и обе константы. Тогда существует алгоритм распознавания полноты систем вида $P_D \cup \{M\}$, где M — произвольное конечное множество о.-д. функций.*

Интересно, что алгоритм распознавания полноты существует несмотря на континуальность предполных классов, содержащих P_D. Таким образом, P-множества являются важным объектом с точки зрения задач распознавания полноты. Поэтому интересно рассмотреть P-множество как самостоятельную функциональную систему.

Одной из важных задач, возникающих в любой функциональной системе является исследование свойств полных систем. Очевидно, что не существует конечных полных систем в P-множестве (за исключением тривиальных случаев). В P^2 также не существует конечных полных систем. В [1] показано, что в P^2 существует полная система, не содержащая базиса, вместе с тем, в P^2 можно выделить базис. С этой точки зрения интерес представляет аналогичная задача для функциональной системы P_D, порожденной произвольным множеством D.

Целью данной работы является доказательство следующих утверждений.

Теорема 1. *Пусть $0, 1, x \in D$. Тогда в P_D существует полная система, не содержащая базиса.*

Теорема 2. *Пусть $0, 1, x \in D$. Тогда в P_D существует базис.*

Теорема 3. *Пусть порождающее множество D содержит тождественную функцию алгебры логики и функцию отрицания. Тогда в P_D существует полная система, из которой нельзя выделить базис.*

Теорема 4. *Пусть порождающее множество D содержит тождественную функцию алгебры логики и функцию отрицания. Тогда в P_D существует базис.*

Доказательство всех сформулированных теорем конструктивно.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С Введение в теорию автоматов. — М.: Наука, 1985.

2. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

3. Родин А. А. О некоторых свойствах P-множеств ограниченно-детерминированных функций // Вестник Московского университета. Сер. 1. Математика. Механика. — 2013. — 1. — С. 51–53.

4. Родин А. А. Критерий полноты некоторых систем, содержащих P-множества о.-д. функций // Дискретная математика. — 2013. — Т. 25, вып. 1. — 76–89.

МОЩНОСТЬ МНОЖЕСТВА ДЕЛЬТА-ЗАМКНУТЫХ КЛАССОВ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Д. Е. Стародубцев (Москва)

Исследуются замкнутые классы функций k-значной логики [1, 2]. Известно, что семейство таких замкнутых классов при $k \geq 3$ имеет мощность континуума [1, 3]. С целью получить более "просто" устроенную решетку замкнутых классов функций рассматриваются различные усиления операции суперпозиции (обзор работ в этом направлении см., например, в [4]). В данной работе на множестве функций k-значной логики вводится дополнительная операция — операция обращения, которая в некотором смысле является обратной к операции отождествления переменных. Один из вариантов операции обращения рассматривался в работе [5]. В этой работе были описаны все классы функций k-значной логики ($k \geqslant 3$), замкнутые относительно суперпозиции и введенного варианта обращения. В настоящей работе рассматривается "слабый" вариант операции обращения и показано, что существует континуум классов, замкнутых относительно суперпозиции и "слабого" варианта обращения.

Пусть $k \geqslant 3$. Обозначим через E_k множество $\{0, 1, \ldots, k-1\}$, через P_k — множество всех функций k-значной логики. Для каждого $\varkappa \in E_k$ на множестве функций k-значной логики определим операцию *обращения* с параметром $\varkappa$ следующим образом. Для $n \geqslant 2$

обозначим через A_n множество наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_k^n$, таких, что $\alpha_n = \alpha_i$ для некоторого $i \in \{1, \ldots, n-1\}$. Рассмотрим функцию $f(x_1, \ldots, x_n)$ из P_k. Будем говорить, что функция $g(x_1, \ldots, x_{n+1})$ получена из функции f с помощью операции обращения, если выполнено $g(\alpha_1, \ldots, \alpha_{n+1}) = f(\alpha_1, \ldots, \alpha_n)$ при $(\alpha_1, \ldots, \alpha_{n+1}) \in A_{n+1}$ и $g(\alpha_1, \ldots, \alpha_{n+1}) = \varkappa$ в остальных случаях. Определенную таким образом функцию g будем обозначать через $\Delta_\varkappa(f)$. Через $[F]_\varkappa$ будем обозначать замыкание множества функций F относительно операций суперпозиции и обращения с параметром $\varkappa$. Соответствующие замкнутые классы будем называть *дельта-замкнутыми с параметром* $\varkappa$.

Пусть $\varkappa_1 = \varkappa - 1$ при $\varkappa > 0$ и $\varkappa_1 = 1$ при $\varkappa = 0$; пусть $\varkappa_2 = \varkappa - 2$ при $\varkappa > 1$ и $\varkappa_2 = 2$ при $\varkappa \leqslant 1$. Обозначим при $m \geqslant 2$ через R_m множество всех наборов из E_k^m вида $(\varkappa_2, \ldots, \varkappa_2, \varkappa_1, \varkappa_2, \ldots, \varkappa_2)$. При $n \geqslant 2$ рассмотрим функции $\varphi_n(x_1, \ldots, x_n)$, такие, что $\varphi_n(\alpha_1, \ldots, \alpha_n) = \varkappa_1$ при $\tilde{\alpha} \in R_n$ и $\varphi_n(\alpha_1, \ldots, \alpha_n) = \varkappa$ в остальных случаях. Для каждой функции $f^{(n)} \in P_k$ определим множество $N_f \subseteq E_k^n$ как множество наборов, на которых функция f принимает значения, отличные от $\varkappa$. Далее будем рассматривать только функции, принимающие значения $\varkappa$ и $\varkappa_1$, такие функции, соответственно, на всех наборах из N_f принимают значение $\varkappa_1$. Для набора $(\alpha_1, \ldots, \alpha_n)$ набор $(\alpha_1, \ldots, \alpha_m)$ при $m \leqslant n$ будем называть его *префиксом* длины m.

Пусть $M = \{m_1, m_2, \ldots\} \subseteq (\mathbb{N} \setminus \{1\})$. Будем считать, что M непустое и $m_1 \leqslant m_2 \leqslant \ldots$. Обозначим через Φ_M множество функций, содержащее константу $\varkappa$ и все функции $f(x_1, \ldots, x_n)$ (а также все функции, получающиеся из них переименованием переменных без отождествления), удовлетворяющие следующим условиям:

1. Функция f принимает только значения $\varkappa_1$ и $\varkappa$.

2. Все наборы в N_f состоят только из значений $\varkappa_1$ и $\varkappa_2$.

3. Множество всех переменных, от которых зависит функция f, представимо в виде объединения групп $\{x_1, \ldots, x_p\}$, $\{x_{p+1}, \ldots, x_{p+q}\}$, $\{x_{p+q+1}, \ldots, x_{p+q+r}\}$ (здесь $n = p + q + r$, $q \geqslant m_1$), таких, что:

a) для каждого $i \in \{1, \ldots, p\}$ существует $a \in \{\varkappa_1, \varkappa_2\}$, такое, что из $\tilde{\alpha} \in N_f$ следует, что $\alpha_i = a$;

b) для каждого $i \in \{p+1, \ldots, p+q\}$ найдется $m \in M$, такое, что существуют различные $j_1, \ldots, j_{m-1} \in (\{p+1, \ldots, p+q\} \setminus \{i\})$, такие, что из $\tilde{\alpha} \in N_f$ следует, что $(\alpha_i, \alpha_{j_1}, \ldots, \alpha_{j_{m-1}}) \in R_m$;

c) для каждого $i \in \{p+q+1, \ldots, p+q+r\}$ из $\tilde{\alpha} \in N_f$ следует, что для каждого набора $\tilde{\beta} \in \{\varkappa_1, \varkappa_2\}^r$ набор $(\alpha_1, \ldots, \alpha_{p+q}, \beta_1, \ldots, \beta_r)$ принадлежит N_f.

Переменная первой группы в некоторых случаях может быть отнесена ко второй группе, а переменная второй группы — к первой. Третья группа переменных определяется однозначно.

Пусть $m \geqslant 2$. Обозначим через Ψ_m множество функций $f \in P_k$, удовлетворяющих хотя бы одному из следующих условий:

1. $f \in \Phi_{\mathbb{N}\setminus\{1,m\}}$.

2. $f \in \Phi_{\mathbb{N}\setminus\{1\}}$ и среди переменных, от которых зависит функция f, найдется такая, которая во всех наборах из N_f принимает значение $\varkappa_2$.

Семейства функций Ψ_m обладают следующими свойствами:

Утверждение 1. *При любом $p \geqslant 2$ и любом $\varkappa \in E_k$ класс Ψ_p замкнут относительно операций суперпозиции и обращения с параметром $\varkappa$.*

Утверждение 2. *Для любого $m \geqslant 2$ имеет место соотношение* $\left[\bigcup_{i\in\mathbb{N}\setminus\{1,m\}}\{\varphi_i(x_1,\ldots,x_i)\}\right]_{\varkappa} \subset \Psi_m$.

Из этих утверждений следует факт, приведенный ниже, помогающий доказать основную теорему при помощи рассуждения, аналогичного приведённому в [3].

Утверждение 3. *При всех $m \geqslant 2$ имеет место соотношение* $\varphi_m(x_1,\ldots,x_m) \notin \left[\bigcup_{i\in\mathbb{N}\setminus\{1,m\}}\{\varphi_i\}\right]_{\varkappa}$.

Теорема. *При всех $k \geqslant 3$ и при всех $\varkappa \in E_k$ в P_k существует континуум классов, замкнутых относительно операций суперпозиции и $\Delta_{\varkappa}$.*

Работа выполнена при поддержке РФФИ, проект 14-01-00598 ("Вопросы синтеза, сложности и контроля управляющих систем") и программы фундаментальных исследований ОМН РАН "Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения"(проект "Задачи оптимального синтеза управляющих систем").

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

2. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Berlin: Springer, 2006.

3. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Докл. АН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

4. Угольников А. Б. О некоторых задачах в области многозначных логик // Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, МГУ, 1–6 февраля

2010 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 18–34.

5. Стародубцев Д. Е. Классы функций многозначной логики, замкнутые относительно операций суперпозиции и обращения. Материалы X молодежной научной школы по дискретной математике и ее приложениям (Москва, 5–11 октября 2015 г.) / Под редакцией А. В. Чашкина. — М.: ИПМ им. М. В. Келдыша, 2015. — С. 69–73.

КРИТЕРИЙ НЕЯВНОЙ ПОЛНОТЫ В ТРЕХЗНАЧНОЙ ЛОГИКЕ

М. В. Старостин (Москва)

Понятие неявной выразимости в k-значной логике введено А. В. Кузнецовым как одно из обобщений понятия выразимости по суперпозиции [1].

Функция называется *явно выразимой* над системой Σ функций k-значной логики, если она выразима над системой $\Sigma \bigcup \{x\}$ посредством суперпозиций. Множество всех функций, явно выразимых над системой Σ, называется *явным замыканием* системы Σ и обозначается через $E(\Sigma)$. Говорят, что функция $f(x_1, \ldots, x_n)$ *неявно выразима* над системой функций Σ, если существуют такие явно выразимые над Σ функции $A_j(x_1, x_2, ..., x_n, z)$ и $B_j(x_1, x_2, ..., x_n, z)$, $1 \leq j \leq m$, где z — вспомогательная переменная, что построенная из этих функций система неявных уравнений вида

$$A_j(x_1, x_2, ..., x_n, z) = B_j(x_1, x_2, ..., x_n, z),\ j = 1, ..., m.$$

имеет единственное решение $z = f(x_1, x_2, ..., x_n)$. Множество всех функций, неявно выразимых над Σ, называется *неявным расширением* Σ и обозначается через $I(\Sigma)$. Система $\Sigma \subseteq P_k$ называется *неявно полной* в P_k, если $I(\Sigma) = P_k$. Систему Σ в P_k назовём *неявно предполной*, если она не является неявно полной, но становится таковой при добавлении всякой не принадлежащей ей функции [2].

Проблема неявной выразимости в P_2 решена в [3], где найдены все неявно предполные классы. В работах [2, 4] найдены различные

критерии неявной полноты систем функций в P_k при произвольном $k \geq 2$. Критерий неявной полноты в P_3 в терминах минимальных неявно полных классов функций был получен в [5].

В настоящей работе получен критерий неявной полноты в P_3 в терминах неявно предполных классов. Введем обозначения для этих классов.

Пусть A — замкнутый по суперпозиции класс булевых функций. Через $\Sigma_A^{\{a,b\}}$ обозначим класс всех функций из P_3, сохраняющих подмножество $\{a,b\}$, таких, что при ограничении их на множество $\{a,b\}$ и последующей замене a на 0, b на 1, полученные булевы функции лежат в классе A.

Класс эквивалентности наборов значений переменных функций трёхзначной логики относительно некоторого разбиения множества $\{0,1,2\}$ называется *блоком*.

Пусть A — замкнутый по суперпозиции класс булевых функций. Через $\Sigma_A^{\{a,b\}\{c\}}$ обозначим класс всех функций из P_3, сохраняющих разбиение $\{a,b\}\{c\}$, таких, что все ограничения этой функции на блоках либо совпадают с константой c, либо после замены a на 0, b на 1 становятся функциями из класса A.

Пусть $\mathfrak{N}_3$ — класс квазилинейных функций [4], $DM_i^3, KM_i^3, i \in \{1,2,3\}$ — классы функций, перестановочных с функциями $\max(x,y)$ и $\min(x,y)$ относительно линейных порядков $0 \prec 1 \prec 2, 1 \prec 2 \prec 0, 2 \prec 0 \prec 1$ соответственно [6], F_c — класс сохранения предиката, задаваемого матрицей

$$\begin{pmatrix} a & b & a & a & b & b & c \\ a & b & a & b & a & b & c \\ a & b & c & c & c & c & c \end{pmatrix},$$

R'_c — класс сохранения предиката, задаваемого матрицей [5]

$$\begin{pmatrix} a & b & a & b & c & c & c \\ a & b & c & c & a & b & c \\ a & b & c & c & c & c & c \end{pmatrix},$$

W'_c — класс сохранения предиката, задаваемого матрицей

$$\begin{pmatrix} a & b & a & b & a & b & c \\ a & b & a & b & c & c & c \\ a & b & c & c & a & b & c \end{pmatrix}.$$

Здесь a, b и c — попарно различные элементы множества $\{0,1,2\}$.

Через K (соответственно, D) обозначим класс всех функций равных конъюнкциям (дизъюнкциям) переменных или константам 0, 1. Остальные обозначения см. в [7].

Теорема. *Система $\Sigma \subseteq P_3$ неявно полна тогда и только тогда, когда она целиком не содержится ни в одном из следующих* 54 *неявно предполных классов:* S^3, L^3, $\mathfrak{N}_3$, $T^3_{\epsilon_0,0}$, $T^3_{\epsilon_1,0}$, $T^3_{\epsilon_2,0}$, $\Sigma^{\{0,1\}}_S$, $\Sigma^{\{0,1\}}_K$, $\Sigma^{\{0,1\}}_D$, $\Sigma^{\{0,1\}}_L$, $\Sigma^{\{0,2\}}_S$, $\Sigma^{\{0,2\}}_K$, $\Sigma^{\{0,2\}}_D$, $\Sigma^{\{0,2\}}_L$, $\Sigma^{\{1,2\}}_S$, $\Sigma^{\{1,2\}}_K$, $\Sigma^{\{1,2\}}_D$, $\Sigma^{\{1,2\}}_L$, $\Sigma^{\{0,1\}\{2\}}_{T_0}$, $\Sigma^{\{0,1\}\{2\}}_{T_1}$, $\Sigma^{\{0,1\}\{2\}}_K$, $\Sigma^{\{0,1\}\{2\}}_D$, $\Sigma^{\{0,1\}\{2\}}_L$, $\Sigma^{\{0,2\}\{1\}}_{T_0}$, $\Sigma^{\{0,2\}\{1\}}_{T_1}$, $\Sigma^{\{0,2\}\{1\}}_K$, $\Sigma^{\{0,2\}\{1\}}_D$, $\Sigma^{\{0,2\}\{1\}}_L$, $\Sigma^{\{1,2\}\{0\}}_{T_0}$, $\Sigma^{\{1,2\}\{0\}}_{T_1}$, $\Sigma^{\{1,2\}\{0\}}_K$, $\Sigma^{\{1,2\}\{0\}}_D$, $\Sigma^{\{1,2\}\{0\}}_L$, DM^3_1, KM^3_1, DM^3_2, KM^3_2, DM^3_3, KM^3_3, $U^3_{\epsilon_{0,1},\epsilon_2} \bigcap U^3_{\epsilon_{0,2},\epsilon_1}$, $U^3_{\epsilon_{0,1},\epsilon_2} \bigcap U^3_{\epsilon_{1,2},\epsilon_0}$, $U^3_{\epsilon_{1,2},\epsilon_0} \bigcap U^3_{\epsilon_{0,2},\epsilon_1}$, F_0, F_1, F_2, R'_0, R'_1, R'_2, W'_0, W'_1, W'_2, $T^3_{\epsilon_{0,1},0} \bigcap U^3_{\epsilon_{0,1},\epsilon_2} \bigcap T^3_{\epsilon_2,1}$, $T^3_{\epsilon_{0,2},0} \bigcap U^3_{\epsilon_{0,2},\epsilon_1} \bigcap T^3_{\epsilon_1,1}$, $T^3_{\epsilon_{1,2},0} \bigcap U^3_{\epsilon_{1,2},\epsilon_0} \bigcap T^3_{\epsilon_0,1}$.

Часть приведенных в теореме классов была описана в [4–6, 8].

Работа выполнена при финансовой поддержке РФФИ (проект № 14–01–00598) и Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука. 1979.

2. Касим-Заде О. М. О неявной полноте в k-значной логике // Вестник МГУ. Серия 1. Математика. Механика. — 2007. — № 3.

3. Касим-Заде О. М. О неявной выразимости булевых функций // Вестник МГУ. Серия 1. Математика. Механика. — 1995. — № 2.

4. Орехова Е. А. Об одном критерии неявной полноты в k-значной логике // Математические вопросы кибернетики. Выпуск 11. — М.: Физматлит, 2002.

5. Орехова Е. А. Об одном критерии неявной полноты в трёхзначной логике // Математические вопросы кибернетики. Выпуск 12. — М.: Физматлит, 2003.

6. Данильченко А. Ф. О параметрической выразимости функций трёхзначной логики // Алгебра и логика. — 1977. Т. 16, № 4.

7. Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН СССР. — 1958. — Т. 51. — С. 5–142.

8. Орехова Е. А. О критерии неявной шефферовости в

трёхзначной логике // Дискретный анализ и исследование операций. Серия 1. — 2003. — Т. 10. № 3.

9. Касим-Заде О. М. О неявной выразимости в двузначной логике и криптоморфизмах двухэлементных алгебр // Доклады РАН. — 1996. — Т. 448, № 3. — С. 299–301.

КВАЗИУНИВЕРСАЛЬНЫЕ ИНИЦИАЛЬНЫЕ БУЛЕВЫ АВТОМАТЫ С КОНСТАНТНЫМИ СОСТОЯНИЯМИ

Л. Н. Сысоева (Москва)

Пусть $P_2(n)$ — множество всех булевых функций, зависящих от фиксированных переменных $x_1, x_2, \ldots, x_n$, $n \geq 1$. Под *булевым автоматом* будем понимать автомат $V = (\{0,1\}, \{0,1\}, Q, F, G)$ с произвольным числом входов, входным алфавитом $\{0,1\}$, выходным алфавитом $\{0,1\}$, алфавитом состояний Q, функцией перехода G и функцией выхода F. Определения автомата и инициального автомата можно найти в [1, 2]. Пусть n — число входов автомата V. Без ограничения общности будем полагать, что входы автомата V занумерованы от 1 до n и на i-й вход автомата V подается значение булевой переменной x_i. Тем самым можно считать, что в каждый момент времени на входы автомата V подается некоторый двоичный набор значений переменных $x_1, x_2, \ldots, x_n$ и для любого состояния $q \in Q$ функция выхода $F(q, x_1, x_2, \ldots, x_n)$ является булевой функцией от переменных $x_1, x_2, \ldots, x_n$. Булев автомат V будем называть *булевым автоматом с константными состояниями*, если для любого $q \in Q$ функция $F(q, x_1, x_2, \ldots, x_n)$ является константной булевой функцией 0 или 1.

Пусть $V_{q_1} = (\{0,1\}, \{0,1\}, Q, F, G, q_1)$ — инициальный булев автомат с начальным состоянием q_1 и n входами. Пусть $C = (\widetilde{\beta}_1, \widetilde{\beta}_2, \ldots, \widetilde{\beta}_{2^n})$ — упорядоченная последовательность всех двоичных наборов длины n, $n \geq 1$. Будем говорить, что *автомат V_{q_1} с последовательностью C реализует булеву функцию* $f(x_1, x_2, \ldots, x_n)$, если при последовательной подаче на входы автомата V_{q_1} наборов из C в каждый момент $t = 1, 2, \ldots, 2^n$ на выходе автомата V_{q_1} выдается

значение $f(\widetilde{\beta}_t)$. Будем также говорить, что *функция f реализуется автоматом V_{q_1}*, если для некоторой последовательности наборов C автомат V_{q_1} с последовательностью C реализует f. Обозначим через $P(V_{q_1})$ множество всех булевых функций, реализуемых автоматом V_{q_1}.

Под 0-*состоянием* булевого автомата V будем понимать состояние с функцией выхода $0(x_1, x_2, \ldots, x_n)$, а под 1-*состоянием* — состояние с функцией выхода $1(x_1, x_2, \ldots, x_n)$. Без существенного ограничения общности мы будем рассматривать инициальные булевы автоматы, содержащие хотя бы одно 0-состояние и хотя бы одно 1-состояние, при этом начальным состоянием является 0-состояние. Множество всех таких автоматов с n входами обозначим через $\mathfrak{V}(n)$. Множество всех таких автоматов с k константными состояниями и n входами обозначим через $\mathfrak{V}_k(n)$.

Обозначим через $p_k(n)$ максимальную мощность множества булевых функций из $P_2(n)$, реализуемых автоматом из $\mathfrak{V}_k(n)$. Автоматы из $\mathfrak{V}_k(n)$, реализующие $p_k(n)$ функций, называются *квазиуниверсальными*. В данной работе рассматривается задача получения точного значения $p_3(n)$. Получено, что $p_3(n) = 2^{2^n} - 2^n$, при $n \geq 6$, и описаны все квазиуниверсальные автоматы из $\mathfrak{V}_3(n)$. Аналогичная задача для инициальных булевых автоматов с двумя константными состояниями рассматривалась в работе [3], где было получено, что $p_2(n) = \frac{5}{8} \cdot 2^{2^n}$, при $n \geq 1$, и описаны все квазиуниверсальные автоматы из $\mathfrak{V}_2(n)$. В работах [4, 5] исследовались вопросы реализации булевых функций формулами над автоматными функциями. Сформулируем основные результаты данной работы.

Теорема 1. *Для любого $n \geq 6$ выполняется $p_3(n) = 2^{2^n} - 2^n$.*

Теорема 2. *Для любого $n \geq 2$ максимальная мощность множества $P(V_{q_1})$ для автомата V_{q_1} из $\mathfrak{V}(n)$ равна $2^{2^n} - 2$.*

Можно описать все квазиуниверсальные автоматы из $\mathfrak{V}_3(n)$. Обозначим через $\mathfrak{V}_3^0(n)$ множество всех автоматов из $\mathfrak{V}_3(n)$, содержащих ровно одно 1-состояние. Пусть V_{q_1} — автомат из $\mathfrak{V}_3^0(n)$. Обозначим через A_{00} множество всех наборов, при подаче которых автомат V_{q_1} переходит из начального 0-состояния в 0-состояние, не являющееся начальным. Через A_{01} обозначим множество всех наборов, при подаче которых автомат V_{q_1} переходит из начального 0-состояния в 1-состояние. Через A_{10} обозначим множество всех наборов, при подаче которых автомат V_{q_1} переходит из 1-состояния в начальное 0-состояние. Через B_{00} обозначим множество всех наборов, при подаче которых автомат V_{q_1} переходит из 0-состояния, не являющегося

начальным, в начальное 0-состояние. Через B_{01} обозначим множество всех наборов, при подаче которых автомат V_{q_1} переходит из 0-состояния, не являющегося начальным, в 1-состояние. Через B_{10} обозначим множество всех наборов, при подаче которых автомат V_{q_1} переходит из 1-состояния в 0-состояние, не являющееся начальным. Верна следующая теорема.

Теорема 3. *При $n \geq 9$ автомат V из множества $\mathfrak{V}_3(n)$ является квазиуниверсальным тогда и только тогда, когда V принадлежит $\mathfrak{V}_3^0(n)$ и задается одним из следующих наборов условий:*

1. $A_{00} = \{\widetilde{\alpha}\}$, $A_{01} = \{0,1\}^n \backslash \{\widetilde{\alpha}\}$, $A_{10} = \{\widetilde{\beta}\}$, $B_{01} = \{\widetilde{\beta}\}$, $B_{10} = \{\widetilde{\alpha}\}$, $B_{00} \subseteq \{\widetilde{\mu}, \widetilde{\alpha}\}$;

2. $A_{00} = \{\widetilde{\alpha}\}$,$A_{01} = \{0,1\}^n \backslash \{\widetilde{\alpha}\}$, $A_{10} = \{\widetilde{\beta}\}$, $B_{01} = \{\widetilde{\alpha}, \widetilde{\beta}\}$, $B_{10} = \{\widetilde{\alpha}\}$, $B_{00} \subseteq \{\widetilde{\mu}\}$;

3. $A_{00} = \{\widetilde{\alpha}\}$, $A_{01} = \{0,1\}^n \backslash \{\widetilde{\alpha}, \widetilde{x}\}$, $A_{10} = \{\widetilde{\beta}\}$, $B_{01} = \{\widetilde{\beta}, \widetilde{x}\}$, $B_{10} = \{\widetilde{\alpha}\}$, $B_{00} \subseteq \{\widetilde{\mu}, \widetilde{\alpha}\}$;

4. $A_{00} = \{\widetilde{\alpha}\}$, $A_{01} = \{0,1\}^n \backslash \{\widetilde{\alpha}, \widetilde{x}\}$, $A_{10} = \{\widetilde{\beta}\}$, $B_{01} = \{\widetilde{\alpha}, \widetilde{\beta}, \widetilde{x}\}$, $B_{10} = \{\widetilde{\alpha}\}$, $B_{00} \subseteq \{\widetilde{\mu}\}$;

5. $A_{00} = \{\widetilde{\alpha}, \widetilde{\varkappa}\}$, $A_{01} = \{0,1\}^n \backslash \{\widetilde{\alpha}, \widetilde{\varkappa}\}$, $A_{10} = \{\widetilde{\beta}\}$, $B_{01} = \{\widetilde{\beta}, \widetilde{\varkappa}\}$, $B_{10} = \{\widetilde{\alpha}\}$, $B_{00} \subseteq \{\widetilde{\mu}, \widetilde{\alpha}\}$,

где $\widetilde{\alpha}, \widetilde{\beta}, \widetilde{x}, \widetilde{\mu}$ — различные наборы из $\{0,1\}^n$.

Автор выражает искреннюю признательность Р. М. Колпакову за постановку задачи и обсуждение результатов работы и О. С. Дудаковой за ценные советы и замечания.

Работа выполнена при поддержке РФФИ, проект № 14-01-00598 (“Вопросы синтеза, сложности и контроля управляющих систем”).

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006.

2. Конспект лекций О. Б. Лупанова по курсу “Введение в математическую логику” / Отв. ред. А. Б. Угольников. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М. В. Ломоносова, 2007.

3. Сысоева Л. Н. О реализации булевых функций обобщенными α-формулами // Ученые записки Казанского университета. Сер. Физико-математические науки. — 2014. — Т. 156, вып. 3. — С. 116–122.

4. Сысоева Л. Н. Максимальное число булевых функций, порождаемых инициальным автоматом с двумя константными состояниями // IX Международная конференция «Дискретные модели в тео-

рии управляющих систем», Москва и Подмосковье, 20–22 мая 2015 г.: Труды. — М.: МАКС Пресс, 2015. — С. 239–241.

5. Сысоева Л. Н. О некоторых свойствах обобщенных α-формул // Вестник Московского университета. Сер. 1. Математика. Механика. — 2013. — № 4. — С. 51–55.

ОПТИМИЗИРУЮЩИЕ ПРЕОБРАЗОВАНИЯ ПОТОКОВЫХ ПРОГРАММ

Г. Г. Темербекова, В. А. Захаров (Москва)

Потоковые алгоритмы возникают при решении многих прикладных задач [1]. В статье [2] предложена модель потоковых программ — автоматов-преобразователей над полугруппами — и для нее была исследована проблема эквивалентности. В настоящей работе описан метод оптимизации потоковых программ. Этот метод является обобщением ранее известного подхода, предложенного в статье [3] для минимизации автоматов-преобразователей. Решение задачи минимизации потоковых программ над группами представлено в статье [4].

Пусть заданы конечные множества *операторов* $\mathcal{A}$ и *событий* $\mathcal{C}$. Операторы из $\mathcal{A}$ являются образующими моноида $(S, \circ, e)$; элементы которого играют роль состояний данных. Всякое слово α в алфавите $\mathcal{C}$ (включая пустое слово ε) будем называть *потоком событий*.

Потоковая программа $\pi = \langle V, v_{in}, V_{out}, T, h_0 \rangle$ — это система переходов, состоящая из множества *точек программы* V, *точки входа* v_{in}, множества *точек выхода* V_{out}, *функции переходов* $T\colon\ V \times \mathcal{C} \to V \times \mathcal{A}^*$ и *инициализатора* $h_0, h_0 \in \mathcal{A}^*$. Функцию переходов T можно распространить на потоки событий следующим образом: 1) $T^*(v, \varepsilon) = (v, e)$, и 2) $T^*(v, c\alpha) = (v'', hg)$, если $T(v, c) = (v', h)$ и $T^*(v', \alpha) = (v'', g)$. Программа π вычисляет функцию $\Phi_\pi : C^* \to S$, значения которой определяются следующим образом: если $T^*(v_{in}, \alpha) = (v, h)$ и $v \in V_{out}$, то $\Phi_\pi(\alpha) = h_0 h$; в противном случае значение $\Phi_\pi(\alpha)$ неопределено. Программы π_1 и π_2 называются *S-эквивалентными*, если для любого потока событий α выполняется равенство $\Phi_{\pi_1}(\alpha) =_S \Phi_{\pi_2}(\alpha)$.

Задача минимизации потоковых программ состоит в том, чтобы для заданной программы π построить S-эквивалентную программу с наименьшим числом точек. Решение этой задача приводится для моноидов S, обладающих свойствами R1-R3, описанными ниже.

R1: Для любых g, h_1, h_2 из S верно $gh_1 =_S gh_2 \Rightarrow h_1 =_S h_2$.

В полугруппе S определим бинарное отношение $\preceq_S$, полагая $h_1 \preceq_S h_2 \Leftrightarrow \exists g : h_1 g =_S h_2$, и потребуем, чтобы это отношение обладало следующим свойством.

R2: $(S, \preceq_S)$ — это фундированная решетка, в которой точная нижняя грань любой пары элементов эффективно вычислима.

Для обозначения операции взятия точной нижней грани элементов h_1 и h_2 в решетке $(S, \preceq_S)$ воспользуемся записью $h_1 \vee h_2$. Добавим к S особый элемент τ, полагая $g\tau =_S \tau g =_S \tau$ для любого элемента g из S. Обозначим множество $S \cup \{\tau\}$ записью S^τ. Очевидно, что τ — наибольший элемент ЧУМ $(S^\tau, \preceq_S)$.

R3: Существует алгоритм решения уравнений $hX =_S g$ в моноиде S.

Из условия R3 следует, что проблема тождества в моноиде S разрешима. Требованиям R1-R3 удовлетворяют, например, свободные моноиды, свободные частично коммутативные моноиды (трассы) [5], моноиды консервативных подстановок [6].

Минимизация потоковых программ для моноидов, удовлетворяющих требованиям R1-R3, проводится в три этапа.

Этап 1: вычисление НОД. Наибольшим общим делителем $H(\pi, v)$ точки v программы π назовем точную нижнюю грань множества элементов $\{h : \exists w, v' : \alpha \in C^*, v' \in V_{out}, T^*(v, \alpha) = (v', h)\}$. Для вычисления НОД всех точек программы π составим систему уравнений $EQ = \{X_v = E_v : v \in V\}$ относительно переменных X_v. Для каждой точки v выражение E_v либо является единицей e моноида S в случае $v \in V_{out}$, либо имеет вид $\bigvee\limits_{(u,h)\in\{T(v,c):c\in C\}} hX_u$, если $v \notin V_{out}$.

Теорема 1. *Для любой программы* π *множество* $\{H(\pi, v) : v \in V\}$ *является единственным решением системы уравнений* EQ.

Для решения системы уравнений EQ можно воспользоваться итеративной процедурой последовательной аппроксимации НОД. Здесь существенно важна фундированность решетки $(S^\tau, \preceq_S)$.

Этап 2: редукция программы. Программа π' называется *приведенной*, если $H(\pi', v') = e$ для любой точки v'. Для произвольной программы $\pi = \langle V, v_{in}, V_{out}, T, h_0\rangle$ ее *редукцией* $red(\pi)$ назовем программу $\pi' = \langle V, v_{in}, V_{out}, T', h'_0\rangle$, в которой $h'_0 = h_0 H(\pi, v_{in})$, а значения функции переходов T' для любой пары (v, c) из множества

$V \times \mathcal{C}$ определяется соотношением $T'(v,c) = (u,h') \Leftrightarrow T(v,c) = (u,h)$ и $H(\pi,v)h' =_S hH(\pi,u)$.

Теорема 2. *Для любой программы π ее редукция $red(\pi)$ является приведенной программой, S-эквивалентной π.*

Если вычислены НОД для всех точек программы π, и моноид S удовлетворяет требованию R3, то преобразование программы π в ее редукцию $red(\pi)$ вычисляется эффективно.

Этап 3: минимизация программы. Поставим в соответствие каждой программе $\pi = \langle V, v_{in}, V_{out}, T, h_0\rangle$ автомат Рабина-Скотта $M_\pi = (\mathcal{C} \times \mathcal{A}^*, V, v_{in}, V_{out}, \varphi)$, в котором функция переходов φ определяется условием $\varphi(v,(c,h)) = u \Leftrightarrow T(v,c) = (u,h)$. Программы π_1 и π_2 назовем *автоматно эквивалентными*, если автоматы M_{π_1} и M_{π_2} допускают один и тот же язык.

Теорема 3. *Приведенные программы π_1 и π_2 эквивалентны тогда и только тогда, когда эти программы автоматно эквивалентны.*

В доказательстве теоремы 3 используется тот факт, что в ЧУМ $(S^\tau, \preceq_S)$ любые два элемента имеют точную верхнюю грань.

Таким образом, для минимизации приведенной программы можно применить любой из известных алгоритмов минимизации детерминированных конечных автоматов.

Работа выполнена при финансовой поддержке гранта РФФИ (проект 15-01-05742).

Список литературы

1. Veanes M., Hooimeijer P., Livshits B., et al. Symbolic finite state transducers: algorithms and applications // Proceedings of the 39th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages. — 2012. — P. 137–150.

2. Захаров В. А. Моделирование и анализ поведения последовательных реагирующих программ // Тр. Института системного программирования РАН. — 2015. — Т. 27, № 2. — С. 221–250.

3. Mohri M. Minimization algorithms for sequential transducers // Theoretical Computer Science. — 2000. — V. 234. — P. 177–201.

4. Захаров В. А. Подымов В. В. Применение алгоритмов проверки эквивалентности для оптимизации программ // Тр. Института системного программирования РАН. — 2015. — Т. 27, № 4. — С. 145–174.

5. Diekert V., Metivier Y. Partial commutation and traces // Handbook of formal languages. — 1997. — V. 3 — P. 457–533.

6. Zakharov V.A. On the decidability of the equivalence problem for orthogonal sequential programs // Grammars. — 1999. — V. 2, Is. 3. — P. 271–281.

О ПРИБЛИЖЕНИЯХ РАСПРЕДЕЛЕНИЙ ВЕРОЯТНОСТЕЙ С ПОМОЩЬЮ БУЛЕВЫХ ФУНКЦИЙ ИЗ ЗАМКНУТЫХ КЛАССОВ

А. Д. Яшунский (Москва)

Рассматривается задача приближения бернуллиевских распределений путем подстановки вместо переменных некоторых булевых функций независимых бернуллиевских случайных величин, равных 1 с вероятностью p и 0 с вероятностью $1-p$.

Р. Л. Схиртладзе в [1] показал, что функции, выражаемые бесповторными формулами над $\{\&, \vee, {}^-\}$, позволяют сколь угодно точно приблизить произвольное бернуллиевское распределение. Автором в [2] показано, что для приближения произвольных распределений достаточно бесповторных формул над $\{\&, \vee\}$, а также найдены некоторые достаточные условия приближения произвольного распределения бесповторными формулами над заданной системой функций.

Рассмотрение произвольных (а не только бесповторных) формул над заданной системой булевых функций естественным образом приводит к изучению приближений распределений булевыми функциями из замкнутых классов. В данной работе исследуется, какие распределения могут быть приближены функциями из различных замкнутых классов.

Введем необходимые определения. *Весом* набора $\alpha \in \{0,1\}^n$ называется число единичных компонент в α. Пусть задана булева функция $f(x_1, \ldots, x_n)$. Количество наборов веса i, на которых f равна единице, обозначим через A_i. Тогда *характеристическим многочленом* функции $f(x_1, \ldots, x_n)$ называется

$$h_f(p) = \sum_{i=0}^{n} A_i p^i (1-p)^{n-i}.$$

Легко видеть, что $0 \le A_i \le \binom{n}{i}$, откуда $0 \le h_f(p) \le 1$ для любой функции f при любом $p \in [0,1]$.

Содержательно характеристический многочлен функции f выражает вероятность обращения в 1 этой функции при подстановке вместо всех ее переменных независимых одинаково распределенных бернуллиевских случайных величин, равных 1 с вероятностью p и 0 с вероятностью $1-p$.

Для множества $X \subseteq [0,1]$ через $cl(X)$ будем обозначать (топологическое) замыкание X, т. е. множество X, дополненное всеми своими предельными точками. Пусть $\mathcal{A}$ — множество булевых функций.

Положим:

$$W_{\mathcal{A}}(p) = cl(\{h_f(p) : f \in \mathcal{A}\}).$$

$W_{\mathcal{A}}(p)$ будем называть *множеством распределений, аппроксимируемых функциями из* $\mathcal{A}$ *в точке* p. Содержательно $W_{\mathcal{A}}(p)$ состоит из всех значений на отрезке $[0,1]$, которые могут быть сколь угодно точно приближены значениями характеристических многочленов функций из множества $\mathcal{A}$ в точке p. В частности, если $W_{\mathcal{A}}(p) = [0,1]$, то, подставляя в функции из множества $\mathcal{A}$ независимые одинаково распределенные случайные величины с заданным бернуллиевским распределением $(1-p, p)$, можно сколь угодно точно приблизить произвольное бернуллиевское распределение.

В настоящей работе установлен вид множества $W_{\mathcal{A}}(p)$ для всех замкнутых классов булевых функций $\mathcal{A}$ при всех $p \in (0,1)$. В дальнейшем изложении используются обозначения замкнутых классов, принятые в [3].

Теорема 1. *Пусть* $\mathcal{A}$ *— один из замкнутых классов* M_{01}, M_0, M_1, T_0, T_1, T_{01}, M, P_2. *Тогда* $W_{\mathcal{A}}(p) = [0,1]$ *при всех* $p \in (0,1)$.

Теорема 2.

$$W_S(p) = W_{S_{01}}(p) = \begin{cases} [0,1] \text{ при } p \in (0,1/2) \cup (1/2,1), \\ \{1/2\} \text{ при } p = 1/2. \end{cases}$$

Теорема 3. *Пусть* $\mathcal{A}$ *— один из классов* I^μ, MI^μ, I_1^μ, MI_1^μ. *Тогда*

$$W_{\mathcal{A}}(p) = \begin{cases} [0,p], \text{ если } 0 < p \le 1 - \frac{1}{\mu}, \\ [0,1], \text{ если } 1 - \frac{1}{\mu} < p < 1. \end{cases}$$

Пусть $\mathcal{A}$ *— один из классов* O^μ, MO^μ, O_0^μ, MO_0^μ. *Тогда*

$$W_{\mathcal{A}}(p) = \begin{cases} [0,1], \text{ если } 0 < p < \frac{1}{\mu}, \\ [p,1], \text{ если } \frac{1}{\mu} \le p < 1. \end{cases}$$

Теорема 4. *Пусть* $\mathcal{A}$ *— один из классов* I^∞, MI^∞, I_1^∞, MI_1^∞. *Тогда* $W_{\mathcal{A}}(p) = [0,p]$. *Пусть* $\mathcal{A}$ *— один из классов* O^∞, MO^∞, O_0^∞, MO_0^∞. *Тогда* $W_{\mathcal{A}}(p) = [p,1]$.

Теорема 5.

$$W_{SM}(p) = \begin{cases} [0,p], \text{ при } 0 < p < 1/2, \\ 1/2, \text{ при } p = 1/2, \\ [p,1], \text{ при } 1/2 < p < 1. \end{cases}$$

Теорема 6. *Пусть $\mathcal{A}$ — один из классов K, K_0, K_1, K_{01}. Тогда при любом $p \in (0,1)$ имеет место $W_{\mathcal{A}}(p) \subseteq \bigcup\limits_n \{p^n\} \cup \{0,1\}$.*

Теорема 7. *Пусть $\mathcal{A}$ — один из классов D, D_0, D_1, D_{01}. Тогда при любом $p \in (0,1)$ имеет место $W_{\mathcal{A}}(p) \subseteq \bigcup\limits_n \{1-(1-p)^n\} \cup \{0,1\}$.*

Теорема 8. *Пусть $\mathcal{A}$ — один из классов L, L_0, L_1, L_{01}, SL. Тогда при любом $p \in (0,1)$ имеет место $W_{\mathcal{A}}(p) \subseteq \bigcup\limits_n \{\frac{1}{2}(1 \pm (1-2p)^n)\} \cup \{\frac{1}{2}\}$.*

Теорема 9. *Пусть $\mathcal{A}$ — один из классов U, SU, U_0, U_1, MU, C, C_0, C_1, U_{01}. Тогда при любом $p \in (0,1)$ имеет место $W_{\mathcal{A}}(p) \subseteq \{0, 1, p, 1-p\}$.*

Автор выражает благодарность О. М. Касим-Заде за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект № 14–01–00598) и Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Схиртладзе Р. Л. О методе построения булевой величины с заданным распределением вероятностей // Дискретный анализ. Вып. 7. — Новосибирск: ИМ СО АН СССР, 1966. — С. 71–80.

2. Яшунский А. Д. О преобразованиях вероятности бесповторными булевыми формулами // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.) — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 150–155.

3. Угольников А. Б. Классы Поста. Учебное пособие. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М. В. Ломоносова, 2008.

Секция «Комбинаторный анализ»

ОБОБЩЕННЫЕ МНОГОЧЛЕНЫ МОЦКИНА И ИХ СВОЙСТВА

Л. Н. Бондаренко (Пенза), М. Л. Шарапова (Москва)

В [1] рассматриваются гибридные многочлены Эрмита—Лагерра

$$P_n^{(\alpha)}(x,t) = \sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{x^k t^{n-2k}}{(n-2k)!k!\Gamma(k+\alpha+1)}, \qquad (1)$$

где $[\cdot]$ — целая часть числа, $\Gamma(z)$ — гамма-функция. Их производящая функция $\sum_{n=0}^{\infty} P_n^{(\alpha)}(x,t)\, u^n/n! = (xu^2)^{-\alpha/2} e^{tu} I_\alpha(2u\sqrt{x})$, где $I_\alpha(z)$ — модифицированная функция Бесселя первого рода порядка α.

На базе многочленов (1) в [1] введены s-ассоциированные центральные триномиальные коэффициенты $C_n^{(s)} = P_n^{(s)}(1,1), s = 0,1,\ldots$, удовлетворяющие соотношению $2(n+1)C_n^{(s+1)} = C_{n+2}^{(s)} - C_{n+1}^{(s)}$, а числа $M_n = C_n^{(1)}$ являются известными числами Моцкина [2, 3]. Несмотря на привлекательность этого подхода, для обобщения чисел Моцкина лучше подходит другой путь, базирующийся на следующем понятии.

Определение 1. Многочлены Моцкина $L_n^{(r)}$ порядка $r = 1, 2, \ldots$ зададим выражением

$$L_n^{(r)}(t) = \frac{1}{rn+1} \sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{rn+1}{n-2k} \binom{(r-1)n+2k+1}{k} t^{n-2k}. \qquad (2)$$

Это определение мотивировано тем, что $M_n = L_n^{(1)}(1)$, а числа $M_n^{(2)} = L_n^{(2)}(1)$ [4] являются обобщением чисел Моцкина. Поэтому $M_n^{(r)} = L_n^{(r)}(1)$ назовем числами Моцкина порядка r.

Теорема 1. *Для многочленов $L_n^{(r)}(t)$ справедливо соотношение*

$$L_n^{(r)}(t) = \frac{1}{2^n n!} D_v^{n-1} \left((\sqrt{4v+t^2}+t)^n (v+1)^{rn} \right)\Big|_{v=0}, \; D_v = \frac{\partial}{\partial v}. \qquad (3)$$

Доказательство. Применение к равенству (3) формул бинома Ньютона и Лейбница для $(n-1)$-й производной от произведения функций позволяет получить выражение

$$L_n^{(r)}(t) = \frac{(rn)!}{2^n n!} \sum_{k=0}^{n-1} \binom{n-1}{k} \frac{t^{n-2k}}{((r-1)n+k+1)!} 2^k \sum_{i=0}^{n} \binom{n}{i} \prod_{j=0}^{k-1} (i-2j),$$

внутренняя сумма в котором при $k = 0, 1, \ldots, n-1$ равна

$$\sum_{i=0}^{n} \binom{n}{i} \prod_{j=0}^{k-1} (i-2j) = 2^k D_z^k \, (1+\sqrt{z})^n \big|_{z=1} = \frac{2^{n-k} n (n-k+1)!}{(n-2k)!}$$

и обращается в нуль при $k > [n/2]$, что доказывается с помощью гипергеометрических функций и приводит к выражению (2).

Теорема 2. *Производящей функции* $v = F_r(t,u) = \sum_{n=1}^{\infty} L_n^{(r)}(t) u^n$, *описывающей многочлены Моцкина порядка* r, *отвечает обратная функция* $u = F_r^{-1}(t,v) = 2v(\sqrt{4v+t^2}+t)^{-1}(v+1)^{-r}$, *и справедливо рекуррентное соотношение*

$$L_0^{(r)}(t) = 1, \; L_{n+1}^{(r)}(t) = t \left\langle L_n^{(r)}(t) \right\rangle^r + \left\langle L_{n-1}^{(r)}(t) \right\rangle^{2r}, \; n \geq 0, \qquad (4)$$

где $\langle Q_n(t) \rangle^m = \sum_{k_1+\ldots+k_m=n,\, k_i \geq 0} Q_{k_1}(t) \ldots Q_{k_m}(t)$ — *свертка кратности* m *последовательности многочленов* $\{Q_k(t)\}_0^n$ k*-й степени.*

Доказательство. Первое утверждение теоремы 2 вытекает из формулы (3) и теоремы Лагранжа [3]. Применение производящей функции $v = F_r(t,u)$, увеличенной на 1, к выражению для функции $u = F_r^{-1}(t,v)$ дает алгебраическое уравнение для вычисления производящей функции $u^2(v+1)^{2r} + tu(v+1)^r - (v+1) + 1 = 0$. Так как коэффициент при u^n степенного ряда $(v+1)^r$ равен r-кратной свертке $\langle L_n^{(r)}(t) \rangle^r$, то сравнение коэффициентов в этом уравнении при степенях u приводит к рекуррентной формуле (4). Отметим, что при $r = 1$, $t = 1$ записанное уравнение и соотношение (4) соответствуют известным формулам для чисел Моцкина [2].

В [5] изучались перестановки Гесселя—Стенли (ГС-перестановки) порядка r, т. е. перестановки $\sigma = \sigma_1 \ldots \sigma_{rn}$, $r = 1, 2, \ldots$ мультимножества $\{1^r, \ldots, n^r\}$, у которых все буквы, стоящие между любыми двумя вхождениями символа $i \in \{1, \ldots, n\}$ не меньше этого i.

Подслово ГС-перестановки σ порядка r с совпадающими окаймляющими символами, в котором каждый символ повторяется ровно r раз, назовем ГС-подсловом (при $r = 1$ все символы σ являются ГС-подсловами), причем σ имеет n ГС-подслов. Например, перестановка 123332244411 имеет ГС-подслова: $123332244411, 233322, 333, 444$.

Для двух смежных ГС-подслов η_1, η_2 ГС-перестановки порядка r естественно вводится отношение порядка: $\eta_1 < \eta_2$, если окаймляющий символ η_1 меньше окаймляющего символа η_2.

Определение 2. ГС-перестановку σ порядка r будем называть М-перестановкой порядка r, если она обладает свойствами: 1) σ является 312-избегающей ГС-перестановкой порядка r, т. е. не существует тройки индексов $i < j < k$, для которых выполняется неравенство $\sigma_j < \sigma_k < \sigma_i$; 2) в σ отсутствуют три смежных возрастающих ГС-подслова, т. е. нет смежных ГС-подслов η_1, η_2, η_3, для которых $\eta_1 < \eta_2 < \eta_3$.

Отметим, что 312-избегающие обычные перестановки были введены Д. Кнутом, а их свойства описаны, например, в [3].

Пусть $\mathcal{M}_n^{(r)}$ — множество всех М-перестановок порядка r над алфавитом $\{1, \ldots, n\}$. Для каждого слова $\sigma \in \mathcal{M}_n^{(r)}$ определим число подъемов $0 \le \mathrm{rim}(\sigma) \le [n/2]$ всех смежных ГС-подслов выражением $\mathrm{rim}(\sigma) = \#\{i : \eta_i < \eta_j,\ \eta_i, \eta_j - \text{смежные подслова},\ \sigma \in \mathcal{M}_n^{(r)}\}$. Например, для $\sigma = 123344432211 \in \mathcal{M}_4^{(3)}$ имеем $\mathrm{rim}(\sigma) = 0$, а для $\sigma = 111233344422 \in \mathcal{M}_4^{(3)}$ — $\mathrm{rim}(\sigma) = 2$.

Теорема 3. $L_n^{(r)}(t) = \sum_{\sigma \in \mathcal{M}_n^{(r)}} t^{n-2\mathrm{rim}(\sigma)}$, $M_n^{(r)} = L_n^{(r)}(1) = |\mathcal{M}_n^{(r)}|$, *коэффициент при* t^{n-2k} *в* $L_n^{(r)}(t)$ *равен* $\#\{\sigma \in \mathcal{M}_n^{(r)} : \mathrm{rim}(\sigma) = k\}$.

Теорема 3 дает комбинаторную интерпретацию обобщенных чисел Моцкина и коэффициентов многочлена $L_n^{(r)}(t)$.

Работа выполнена при финансовой поддержке первого автора грантом РФФИ (проект 14-01-00273).

Список литературы

1. Blasiak P., Dattoli G., Horzela A., Penson K. A., Zhukovsky K. Motzkin numbers, central trinomial coefficients and hybrid polynomials // Jornal of Integer Sequenses. — 2008. — 11. — Art. 08.1.1. — P. 11.

2. Sloane N. J. A. The on-line encyclopedia of integer sequences. — `http://oeis.org/A001006` — 2015.

3. Стенли Р. Перечислительная комбинаторика. Т. 2. — М.: Мир, 2009.

4. Sloane N. J. A. The on-line encyclopedia of integer sequences. — http://oeis.org/A006605 — 2015.

5. Бондаренко Л. Н., Шарапова М. Л. Параметрические комбинаторные задачи и методы их исследования // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2010. — № 4. — С. 50–63.

ЗАДАЧА ПОИСКА ШИРИНЫ СИМПЛЕКСА, ЗАДАННОГО СИСТЕМОЙ С ОГРАНИЧЕННЫМ СПЕКТРОМ МИНОРОВ

Д. В. Грибанов (Нижний Новгород)

В данной работе рассматривается сложность задачи поиска ширины симплекса заданного целочисленной системой линейных неравенств. Пусть $A \in \mathbb{Z}^{m\times n}$ и $b \in \mathbb{Z}^n$, как $P(A,b)$ обозначим полиэдр заданный системой неравенств $Ax \leq b$, другими словами $P(A,b) = \{x \in \mathbb{R}^n : Ax \leq b\}$. Пусть $\Delta_k(A)$ и $\delta_k(A)$ есть максимальное и минимальное абсолютные значение $k \times k$ миноров матрицы A.

Шириной выпуклого тела P будем называть следующую величину: $\mathrm{width}(P) = \min_{c\in\mathbb{Z}^n\setminus\{0\}}\{\max\{c^\top x : x \in P\} - \min\{c^\top x : x \in P\}\}$. Хинчиным [4] был установлен следующий факт: если P не содержит точек из $\mathbb{Z}^n$, то $\mathrm{width}(P) \leq f(n)$, где величина $f(n)$ зависит только от размерности. Существует много оценок на величину $f(n)$. Наилучшая оценка $O(n^{3/4}\log^c(n))$ дана в работе [6]. Наилучшая оценка для симплексов $O(n\,\log(n))$ дана в работе [1]. Дополнительные результаты о ширине симплксов приведены в работе [5].

В работах [2, 3] приведены аналоги теоремы Хинчина, где дополнительным условием является некоторое ограничение на миноры системы задающей политоп. Приведем один из основных результатов данных работ, верный для симплексов.

Теорема 1. *Пусть $A \in \mathbb{Z}^{(n+1)\times n}$, $b \in \mathbb{Z}$ и $P = P(A,b)$ есть симплекс размерности n. Если* $\mathrm{width}(P) \geq \delta_n(A) - 1$, *то $P \cap \mathbb{Z}^n \neq \emptyset$. Более того, в данном случае существует полиномиальный алгоритм предъявляющий целую точку внутри P.*

Задача подсчета ширины симплекса является NP-трудной, как было показано в работе [8]. В случае же ограниченности миноров

системы, задающей симплекс, сложность задачи становится полиномиальной, что показано в данной работе. Имеет место следующая теорема.

Теорема 2. *Пусть* $A \in \mathbb{Z}^{(n+1)\times n}$, $b \in \mathbb{Z}$ *и* $P = P(A, b)$ *есть симплекс размерности* n. *Если величина* $\max\{\Delta_n(A\,b), \Delta_{n-1}(A)\}$ (*под* $(A\,b)$ *имеется в виду расширенная матрица системы*) *фиксирована, то задача вычисления ширины* P *является полиномиально разрешимой.*

Для симплексов, не имеющих целых точек, условия теоремы 2 можно смягчить, а именно можно избавиться от условий на правую часть системы.

Теорема 3. *Пусть* $A \in \mathbb{Z}^{n\times(n+1)}$, $b \in \mathbb{Z}$ *и* $P = P(A, b)$ *есть симплекс размерности* n, *причем* $P \cap \mathbb{Z}^n = \emptyset$. *Если величина* $\max\{\Delta_n(A), \Delta_{n-1}(A)\}$ *фиксирована, то задача вычисления ширины* P *является полиномиально разрешимой.*

Алгоритм, лежащий в основе данной теоремы, использует алгоритмический результат о разбиении произвольного простого конуса на унимодулярные конуса, принадлежащий А. Ю. Чиркову и упомянутый в монографии [9]. Алгоритм также использует процедуру построения *нормальной диагональной формы Смита* [7], одна из наиболее оптимальных версий данной процедуры приведена в работе [10].

Также в данной работе была исследована задача целочисленной оптимизации на симплексе заданном выпуклой оболочкой точек, образующих матрицу с ограниченными минорами. Было показано существование квази-полиномиального алгоритма в данном случае где под квази-полиномиальным алгоритмом понимается алгоритм со сложностью $O(2^{poly(\log\, n)})$.

Теорема 4. *Пусть* $A \in \mathbb{Z}^{(n+1)\times n}$, $c \in \mathbb{Z}^n$ *и* $P = \mathrm{conv}(A)$ *есть симплекс размерности* n (*под* $\mathrm{conv}(A)$ *будем понимать выпуклую оболочку столбцов матрицы* A). *Если величина* $\Delta_n(A)$ *фиксирована, то для решения задачи* $\max\{c^\top x : x \in P \setminus \mathrm{vert}(P) \cap \mathbb{Z}^n\}$ *существует квази-полиномиальный алгоритм. Более того, если величина, равная сумме* $n \times n$ *миноров матрицы* A *фиксирована, то для решения задачи* $\max\{c^\top x : x \in P \setminus \mathrm{vert}(P) \cap \mathbb{Z}^n\}$ *существует полиномиальный алгоритм.*

Список литературы

1. Banaszczyk W., Litvak A. E., Pajor A., Szarek S.J̇. The flatness theorem for non-symmetric convex bodies via the local theory of Banach spaces // Mathematics of operations research. — 1999. — 24 (3). —

P. 728–750.

2. Gribanov D. V. The flatness theorem for some class of polytopes and searching an integer point // Springer Proceedings in Mathematics & Statistics. Models, Algorithms and Technologies for Network Analysis. — 2013. — 104. — P. 37–45.

3. Gribanov D. V., Veselov S. I. On integer programming with bounded determinants // Optimization Letters. Online first.

4. Khinchine A. A quantitative formulation of Kronecker's theory of approximation // Izvestiya Akademii Nauk SSR Seriya Matematika. — 1948. — 12. — P. 113–122.

5. Haase C., Ziegler G. On the maximal width of empty lattice simplices // Europ. J. Combinatorics. — 2000. — 21. — P. 111-119.

6. Rudelson M. Distances between non-symmetric convex bodies and the MM^* -estimate // Positivity. — 2000. — 4(2). — P. 161–178.

7. Schrijver A. Theory of linear and integer programming. — WileyInterscience series in discrete mathematics. John Wiley & Sons, 1998.

8. Sebö A. An introduction to empty lattice simplexes // Cornuéjols, G., Burkard, R.R., Woeginger, R.E. LNCS. — 1999. — 1610. — P. 400–414.

9. Shevchenko V.N. Qualitative topics in integer linear programming (Translations of Mathematical Monographs). — AMS, 1996.

10. Storjohann A. Near optimal algorithms for computing Smith normal forms of integer matrices // ISSAC'96 Proceedings of the 1996 international symposium on Symbolic and algebraic computation. ACM Press. — 1996. — P. 267–274.

О ВОЗМОЖНЫХ ЗНАЧЕНИЯХ МАКСИМУМА ОТНОСИТЕЛЬНОГО ВЛИЯНИЯ ПЕРЕМЕННЫХ ДЛЯ БУЛЕВЫХ ФУНКЦИЙ

И. В. Грибушин (Москва)

В работе [1] дана нижняя оценка максимального значения влияния переменных булевой функции, что позволяет описать класс булевых функций, на которых достигается минимум максимального влияния переменных. В настоящей работе предложены точные верхняя и нижняя оценки максимального относительного влияния переменных для булевых функций и описан класс функций, на котором достигаются граничные значения.

Рассмотрим булеву функцию $f : \{-1,1\}^n \to \{-1,1\}$ от n переменных. Пусть $[n] := \{1, ..., n\}$.

Определение 1 [2]. Характеристической функцией множества $S \subseteq [n]$ называется: $\chi_S := \prod_{i \in S} x_i, \chi_\emptyset := 1$.

Определение 2 [2]. Пусть x равномерно распределено на пространстве $\{-1,1\}^n$. Коэффициентом Фурье функции f относительно $S \subseteq [n]$ называется: $\hat{f}(S) := \hat{f}_S := \mathbf{E} f(x)\chi_S(x)$.

Из равенства Парсеваля [2] следует, что $\sum_{S \subseteq [n]} \hat{f}(S)^2 = 1$.

Определение 3 [3]. Влиянием i-й переменной на функцию f называется: $Inf_i := \mathbf{Pr}_{x \in \{-1,1\}^n}[f(x) \neq f(x^{\oplus i})]$.

Замечание 1 [1]. $Inf_i(f) = \sum_{i \in S \subseteq [n]} \hat{f}(S)^2$.

Определение 4 [3]. Полным влиянием функции f называется величина $Inf(f) := \sum_{i=1}^{n} Inf_i(f)$.

Определение 5. Функции f и $\tilde{f}$ называются эквивалентными, если они имеют одинаковые множества влияний переменных:

$$\{Inf_i(f) | i \in [n]\} = \{Inf_i(\tilde{f}) | i \in [n]\}.$$

Определение 6. Относительным влиянием i-ой переменной на функцию f называется величина $\tau_i = \frac{Inf_i(f)}{Inf(f)}$.

Определение 7 [4]. f называется τ-регулярной для некоторого $\tau > 0$, если $\forall i \in [n] : Inf_i(f) \leq \tau Inf(f)$.

Из определения 7 имеем:

$$\max_{i \in [n]} Inf_i(f) \leq \tau Inf(f) \Rightarrow \max_{i \in [n]} \frac{Inf_i(f)}{Inf(f)} \leq \tau.$$

Так как для любой τ-регулярной функции имеет смысл рассматривать только наименьшее возможное значение τ, получаем, что $\tau = \max_{i \in [n]} \frac{Inf_i(f)}{Inf(f)}$.

Пусть $a \in \{-1,1\}^n$ — точка на булевом кубе, тогда положим $\delta_a(x) = \{1, \text{если } x = a; -1, \text{в противном случае}\}$.

Обозначим I_f — множество, на котором $f = 1$; $k_1(f) := |I_f|$; $M_+ := \{1\} \times \{-1,1\}^{n-1}$ и $M_- := \{-1\} \times \{-1,1\}^{n-1}$ — множества, на которых $x_1 = 1$ и $x_1 = -1$ соответственно. Пусть $k_+(f) := |M_+ \cap I_f|$ и $k_-(f) := |M_- \cap I_f|$ — количество точек в верхнем и нижнем полугиперпространствах относительно переменной x_1, в которых $f = 1$.

Положим $k'_- := \min(k_-, 2^{n-1} - k_-)$; $k'_+ := \min(k_+, 2^{n-1} - k_+)$; $k'_1(f) := k'_+(f) + k'_-(f)$.

Утверждение 1. *Любая булева функция f может быть представлена в виде*: $f = \sum_{x \in I_f} \delta_x + |I_f| - 1$.

Лемма 1. *Для любой булевой функции f и любого $S \neq \emptyset, \{1\}$ выполнено* : $\left|\hat{f}_S\right| \leq \frac{k'_+ + k'_-}{2^{n-1}}$.

Утверждение 2. *Если k'_1 нечетное, то $\tau \leq \frac{2^{n-1}-1}{2^{n-1}+n-2}$. Равенство достигается тогда и только тогда, когда $Inf_1 = \frac{2^{n-1}-1}{2^{n-1}}$ и $Inf_{i \neq 1} = \frac{1}{2^{n-1}}$.*

Утверждение 3. *Если k'_1 четное, то $\tau \leq \frac{2^{n-2}}{2^{n-2}+n-1}$. Равенство достигается тогда и только тогда, когда $Inf_1 = 1$ и $Inf_{i \neq 1} = \frac{1}{2^{n-2}}$.*

Утверждение 4. *Все возможные значения τ для τ-регулярных булевых функций от не более, чем 3 переменных*: $0, \frac{1}{3}, \frac{3}{7}, \frac{1}{2}, \frac{3}{5}$ *и* 1.

Теорема 1. *Множество возможных значений τ для пороговых функций, существенно зависящих от 4 переменных равно*:

$$\left\{\frac{1}{4}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{5}{12}, \frac{1}{2}, \frac{7}{10}\right\}.$$

Далее везде далее предполагаем, что $n \geq 4$. Оценим относительное влияние переменных τ для любой булевой функции.

Теорема 2. *Относительное влияние переменных любой булевой функции, существенно зависящей от n переменных, не превосходит $\frac{2^{n-1}-1}{2^{n-1}+n-2}$. Для функций, таких, что $k'_1 \neq 1$, относительное влияние меньше $\frac{2^{n-1}-1}{2^{n-1}+n-2}$.*

Определение 8 [5]. Пусть $p : \{-1, 1\}^n \to \mathbf{R}$ — линейный многочлен, $f = \text{sign}(p)$, тогда функция $f : \{-1, 1\}^n \to \{-1, 1\}$ называется пороговой.

Определение 9 [5]. Весом пороговой функции $f = sign(p(x))$, где $p = \sum_{i=1}^n a_i x_i - \theta$ называется величина $w(f) := \sum_{i=1}^n a_i^2 + \theta^2$.

Рассмотрим функции, такие, что $k'_1 = 1$. Все они являются пороговыми. Так как для любой пороговой функции f существует эквивалентная ей монотонная пороговая функция [5], рассматриваемые функции эквивалентны функции вида: $x_1^\delta = x_1 + \delta_{\{-1\} \times \{1\}^{n-1}} + 1$. Обозначим класс таких функций через X_1^δ.

Теорема 3. *Функции из класса X_1^δ имеют вес равный n^2-n+1. Их количество равно $n2^{(n+1)}$.*

Из теорем 2 и 3 следует теорема 4.

Теорема 4. *Среди булевых функций, существенно зависящих от n переменных, равенство $\tau = \frac{2^{n-1}-1}{2^{n-1}+n-2}$ выполнено на функциях из X_1^δ и только на них.*

Автор выражает благодарность своему научному руководителю А. А. Ирматову за внимание к работе и полезные обсуждения.

Список литературы

1. J. Kahn, G. Kalai, N. Linial. The influence of variables on Boolean functions // Proceedings of the 29th Annual Symposium on Foundations of Computer Science (1988). — P. 68–80.

2. R. O'Donnell. Analysis of Boolean functions. — Cambridge: Cambridge University Press, 2014.

3. Ben-Or, N. Linial. Collective coin flipping // Randomness and computation. — 1990. — V. 5. — P. 91–115.

4. I. Diakonikolas, P. Harsha, A. Klivans, R. Meka, P. Raghavendra, R. Servedio, Li-Yang Tan. Bounding the average sensitivity and noise sensitivity of polynomial threshold functions // Proceedings of the 42nd ACM symposium on theory of computing (2010). — 2010. — P. 533–542.

5. S. Muroga. Threshold logic and its applications. — New York: Wiley-Interscience, 1971.

ОПРЕДЕЛЕНИЕ МАТРОИДА КАК ГЕОМЕТРИЧЕСКОЙ КОНФИГУРАЦИИ

А. В. Ильев (Омск), В. П. Ильев (Новосибирск)

Впервые определение конечного матроида было дано в 1935 г. Уитни [1]. В дальнейшем было предложено множество эквивалентных определений матроида (см., например, [2]). Большая часть этих определений относится к следующим двум группам.

Первая группа определений. Матроид определяется как булева решетка 2^U всех подмножеств непустого конечного множества U с выделенным семейством подмножеств.

К этой группе относится данное Уитни определение в терминах независимых множеств. В этом определении выделено непустое семейство $\mathcal{A} \subseteq 2^U$ *независимых множеств*, обладающее свойствами:

$(A1)$ если $A \in \mathcal{A},\ B \subseteq A$, то $B \in \mathcal{A}$;

$(A2)$ для любых $A, B \in \mathcal{A}$ таких, что $|B| = |A| + 1$, существует элемент $b \in B \setminus A$, для которого $A \cup \{b\} \in \mathcal{A}$.

Обозначается матроид обычно как $M = (U, \mathcal{A})$.

Обыкновенный матроид — это пара $M = (U, \mathcal{A})$, где U — непустое конечное множество, $\mathcal{A}$ — непустое семейство его независимых подмножеств, обладающее свойствами $(A1)$, $(A2)$, а также свойствами:

$(A3)$ для любого $u \in U$ выполнено $\{u\} \in \mathcal{A}$;

$(A4)$ для любых $u, v \in U$, если $u \neq v$, то $\{u, v\} \in \mathcal{A}$.

К первой группе относятся также хорошо известные определения матроида в терминах баз, циклов и другие.

Вторая группа определений. Матроид определяется как булева решетка 2^U всех подмножеств непустого конечного множества U с заданным на 2^U отображением.

Наиболее известными определениями второй группы являются определение в терминах ранговой функции и следующее определение в терминах оператора замыкания.

Матроид — это пара $M = (U, \varphi)$, где U — непустое конечное множество, φ — отображение булевой решетки 2^U всех подмножеств множества U в себя, которое ставит в соответствие любому множеству $X \subseteq U$ его замыкание $\overline{X}$ и обладает следующими свойствами:

$(\varphi 1)$ $X \subseteq \overline{X}$ для любого $X \subseteq U$;

$(\varphi 2)$ для любых $X, Y \subseteq U$ если $X \subseteq Y$, то $\overline{X} \subseteq \overline{Y}$;

$(\varphi 3)$ $\overline{\overline{X}} = \overline{X}$ для любого $X \subseteq U$;

$(\varphi 4)$ для любых элементов $u, v \in U$ и любого подмножества $X \subseteq U$ если $u \notin \overline{X}$ и $u \in \overline{X \cup \{v\}}$, то $v \in \overline{X \cup \{u\}}$

Матроид $M = (U, \varphi)$ называется *обыкновенным*, если он, кроме того, обладает свойством $(\varphi 5)$:

$(\varphi 5)$ $\overline{\emptyset} = \emptyset$ и $\overline{\{u\}} = \{u\}$ для любого $u \in U$.

Определение в терминах оператора замыкания часто принимают в качестве определения *комбинаторной геометрии*, отождествляя комбинаторные геометрии и обыкновенные матроиды [3, 4]. Если в этом определении отказаться от условия $(\varphi 5)$, то мы получаем определение *комбинаторной предгеометрии*. Таким образом, комбинаторная предгеометрия и матроид — это один и тот же объект.

Весьма естественно выглядело бы определение комбинаторной геометрии как геометрической конфигурации, т. е. системы поверхностей различного ранга, удовлетворяющих заданным аксиомам инцидентности. Хотя изучению вопросов, связанных с комбинаторны-

ми геометриями, посвящена обширная литература (см., например, [3–7]), нам нигде не удалось найти общего геометрического определения комбинаторной предгеометрии (геометрии), которое было бы эквивалентно определению матроида (обыкновенного матроида).

Мы предлагаем геометрическое определение комбинаторной предгеометрии, эквивалентное определению конечного матроида. Дано также аналогичное определение комбинаторной геометрии.

Комбинаторная предгеометрия — это пара $(U, \mathcal{F})$, где U — непустое конечное множество *точек*, $\mathcal{F}$ — семейство его подмножеств — *поверхностей*, каждой из которых приписан *ранг* $k \in Z_+$, обладающих следующими свойствами:

$(G1)$ поверхность ранга 0 существует;

$(G2)$ никакая поверхность ранга k не лежит в поверхности ранга $k-1$;

$(G3)$ всякая поверхность ранга k и точка, не лежащая на ней, лежат в единственной поверхности ранга $k+1$;

$(G4)$ любые k точек, не лежащие ни в какой поверхности ранга, меньшего k, лежат в единственной поверхности ранга k.

Комбинаторная геометрия — это комбинаторная предгеометрия, для которой выполнено свойство $(G5)$:

$(G5)$ $\emptyset$ и все точки являются поверхностями.

Несложно проверить, что система аксиом $(G1)$–$(G5)$ независима, т. е. любая из них не является следствием остальных аксиом.

Эквивалентность приведенного определения определению обыкновенного матроида вытекает из следующей теоремы.

Теорема. 1) *Пусть* $M = (U, \mathcal{A})$ *— обыкновенный матроид, где* U *– непустое конечное множество его элементов,* $\mathcal{A}$ *— семейство его независимых множеств. Тогда семейство* $\mathcal{F}$*, определенное по правилу*

$$\mathcal{F} = \{F \subseteq U \mid \exists A \in \mathcal{A}\ (F = A \cup \{u \in U \mid A \cup \{u\} \notin \mathcal{A}\})\ \}, \quad (1)$$

обладает свойствами $(G1)$–$(G5)$*, причем имеет место равенство*

$$\mathcal{A} = \{A \subseteq U \mid \forall F \in \mathcal{F}\ (r(F) < |A| \to A \not\subseteq F)\}. \quad (2)$$

2) *Пусть* $(U, \mathcal{F})$ *— комбинаторная геометрия, где* U *— непустое конечное множество точек, а* $\mathcal{F}$ *— семейство ее поверхностей. Тогда семейство* $\mathcal{A}$*, определенное по правилу* (2)*, обладает свойствами* $(A1)$–$(A4)$*, причем имеет место равенство* (1).

Доказана также эквивалентность предложенного нами определения комбинаторной предгеометрии и определения матроида общего вида.

Работа первого автора выполнена при поддержке Программы фундаментальных научных исследований государственных академий наук на 2013-2020 годы, п.I.1.1.3. «Теоретико-модельные и алгебро-геометрические свойства алгебраических систем».

Работа второго автора выполнена при финансовой поддержке РНФ (проект 15-11-10009).

Список литературы

1. Whitney H. On the abstract properties of linear dependence // American Journal of Mathematics. — 1935. — V. 57. — P. 509–533.

2. Welsh D. J. A. Matroid theory. — London: Academic Press, 1976.

3. Айгнер М. Комбинаторная теория. — М.: Мир, 1982.

4. Crapo H. H., Rota G.-C. On the foundations of combinatorial theory. II. Combinatorial geometries. — Cambridge: MIT Press, 1970.

5. Lint J. H. van, Wilson R. M. A course in combinatorics. — New York: Cambridge University Press, 2001.

6. Mason J. H. Matroids as the study of geometrical configurations // Higher combinatorics, ed. by M. Aigner. — Dordrecht: Reidel Publishing Company, 1977. — P. 133–176.

7. White N., ed. Combinatorial geometries. Encyclopedia of mathematics and its applications. V. 29. — Cambridge: Cambridge University Press, 1987.

НЕКОТОРЫЕ ЗАДАЧИ НА МАТРОИДАХ

А. Н. Исаченко (Минск), А. М. Ревякин (Москва)

Определения из теории матроидов можно найти в [1–3].

Наиболее известные оптимизационные задачи на матроидах — задача поиска базы минимального или максимального веса и задача поиска независимого множества максимального или минимального веса на пересечении двух матроидов. Для их решения применяется «жадный» алгоритм и алгоритм поиска решения на пересечении двух матроидов соответственно [1].

В настоящей статье рассматривается задача поиска гамильтонова цикла матроида минимального веса. Напомним, что цикл матроида $M = (S, \Sigma)$, имеющего ранг k, называется гамильтоновым, если он содержит $k + 1$ элемент. Некоторые свойства гамильтоновых циклов приведены в работах [4–7].

Итак, пусть дан матроид $M = (S, \Sigma)$ ранга k без петель с заданными весами элементов $w(e) \geq 0$, $e \in S$. Считаем, что матроид

определён семейством циклов Σ. То есть Σ является семейством подмножеств из 2^S, удовлетворяющее следующим двум условиям:

C1) если $C_1 \neq C_2$, $C_1, C_2 \in \Sigma$, то $C_1 \not\subset C_2$;

C2) если $C_1, C_2 \in \Sigma$ и $z \in C_1 \cap C_2$, то существует $C_3 \in \Sigma$, такое что $C_3 \subseteq (C_1 \cup C_2) \backslash z$.

Ниже используются следующие обозначения: $\mathrm{list}(I)$ — упорядоченный список элементов множества I, $\mathrm{first}(\mathrm{list}(I))$ первый элемент этого списка; $\sigma(I)$ — замыкание множества I в матроиде $M = (S, \Sigma)$, то есть множество элементов из S, включая элементы I, добавление которых к I не изменяет ранг.

Для решения задачи рассмотрим следующий алгоритм.

Первый шаг.

1. Упорядочиваем элементы матроида по неубыванию их весов. Пусть $w(e_1) \leq w(e_2) \leq \cdots \leq w(e_n)$.

2. $I_0 = \emptyset$, $\mathrm{list}(I_0) = S$, $\mathrm{Fam} = \{I_0\}$.

3. Пересчитываем веса элементов $w(e_i) := w(e_i) - w(e_1)$. Полагаем оценку $\xi(I_0)$ множества I_0 и текущий рекорд f^* равными $w(e_1)$.

4. Полагаем $I_1 = \{e_1\}$, $I_2 = \emptyset$, $\mathrm{list}(I_1) := \mathrm{list}(I_0) - \sigma(e_1)$, $\mathrm{list}(I_2) := \mathrm{list}(I_2) - \{e_1\}$.

5. Преобразуем веса элементов из $\mathrm{list}(I_1)$ и $\mathrm{list}(I_2)$ по формуле $w(e) := w(e) - w(\mathrm{first}(\mathrm{list}(I_j)))$, $e \in \mathrm{list}(I_j)$, $j = 1, 2$. Оценки множеств $\xi(I_j) = \xi(I_0) + w(\mathrm{first}(\mathrm{list}(I_j)))$, $j = 1, 2$.

6. Полагаем $\mathrm{Fam} = \{I_1, I_2\}$.

Общий шаг.

1. Среди множеств семейства Fam находим множество I_p с минимальной оценкой. Если таких множеств несколько, берём любое из тех, которые имеют максимальное число элементов. Полагаем рекорд f^* равным $\xi(I_p)$.

2. Если $|I_p| = k$, то есть I_p — база матроида, идём к пункту 5. Если $|I_p| = k + 1$, то I_p искомый гамильтонов цикл. Завершаем работу.

3. Полагаем множества $I_p^1 = I_p \cup \{\mathrm{first}(\mathrm{list}(I_p))\}$, $I_p^2 = I_p$, списки $\mathrm{list}(I_p^1) = \mathrm{list}(I_p) - \sigma(I_p^1)$, $\mathrm{list}(I_p^2) = \mathrm{list}(I_p) - \mathrm{first}(\mathrm{list}(I_p))$, оценки $\xi(I_p^j) = \xi(I_p) + w(\mathrm{first}(\mathrm{list}(I_p^j)))$, $j = 1, 2$.

4. Полагаем $\mathrm{Fam} := (\mathrm{Fam} \setminus \{I_p\}) \cup \{I_p^1, I_p^2\}$. Перенумеровываем множества Fam от 1 до $|\mathrm{Fam}|$. Возвращаемся к пункту 1 общего шага.

5. Добавляя к I_p по одному элементу из $S \backslash I_p$ в порядке неубывания их весов, находим первый элемент e_l из них, для которого $I_p \cup e_l$ является циклом. Полагаем $I_p := I_p \cup e_l$, $\xi(I_p^j) = \xi(I_p) + w(e_l)$ и идём к пункту 1 общего шага.

Нетрудно видеть, что данный алгоритм является реализацией метода ветвей и границ, аналогичной алгоритму Литтла для задачи коммивояжёра. Прямой перенос вариантов алгоритма Литтла невозможен в силу отсутствия у матроидов отношения инцидентности элементов, которое применяется в задаче коммивояжёра на графе для формулирования правила ветвления и пересчета оценок.

Для матроидов правила ветвления принимают самый общий вид, состоящий в выборе на каждой итерации для включения в гамильтонов цикл любого элемента с минимальным весом. Процедура приведения весов заключается в уменьшении всех весов на величину минимального из весов, что приводит к появлению элементов e с $w(e) = 0$. При включении элемента в текущее решение, для соответствующей ветви дерева поиска решения исключаются все элементы, приводящие к образованию циклов с уже имеющимся независимым множеством.

Список литературы

1. Welsh D. J. A. Matroid theory. — London: Acad. Press, 1976.
2. Айгнер М. Комбинаторная теория. — Москва: Мир, 1982.
3. Ревякин А. М., Исаченко А. Н. Криптоморфные системы аксиом, линейная и алгебраическая представимость матроидов // Сборник научных трудов МИЭТ. Посвящается 70-летию профессора А. С. Поспелова. — М.: МИЭТ, 2016. — С. 99–109.
4. Исаченко А. Н., Исаченко Я. А. Периметр матроида и задача коммивояжёра для матроидов // XI Белорусская математическая конференция. Тез. докл. Междунар. науч. конф., Минск, 5–9 ноября 2012 г. — Ч. 4. — Минск: Институт математики НАН Беларуси, 2012. — С. 87–88.
5. Исаченко А. Н., Исаченко Я. А. Свойства гамильтоновых матроидов // Международный конгресс по информатике: информационные системы и технологии. Материалы меджунар. науч. конгресса, Республика Беларусь, Минск, 4–7 нояб. 2013 г. — Минск: БГУ, 2013. — С. 538–541.
6. Исаченко А. Н., Исаченко Я. А. Циклический граф гамильтонова матроида // Дискретная математика, алгебра и их приложения: Тез. докл. Междунар. науч. конф. Минск, 14–18 сентября 2015 г. — Минск: Институт математики НАН Беларуси, 2015. — С. 108–109.
7. Исаченко А. Н., Исаченко Я. А. О некоторых характеризациях матроидов и свойствах гамильтоновых матроидов // Современные информационные технологии и ИТ-образование. — 2015. — Т. 2 (№ 11). — С. 214–219.

ОПТИМАЛЬНАЯ СТРАТЕГИЯ ВЫБОРА ПЕРЕМЕННОЙ ВЕТВЛЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ О СУММЕ ПОДМНОЖЕСТВ МЕТОДОМ ВЕТВЕЙ И ГРАНИЦ

Р. М. Колпаков, М. А. Посыпкин (Москва)

Рассматривается оптимизационная задача о сумме подмножеств, которая может быть сформулирована следующим образом:

$$\begin{array}{l} \text{maximize } f(\tilde{x}) = \sum_{i\in N} x_i w_i, \\ \text{subject to } f(\tilde{x}) = \sum_{i\in N} x_i w_i \le C, \\ x_i \in \{0,1\}, i \in N, \end{array} \tag{1}$$

где $N = \{1, 2, \ldots, n\}$, $C > 0$ и $w_i > 0$ для $i \in N$. Задача о сумме подмножеств является частным случаем задачи о ранце с одним ограничением [1, 2], в котором веса и стоимости предметов совпадают.

Пусть $I \subseteq N$ и пусть θ — некоторое отображение из I в $\{0, 1\}$. Тогда пара (I, θ) однозначным образом определяет следующую оптимизационную подзадачу P задачи (1):

$$\begin{array}{l} \text{maximize } f(x) = \sum_{i\in N} w_i x_i, \\ \text{subject to } f(x) = \sum_{i\in N} w_i x_i \le C, \\ x_i = \theta(i), i \in I, \\ x_i \in \{0,1\}, i \in N \setminus I. \end{array}$$

Переменные x_i для $i \in I$ называются *фиксированными переменными* подзадачи P, а переменные x_i для $i \in N \setminus I$ называются *свободными переменными* этой подзадачи. Элементы пары (I, θ), определяющей подзадачу P, будем обозначать через $I(P)$ и θ_P. Положим также

$$I_0(P) = \{i \in I(P) : \theta_P(i) = 0\}, \quad I_1(P) = \{i \in I(P) : \theta_P(i) = 1\}.$$

Пусть $W = \sum_{i\in N} w_i$. Будем говорить, что для подзадачи P выполнено *условие отрицательного отсева* **C0**, если $\sum_{i\in I(P)} \theta_P(i) w_i > C$. Очевидно, что подзадача, удовлетворяющая условию **C0**, не имеет решений. Будем говорить, что для подзадачи P выполнено *условие положительного отсева* **C1**, если $\sum_{i\in I(P)} (1-\theta_P(i)) w_i \ge W - C$. Очевидно, что подзадача, удовлетворяющая условию **C1**, имеет единственное оптимальное решение. Пусть подзадача P не удовлетворяет ни одному из условий **C0** и **C1**, x_j — некоторая свободная переменная подзадачи P. Тогда подзадачу P можно разбить на две

подзадачи P_0 и P_1, получаемые из P присваиванием переменной x_j значений 0 и 1 соответственно. Процедуру получения подзадач P_0 и P_1 из подзадачи P будем называть *декомпозицией* подзадачи P по переменной x_j. Переменная x_j называется *переменной ветвления* для подзадачи P.

Рассматривается классический метод ветвей и границ (МВГ) для решения задачи о сумме подмножеств, который состоит в последовательном выполнении итераций следующего цикла (в процессе выполнения данной процедуры поддерживаются список подзадач, подлежащих дальнейшему рассмотрению, и текущее рекордное решение задачи).

1. В список подзадач помещается исходная задача (1).

2. Если список подзадач пуст, то алгоритм завершает свою работу, в противном случае выбирается и удаляется из списка одна из подзадач (подзадача P).

3. Если подзадача P удовлетворяет условию **C0**, выполняется переход к шагу 2.

4. Если подзадача P удовлетворяет условию **C1**, вычисляется оптимальное решение z для данной подзадачи. Если значение целевой функции f на данном решении больше текущего рекорда, текущее рекордное решение заменяется на z. Затем выполняется переход к шагу 2.

5. Для подзадачи P выбирается переменная ветвления и призводится декомпозиция подзадачи P по данной переменной на две подзадачи, которые добавляются в список подзадач. Затем выполняется переход к шагу 2.

Сложностью решения задачи о сумме подмножеств МВГ называется число итераций цикла 2–5, выполняемых при решении задачи данным методом. Очевидно, что данная сложность равна числу подзадач (включая исходную задачу), рассмотренных в процессе решения задачи МВГ.

Пусть G — задача вида (1). Под процедурой выбора переменной ветвления для решения этой задачи МВГ будем понимать произвольное отображение φ, которое ставит в соответствие каждой паре (I, θ), где $I \subset N$ и θ — отображение из I в $\{0, 1\}$, некоторое число $\varphi(I, \theta)$ из $N \setminus I$. Под сложностью решения задачи G МВГ с процедурой φ выбора переменной ветвления понимается сложность процедуры решения задачи G МВГ, при выполнении которой на шаге 5 алгоритма в качестве переменной ветвления для декомпозиции подзадачи P выбирается переменная с номером $\varphi(I(P), \theta_P)$. Процедуру выбора переменной ветвления для решения задачи G МВГ будем называть *оптимальной*, если сложность решения задачи G

МВГ с данной процедурой выбора переменной ветвления является минимальной возможной. В общем случае, под процедурой выбора переменной ветвления для МВГ будем понимать произвольное отображение Φ, которое ставит в соответствие каждой тройке (G, I, θ), где G — задача вида (1), $I \subset N$ и θ — отображение из I в $\{0, 1\}$, некоторое число $\Phi(G, I, \theta)$ из $N \setminus I$. Процедуру Φ выбора переменной ветвления для МВГ будем полагать оптимальной, если для любой задачи G вида (1) процедура $\varphi_G(I, \theta) = \Phi(G, I, \theta)$ решения задачи G МВГ является оптимальной. Далее будем без ограничения общности полагать, что для задачи (1) выполняется $w_1 \geq w_2 \geq \ldots \geq w_n$. Рассмотрим процедуру Φ^M выбора переменной ветвления для МВГ такую, что $\Phi^M(G, I, \theta) = \min\{i \mid i \in N \setminus I\}$, тем самым в качестве переменной ветвления для декомпозиции любой подзадачи задачи G данная процедура выбирает свободную переменную x_i с наибольшим значением w_i. Мы называем такую процедуру выбора переменной ветвления *мажоритарной*. В [3] показано, что мажоритарная процедура выбора переменной ветвления может быть более эффективной, чем общераспространенная процедура выбора дробной переменной в качестве переменной ветвления.

Теорема. *Мажоритарная процедура выбора переменной ветвления является оптимальной для решения задачи о сумме подмножеств.*

Работа выполнена при финансовой поддержке РФФИ (проект 15-07-03102).

Список литературы

1. Martello S., Toth P. Knapsack Problems. — John Wiley & Sons Ltd., 1990.

2. Kellerer H., Pfershy U., Pisinger D. Knapsack Problems. — Springer Verlag, 2004.

3. Колпаков Р. М., Посыпкин М. А. Асимптотическая оценка сложности метода ветвей и границ с ветвлением по дробной переменной для задачи о ранце // Дискретн. анализ и исслед. опер. — 2008. — Т. 15, № 1. — С. 58–81.

О СЛОВАХ, ИЗБЕГАЮЩИХ ПОВТОРЫ

Н. В. Котляров (Москва)

Данная статья посвящена некоторым вопросам, связанным с существованием периодических структур в словах из формальных языков. Наиболее простой и хорошо изученной периодической структурой являются квадраты, то есть фрагменты вида xx, где x — произвольное непустое слово. Слово, не содержащее квадратов, называется бесквадратным. Классическим результатом, связанным с квадратами, является работа Акселя Туэ [1], в которой установлено существование как угодно длинных бесквадратными слов над алфавитом из трех букв. С другой стороны, несложно проверить, что не существует бесквадратных слов над алфавитом из двух букв. Поэтому из результатов Туэ следует, что алфавит из трех букв является минимальным алфавитом, над которым существуют как угодно длинные бесквадратные слова. В дальнейшем было получено много различных альтернативных доказательств данного результата Туэ, одно из наиболее изящных доказательств представлено в [2]. Естественным обобщением результата Туэ является работа [3]. В нашей работе рассматривается случай, когда в словах допускаются достаточно "маленькие" квадраты. Подобное допущение рассматривается, например, в работе [4], где доказано существование бесконечного слова над алфавитом из двух букв, которое содержит только 3 различных коротких квадрата. Другие базовые результаты, касающиеся квадратов, получены в работах [5, 6].

Нетрудно заметить, что задача существования сколь угодно длинных слов, не содержащих фрагментов определенного типа, эквивалентна задаче существования бесконечных слов над тем же алфавитом, не содержащих данных фрагментов. Поэтому в работах, посвященных этой тематике, обычно рассматривается эквивалентная задача существования бесконечных слов.

Слово называется сильно бескубным, если оно не содержит фрагментов вида xxa, где x — непустое слово, a — первая буква слова x. Классическим результатом Акселя Туэ для сильно бескубных слов является работа [3], в которой было доказано существование сколь угодно длинных сильно бескубных слов над двухбуквенным алфавитом. В частности, в данной работе приведен пример бесконечного сильно бескубного слова над двухбуквенным алфавитом. Это слово называется в литературе последовательностью Туэ (Туэ—Морса).

Другим естественным обобщением задачи о существовании сколь угодно длинных бесквадратных слов является рассмотрение в качестве "запретных" фрагментов не только квадратов, но и квадратов

с Δ ошибками замещения, то есть фрагментов вида xy, где слово x отличается от слова y ровно на Δ букв. Отметим, что, например, любой фрагмент длины 2 является либо квадратом, либо квадратом с одной ошибкой замещения, поэтому для данной задачи естественно вводить ограничения снизу как на длины "запретных" квадратов, так и на длины "запретных" квадратов с ошибками замещения. По нашим сведениям данная задача еще не рассматривалась в научной литературе, за исключением предыдущих работ автора [7], где было показано существование над алфавитами различных мощностей сколь угодно длинных слов, не содержащих квадратов и квадратов с одной ошибкой, в зависимости от ограничений снизу на длину квадратов. В данной работе рассматривается следующая задача: можно ли построить над двухбуквенным алфавитом как угодно длинное слово, не содержащее квадратов и квадратов с несколькими ошибками при наличии ограничения на длины этих квадратов, и каким при этом должно быть это ограничение? В данной работе доказано, что существует бесконечное слово над алфавитом из двух букв, не содержащее квадратов с не более чем Δ ошибками таких, что их длина превосходит $4\Delta + 4$. Основной результат работы:

Теорема. *Для любого натурального Δ существует бесконечное слово над алфавитом из двух букв, у которого нет факторов, являющихся квадратами с не более Δ ошибками и периодом больше $2\Delta + 2$.*

При доказательстве данной теоремы строится отображение f_g из множества слов над алфавитом из двух букв в множество слов над алфавитом из двух букв по следующему правилу:

$$f_g(a_1a_2...a_{n-1}a_n) = g(a_1a_2)g(a_2a_3)...g(a_{n-1}a_n),$$

$$f_g(a_1a_2...) = g(a_1a_2)g(a_2a_3)...,$$

где g — отображение из слов двухбуквенного алфавита длины 2 в множество слов двухбуквенного алфавитом, которое подобрано так, что образ последовательности Туэ—Морса при отображении f_g обладал бы требуемыми свойствами. В работе представлен примеры такого отображения для всех возможных значений Δ.

Список литературы

1. Thue A. Uber unendliche Zeichenreihen // Norske, Vid. Selsk. Skr. I, Mat. Nat. Kl. Khristiana — 1906. — 7. — S. 1–22.

2. Саломаа А. Жемчужины теории формальных языков. — М.: Мир, 1986.

3. Thue A. Uber die gegenseitige Lage gleicher Teile gewisser Zeichenreihen // Norske, Vid. Selsk. Skr. I, Mat. Nat. Kl. Kristiania. —

1912. — 1. — S. 1–67.

4. Fraenkel A. S., Simpson R. J. How many squares must a binary sequence contain? // Electr. J. Comb. — 1995. — 2.

5. Crochemore M., Ilie L., Rytter. W. Repetitions in strings: algorithms and combinatorics // Theor. Comput. Sci. — 2009. — 410 (50). — P. 5227–5235.

6. Crochemore M., Rytter. W. Squares, cubes, and time-space efficient string searching // Algorithmica. — 1995. — 13 (5). — P. 405–425.

7. Котляров Н. В. О существовании сколь угодно длинных слов, не содержащих квадратов с одной возможной ошибкой замещения // Дискретная математика. — 2015. — Т. 27, вып. 2. — С. 56–72.

ДИСТРИБУТИВНЫЕ ВЕКТОРНЫЕ ПРОСТРАНСТВА НАД РЕШЕТКАМИ И ИХ СВОЙСТВА

Е. Е. Маренич, В. Е. Маренич (Москва)

В работах [1–3] определены векторные пространства над решетками и рассмотрены их свойства. В работах [4, 5] доказан критерий дистрибутивности пространства над двухэлементной решеткой и доказан критерий регулярности булевых матриц конечного (или бесконечного размера) над двухэлементной решеткой. В работе [1] доказан критерий дистрибутивности пространства над двухэлементной решеткой, использующий идентификаторы.

Предварительные сведения. Пусть $(L, \wedge, \vee, \leq)$ — решетка с частичным порядком $\leq$ и решеточными операциями $\vee$ и $\wedge$. Обозначим: $\widetilde{0}$ и $\widetilde{1}$ — наименьший и наибольший элементы решетки; $join(L)$ — множество всех $\vee$-неразложимых элементов решетки L; множество $J(L) = join(L) \setminus \{\widetilde{0}\}$.

Пусть $L^{m\times n}$ — множество всех (решеточных) $m \times n$ матриц. В работе рассматриваются матрицы (и пространства) только над дистрибутивными решетками с $\widetilde{0}$ и $\widetilde{1}$, где $\widetilde{0} \neq \widetilde{1}$. Операции сложения и умножения матриц над решеткой L задаются как обычно: вместо сложения используется операция $\vee$, а вместо умножения – $\wedge$.

Пусть элемент $\lambda \in P$, матрицы $A = (a_{ij})$, $C = (c_{ij}) \in P^{m\times n}$. Будем писать $C = \lambda A$, если $c_{ij} = \lambda \wedge a_{ij}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Матрица $A \in L^{m\times n}$ называется регулярной, если существует матрица $X \in L^{n\times m}$ такая, что $AXA = A$.

Векторным пространством, порожденным множеством векторов $U = \{u_1, u_2, \ldots, u_n\} \subseteq L^{m\times 1}$, называется множество
$Lin(U) = \{\lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n |\ \lambda_1, \lambda_2, \ldots, \lambda_n \in L\}$.

Столбцовое пространство матрицы $A \in L^{m\times n}$ – это пространство $Column_L(A) = Lin(A^{(1)}, A^{(2)}, \ldots, A^{(n)})$, где $A^{(i)}$ — i-й столбец A.

1. *Векторные пространства как решетки.* Пусть L — решетка, $V = Lin_L(U) \subseteq L^{m\times 1}$, где U — множество векторов $\{u_1, u_2, \ldots, u_n\} \subseteq L^{m\times 1}$.

Арифметическое пространство $L^{m\times 1}$ является дистрибутивной решеткой с решеточными операциями $\vee$ и $\wedge$. Пространство V — полурешетка относительно операции $\vee$. Если для любого множества $S \subseteq V$ существует $\vee S$, то V — полная решетка, [6]. В частности, конечные пространства V являются решетками.

Обозначим $\vee$ и $\widetilde{\wedge}$ решеточные операции в решетке V. Для любых векторов $u, v \in V$ справедливы неравенства $u \,\widetilde{\wedge}\, v \leq u \wedge v$. Если для векторов $u, v \in V$ существует наибольшее $\mu \in L$ такое, что $\mu u \leq v$, то обозначим его через $\langle v/u\rangle_V$. Определение и свойства брауэровых решеток даны [6]. Если L — брауэрова решетка, то для любых векторов $u, v \in V$ существует $\langle v/u\rangle_V$.

Теорема 1.1. *Пусть L — брауэрова решетка. Тогда пространство V — решетка и для любых векторов $v, w \in V$*

$$v\widetilde{\wedge}w = \sum_{r=1}^{n} \left(\langle v/u_r\rangle_V \wedge \langle w/u_r\rangle_V\right) u_r.$$

Теорема 1.2. *Пусть L — цепь с единицей $\widetilde{1}$. Тогда для любых векторов $v, w \in V$ и любого $\lambda \in P$ справедливы равенства:*

$$\lambda(u\widetilde{\wedge}v) = (\lambda u)\widetilde{\wedge}v = u\widetilde{\wedge}(\lambda v) = (\lambda u)\widetilde{\wedge}(\lambda v).$$

Теорема 1.3. *Пусть L — полная брауэрова решетка. Тогда V — полная решетка.*

2. *Дистрибутивность ретрактов.* Пусть L — решетка, матрица $B \in L^{m\times m}$, пространство $V = Column_L(B)$. Матрица B называется идемпотентом, если $B = B^2$. Пространство V называется ретрактом, если $V = Column_L(B)$ для некоторого идемпотента B.

Теорема 2.1. *Пусть матрица B — идемпотент. Тогда V — решетка и $u\widetilde{\wedge}v = B(u \wedge v)$ для любых векторов $u, v \in V$.*

Для брауэровых решеток теорема 2.1 доказана в работе [7].

Следствие 2.1. *Каждый ретракт — дистрибутивное пространство.*

Следствие 2.2. *Пусть пространство V — ретракт. Тогда для любых векторов $u, v \in V$ и для любых $\lambda \in L$ справедливы равенства* $\lambda(u\widetilde{\wedge}v) = (\lambda u)\widetilde{\wedge}v = u\widetilde{\wedge}(\lambda v) = (\lambda u)\widetilde{\wedge}(\lambda v)$.

3. *Идентификаторы.* Пусть P — конечная дистрибутивная решетка, пространство $V \subseteq P^{m\times 1}$. Вектор $id(w) \in P^{m\times 1}$ называется идентификатором вектора $w \in J(V)$, если $id(w)$ есть $\vee$-неразложимый вектор решетки $P^{m\times 1}$ такой, что

$$id(w) \le w, \quad id(w) \not\le \sum_{j\in J(V), w\not\le z} z.$$

Каждый идентификатор $id(w)$ имеет только одну ненулевую компоненту, которая является $\vee$-неразложимым элементом решетки P.

Теорема 3.1. *Пространство V дистрибутивно тогда и только тогда, когда V — пространство с идентификаторами.*

Для решетки $P = \{\widetilde{0}, \widetilde{1}\}$ теорема 3.1 доказана в [1].

4. *Дистрибутивные пространства над цепями.* Пусть P — конечная цепь, пространство $V \subseteq P^{m\times 1}$.

Теорема 4.1. *Пространство V дистрибутивно тогда и только тогда, когда для любого вектора $w \in J(V)$*

$$w \not\le \sum_{j\in J(V), w\not\le z} z.$$

5. *Дистрибутивность пространств над нечеткой решеткой.* Нечеткой решеткой называется решетка $L = ([0;1], \vee, \wedge, \le)$, где $[0;1]$ - числовой интервал, $\le$ — обычный ЧП на числовом множестве и для любых $a, b \in [0;1]$: $a \vee b = \max\{a, b\}$, $a \wedge b = \min\{a, b\}$.

Пусть матрица $A \in L^{m\times n}$, пространство $V = Column_L(A)$. Обозначим $Set(A)$ — множество всех элементов матрицы A.

Теорема 5.1. *Пусть P — множество и $\{1\} \cup Set(A) \subseteq P \subseteq [0;1]$. Тогда решетка $U = Column_P(A)$ — подрешетка решетки V.*

Следствие 5.1. *Следующие утверждения равносильны.*

1. *Пространство V дистрибутивно (модулярно).*
2. *Для любого множества P, такого что $\{1\} \cup Set(A) \subseteq P \subseteq [0;1]$, пространство $U = Column_P(A)$ дистрибутивно (модулярно).*

Следствие 5.2. *Пусть матрица $A \in \{\widetilde{0}, \widetilde{1}\}^{m\times n}$. Если пространство $Column_{\{\widetilde{0},\widetilde{1}\}}(A)$ не дистрибутивно (не модулярно), то и пространство $Column_L(A)$ не дистрибутивно (не модулярно).*

Список литературы

1. Kim K. Boolean matrix theory and applications — New York: Marcel Dekker, 1982.

2. Kim K. and Roush F. Generalized fuzzy matrices // Fuzzy Sets Systems. — 1980. — 4. — P. 293–315.

3. Маренич Е. Е., Маренич В. Е. Базисы и размерность векторных пространств над решётками // Фундамент. и прикл. матем. — 2014. — 19:2. — С. 151–169.

4. Зарецкий К. А. Регулярные элементы полугруппы бинарных отношений // Успехи мат. наук. — 1962. — Т. XVII, вып. 3. — С. 177–179.

5. Зарецкий К. А. Полугруппа бинарных отношений // Математический сборник. — 1963. — 61 (103). — С.291–305.

6. Биркгоф Г. Теория решёток. — М.: Наука, 1984.

7. Marenich V. E. Lattices of matrix rows and matrix columns. Lattices of invariant column eigenvectors // Matrix methods: Theory, Algorithms and Applications — 2010. — P. 104–116.

ДИСКРЕТНЫЕ ВЕРСИИ ТЕОРЕМ О НЕПОДВИЖНЫХ ТОЧКАХ

О. Р. Мусин (Москва)

Лемма Шпернера о раскраске вершин триангуляции, доказанная в 1928 году, является дискретным аналогом теоремы Брауэра о неподвижной точке. У леммы большое число приложений. В частности, эта лемма и ее обобщения играют важную роль в теории игр и математической экономике.

Дискретными версиями теоремы Борсука—Улама являются леммы Таккера, Ки Фана и Шашкина. У этих лемм тоже имеются многочисленные приложения.

В наших работах [1–7] получено большое число обобщений классических теорем о неподвижных точках и их дискретных аналогов. Рассмотрим здесь некоторые из них.

Лемма Шпернера утверждает, что *при любой Шпернеровской раскраске вершин триангуляции n-мерного симплекса в $n+1$ цветов найдется ячейка триангуляции, вершины которой покрашены во все цвета.* В работе [3] мы показываем, что вместо симплекса можно взять произвольное многообразие с краем. Более того, на многообразия можно обощить и так называемую “лемму Шпернера для многогранников.”

В этой же работе мы показываем, что леммы Таккера и Фана тоже могут быть обобщены для симплициальных многообразий. В

работе [1] рассматривается класс многообразий со свободным действием инволяции для которых верна теорема Борсука—Улама. (Мы назвали этот класс БУТ.) В [3] доказано, что если многообразие принадлежит этому классу, то для него верны леммы Таккера и Фана. Большая часть этих результатов может быть обобщена для БУТ-пространств, которые рассматриваются в работе [7].

Оказывается, что не обязательно рассматривать триангуляции. Мы показали, см. [2], что вместо триангуляций можно рассматривать "квадрангуляции", то есть разбиения многообразия с краем на параллелипипеды.

В 1990-х годах уральский математик Ю. А. Шашкин опубликовал несколько работ по теме данной статьи. В частности, в 1996 году он опубликовал работу в которой нашел дискретный аналог теоремы о нечетном отображении сфер. Эта работа была опубликована только на русском и в ней рассматривался только двумерный случай, т.е. триангуляция многоугольника. Более того, Ю. А. Шашкин приписал этот результат Ки Фану. Лемма Шашкина действительно может быть выведена из леммы Фана, однако, этот результат новый, а доказательство Шашкина оригинальное.

В работе [4] мы рассматриваем обобщения леммы Шашкина. Сначала доказывается, что вместо сфер в теореме о нечетном отображении могут быть любые БУТ-многообразия. Это позволяет получить лемму Шашкина для триангуляций многообразий из класса БУТ.

В недавней работе [5] мы рассмотрели обобщения леммы Шпернера без предположении, что раскрасска на границе является Шпернеровской, а число цветов m может быть и меньше чем $n+1$. По раскраске на границе мы определи инвариант μ, который равен 1 при Шпернеровской раскраске. Основной результат:
Если $\mu \neq 0$, то верна лемма Шпернера, т.е. найдется симплекс триангуляции, вершины которого покрашены во все m цветов.

Заметим, что если $m = n+1$, то инвариант μ является степенью отображения, а при $m = n$ это инвариант Хопфа. В работе [6] рассматриваются дальнейшие приложения инварианта μ к леммам Шпернера и Кнастера—Куратовского—Мазуркевича (KKM), а также к их "цветным" обобщениям.

Работа выполнена при поддержке гранта NSF DMS–1400876 и гранта РФФИ 15-01-99563

Список литературы

1. Musin O. R. Borsuk–Ulam type theorems for manifolds // Proc. Amer. Math. Soc. — 2012. — 140. — P. 2551–2560.

2. Musin O. R. Sperner type lemma for quadrangulations // Mosc. J. of Combin. and Number Theory. — 2015. — 5 (1). — P. 26–35.

3. Musin O. R. Extensions of Sperner and Tucker's lemma for manifolds // J. of Combin. Theory Ser. A. — 2015. — 132. — P. 172–187.
4. Musin O. R. Generalizations of Tucker–Fan–Shashkin lemmas // arXiv: 1409.8637.
5. Musin O. R. Homotopy invariants of covers and KKM type lemmas // arXiv:1505.07629.
6. Musin O. R. KKM type theorems with boundary conditions, arXiv:1512.04612
7. Musin O. R., Volovikov A. Yu. Borsuk–Ulam type spaces // Mosc. Math. J. — 2015. — 15 (4) — P. 749–766.

ВОКРУГ ЛЕММЫ ОБ ИЗОЛИРОВАНИИ

А. О. Останин, А. Б. Дайняк (Москва)

Пусть A — некоторое n-элементное множество, F — семейство подмножеств A. Пусть для каждого элемента $x \in A$ его вес $w(x)$ выбирается случайно из множества $\{1, 2, \ldots, m\}$, а вес элемента $E \in F$ определяется как $\sum\limits_{x \in E} w(x)$. Если ровно один элемент F имеет минимальный вес, то весовая функция w называется *изолирующей* для семейства F. Лемма об изолировании утверждает, что при таких условиях вероятность того, что w — изолирующая функция, не меньше $(1 - \frac{1}{m})^n$.

В данной работе мы рассматриваем некоторые вопросы, касающиеся уточнения леммы, получения достижимых оценок вероятности единственности множества с минимальным весом и поиска оптимальных конструкций.

Теорема [точная лемма об изолировании для одноэлементных подмножеств]. *Пусть F — система одноэлементных множеств на n-элементном множестве. Тогда вероятность того, что функция w изолирующая, не меньше*

$$\frac{n \cdot \sum\limits_{x=1}^{m-1} x^{n-1}}{m^n}.$$

Эта оценка достигается тогда и только тогда, когда F содержит все n одноэлементных подмножеств.

Доказательство проводится индукцией по n.

Пусть теперь размер множеств в F ограничен снизу некоторым натуральным числом l. Покажем, как получать примеры для таких систем, используя примеры для систем одноэлементных множеств.

Назовем $(n_1, n_2, \ldots, n_l)$-полной системой систему множеств F на $n = n_1 + n_2 + \ldots n_l$ элементах такую, что $V(G) = \cup_{i=1}^{l} V_i$, где $|V_i| = n_i$, и множества в F получаются взятием из каждого V_i по одному элементу. Нетрудно видеть, что в этом случае F будет содержать $n_1 \cdot n_2 \cdot \ldots \cdot n_l$ множеств. Если $n_i \geq 2$ для любого i, то для такой системы вероятность единственности минимального множества равна $\prod_{i=1}^{l} \alpha(n_i)$, где $\alpha(n_i)$ — вероятность единственности минимума для системы из n_i одноэлементных множеств. Поскольку при фиксированном n количество весовых функций одно и то же, мы будем минимизировать количество тех из них, при которых минимум единственнен.

Теорема [асимптотическая оптимальность $(2, n-2)$-полной системы для $l = 2$]. *Для любого натурального n существует натуральное M такое, что при любом $m > M$ количество изолирующих весовых функций для $(2, n-2)$-полной системы меньше, чем количество хороших расстановок для $(x, n-x)$-полной системы при любом $x \in [3; n-3] \cup \{1, n-1\}$.*

Заметим, что для $(2, 2, 2, \ldots, 2)$-полной системы вероятность изолирующей функции ровна $(\frac{m-1}{m})^{\frac{n}{2}}$, что равняется квадратному корню из оценки Та-Шма. Однако, из предыдущей теоремы следует, что такая система не является оптимальной в своем классе, то есть при больших m можно получить меньшую вероятность единственности минимума.

Компьютерный перебор для небольших значений n, m ($n \leq 7, m \leq 5$) позволяет выдвинуть следующую гипотезу.

Гипотеза. *Для систем F множеств на n элементах, составленных из l-элементных подмножеств ($n \geq 2l$), минимум вероятности изолирующей весовой функции достигается на $(2, 2, \ldots, 2, n-2(l-1))$-полной системе.*

Мы доказали эту гипотезу при $l = 2, m = 2$. В таком случае F удобно рассматривать как множество ребер графа на n вершинах. Для проверки гипотезы нужно доказать, что в любом графе на n вершинах количество весовых функций на вершинах, для которых минимальное ребро единственно, не меньше чем $2(n-2)$.

Теорема [точная лемма об изолировании для $m = 2$ и систем двухэлементных подмножеств]. *Количество изолирующих весовых*

функций на вершинах в любом графе на n вершинах не меньше чем $2(n-2)$.

Опишем идею доказательства.

Лемма. *Если в графе m ребер, то количество изолирующих функций не меньше m.*

Если граф полный, то изолирующих функций не меньше чем $\frac{n(n-1)}{2}$.

В противном случае выберем вершины u, v, не соединенные ребром так, чтобы максимизировать $|N(u) \cup N(v)|$. Пусть $A = N(u) \setminus N(v), B = N(u) \cap N(v), C = N(v) \setminus N(u)$, $a = |A|, b = |B|, c = |C|$. В зависимости от размера множества $|A \cup B \cup C|$ возникает несколько случаев, в каждом из которых можно предъявить $2(n-2)$ изолирующих функций.

Приведем также утверждение, согласно которому оценка вероятности в теореме Та-Шма скорее всего недостижима.

Теорема. *Пусть* $m \geq 3$. *Тогда количество изолирующих весовых функций не меньше чем* $(m-1)^n + \frac{a_1}{2}$, *где* a_1 *— количество изолирующих весовых функций, отображающих хотя бы один элемент в единицу.*

Доказательство теоремы состоит в чуть более подробном анализе конструкции Та-Шма.

Список литературы

1. Jukna S. Extremal combinatorics: with applications in computer science. — Springer, 2001.

2. Ta-Shma N. A simple proof of the Isolation Lemma. — 2015.

3. Mulmuley K., Vazirani Umesh., Vazirani Vijay. Matching is as easy as matrix inversion // Combinatorica. — 1987. — 7 (1). — P. 105–113.

4. Valiant L., Vazirani V. NP is as easy as detecting unique solutions // Theoretical Computer Science. — 1986. — 47. — P. 85–93.

МАТРОИДЫ, СВЯЗАННЫЕ С РАЗБИЕНИЯМИ МНОЖЕСТВ, И ИХ СИЛЬНЫЕ ОТОБРАЖЕНИЯ

А. М. Ревякин (Москва), А. Н. Исаченко (Минск)

Используются терминология и обозначения монографии Оксли [1]. Пусть $M = (S, I)$ — матроид на конечном множестве S с с семейством независимых множеств I и ранговой функцией $r(A)$, $A \subseteq S$, и k — натуральное число, $0 < k \leq r(S)$. Подмножество

A множества S называется замкнутым, если $r(A \cup a) > r(A)$ для каждого $a \in S \setminus A$. Семейство $L(M)$ всех замкнутых множеств матроида образует геометрическую решетку. Матроид M_k с семейством независимых множеств $I_k = \{A \subseteq S : A \in I \text{ и } |A| \leq k\}$ называется k-усечением матроида M. Ранговая функция матроида M_k равна $r_k(A) = \min\{k, r(A)\}$. Решетка замкнутых множеств M_k получается из решетки $L(M)$ вычеркиванием всех элементов ранга, большего или равного k, и заменой всех их единственным максимальным элементом решетки. Если некоторый матроид M на множестве S изоморфен $(r(H)-1)$-усечению матроида H на том же множестве S, то говорят, что H есть наращение матроида M. Решетка $L(H)$ замкнутых множеств матроида H получается из решетки $L(M)$ включением уровня новых коатомов, который лежит между старыми коатомами и единичным элементом решетки. Различные наращения матроида N на конечном множестве S, упорядоченные как антицепи булеана, образуют полную решетку, минимальный элемент FM которого называется свободным наращением матроида M. Конструкция свободного наращения и свойств наращений описаны в [2].

Введем нулевой элемент 0 ($0 \notin S$), который соответствует пустому множеству $\emptyset$ и обозначим через $\{\emptyset\}$ матроид с нулевым рангом на одноэлементном множестве $\{0\}$. Пусть матроид $M_0 = M + \{\emptyset\}$ — прямая сумма матроидов M и $\{\emptyset\}$ на множестве $S \cup 0$. Сильным отображением матроида M на множестве S в матроид N на множестве T (обозначение: $M \Rightarrow N$) называется функция $\sigma : S \cup 0 \to T \cup 0$ такая, что $\sigma(0) = 0$, и прообраз каждого замкнутого множества N_0 замкнут в M_0. Слабым отображением матроида M на множестве S в матроид N на множестве T (обозначение: $M \dashrightarrow N$) называется функция $\sigma : S \cup 0 \to T \cup 0$ такая, что $\sigma(0) = 0$ и если A подмножество множества S таково, что отображение $\sigma|A$ является взаимно однозначным на A и $\sigma(A)$ — независимое множество в матроиде N_0, то A — также независимое множество в матроиде M. Основные результаты о слабых и сильных отображениях можно найти в [3–8].

Пусть M^* — матроид, двойственный к матроиду M, а $M \cup N$ — объединение матроидов M и N на одном и том же множестве S. Тогда тождественная функция на $S \cup 0$ индуцирует сильные отображения $M \cup N \Rightarrow M$ и $M \Rightarrow M_k$. Причем, если $M \Rightarrow N$, то $M \dashrightarrow N$ (обратное неверно) и $N^* \Rightarrow M^*$. Для слабых отображений следующие условия эквивалентны: а) тождественная функция на $S \cup 0$ индуцирует $M \dashrightarrow N$; б) каждое независимое множество в N является также независимым в M; в) каждое зависимое множество в M

также зависимо в N; г) каждый цикл из M содержит цикл из N; д) $r_M(A) \geq r_N(A)$ для каждого $A \subseteq S$.

Теорема 1. *Пусть FN — свободное, а N — произвольное наращения матроида M на S. Тогда тождественная функция индуцирует слабое отображение $FN \dashrightarrow N$.*

Теорема 2. *Если $M \wedge N = (M^* \cup N^*)^*$, то $M \Rightarrow M \wedge N$.*

Матроид $M \wedge N$ из теоремы 2 называется произведением матроидов M и N.

Пусть $G = (V, E)$ — связный граф, M — его циклический матроид на E, а $\omega(v)$ — функция, заданная на вершинах графа, со значениями в некотором поле F, не равная тождественно нулю, что $\sum\limits_{v \in V} \omega(v) = 0$. Будем говорить, что двухкомпонентный лес асиметричен, если сумма весов вершин каждой его компоненты связности не равна $0 \in F$.

Теорема 3. *Асиметричные двухкомпонентные леса графа $G = (V, E)$ образуют базы некоторого матроида N на множестве ребер E и тождественная функция на $E \cup 0$ индуцирует сильное отображение циклического матроида M графа G в N.*

Теорема 4. *Пусть $M = (S, I)$ — матроид ранга k, и пусть $S = B \cup R_1 \cup R_2 \cup \ldots \cup R_p$ — разбиение множества S на попарно непересекающиеся подмножества, $r(B) = k$ и семейство I^* содержит все такие подмножества A множества B, что $A \in I$, $|A| = k - p$ и найдутся $a_i \in R_i$, для которых $A \cup \{a_1, \ldots, a_p\} \in I$. Тогда если I^* непусто, то оно образует семейство баз некоторого матроида $M_{R_1,R_2,\ldots,R_p}$ на множестве B и тождественная функция на $B \cup 0$ индуцирует сильное отображение сужения $M \setminus (R_1 \cup R_2 \cup \ldots \cup R_p)$ в матроид $M_{R_1,R_2,\ldots,R_p}$.*

Для p равных 1, 2 и 3 результат, аналогичный теореме 4, ранее получил А. Речки [8]. Приведенные в работе результаты могут быть использованы в приложениях для определения жесткости планарных ферм с удаленными фрагментами [8] и решения задач электротехники [3, 4]. При этом определение жесткости планарных ферм, состоящих из жестких стержней и соединяющих их шарниров, сводится к проверке сильной связности неких специально построенных ориентированных двудольных графов. Следовательно, минимальное число диагональных стержней, которые необходимо добавить для жесткости квадратной фермы, равно минимальному числу дуг в соответствующем сильно связном остовном подграфе двудольного графа.

Список литературы

1. Oxley J. G. Matroid theory. — N.Y.: Oxford University Press, 2006.

2. Ревякин А. М. О наращениях комбинаторных геометрий //Вестн. Моск. ун-та. Мат. Мех. — 1976. — 4. — С. 59–62.

3. Recski A. Matroid theory and its applications in electric network theory and in statics — Budapest: Akad. Kiado, 1989.

4. Revyakin A. M. Matroids // J. Math. Sci. — 2002. — V. 108, N 1. — P. 71–130.

5. Welsh D. J. A. Matroid Theory. — London: Academic Press, 1976.

6. Kung J. P. S. Strong maps // In: Theory of matroids / Ed. White N. — Cambridge Univ. Press. — 1986. — P. 224–253.

7. Kung J. P. S., Nguyen Hien Quang. Weak maps // In: Theory of matroids / Ed. White N. — Cambridge Univ. Press. — 1986. — P. 254–271.

8. Ревякин А. М., Речки А. Сильные и слабые отображения матроидов и их применение // Материалы YIII Международного семинара "Дискретная математика и ее приложения"(2–6 февраля 2004 г.) — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 219–221.

ПАРАТОПИИ ОРТОГОНАЛЬНЫХ СИСТЕМ ТЕРНАРНЫХ КВАЗИГРУПП

П. Н. Сырбу, Д. К. Чебан (Кишинев)

Понятие паратопии введено В. Д. Белоусовым в [1]. Пусть $\Sigma = \{F, E, A, B\}$ — ортогональная система, где A и B — бинарные квазигруппы, определенные на непустом множестве Q, а F и E — бинарные селекторы на Q: $F(x, y) = x$, $E(x, y) = y$, $\forall x, y \in Q$. Если $\theta : Q^2 \to Q^2$ некоторое отображение, то существуют бинарные операции C и D на Q, такие что $\theta(x, y) = (C(x, y), D(x, y))$ $\forall x, y \in Q$. Положим $\theta = (C, D)$. Отображение θ называется паратопией системы Σ, если $\Sigma\theta = \Sigma$. В. Д. Белоусов показал [1], что существуют в точности девять ортогональных систем, состоящих из двух бинарных квазигрупп и бинарных селекторов F и E, которые обладают по крайней мере одной нетривиальной паратопией. Авторы данного сообщения обобщили результат Белоусова на тернарный случай и

полностью описали ортогональные системы, состоящие из трех тернарных квазигрупп и тернарных селекторов, обладающие по крайней мере одной паратопией.

Напомним, что n-арный группоид (Q, A) называется n-арной квазигруппой, если в равенстве $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ каждый элемент множества $\{x_1, x_2, \ldots, x_{n+1}\}$ однозначно определен остальными n элементами. Если (Q, A) является n-арной квазигруппой и $\sigma \in S_n$, то операция ${}^{\sigma}A$, заданная эквивалентностью

$$ {}^{\sigma}A(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}) = x_{\sigma(n+1)} \Leftrightarrow A(x_1, x_2, \ldots, x_n) = x_{n+1} $$

для любых $x_1, x_2, \ldots, x_n, x_{n+1} \in Q$, называется парастрофом (Q, A). Парастроф ${}^{\sigma}A$ называется главным парастрофом, если $\sigma(n + 1) = n + 1$. Операции $A_1, A_2, \ldots, A_n$, арности n, определенные на множестве Q, называются ортогональными, если, для любых $a_1, a_2, \ldots, a_n \in Q$, система уравнений $\{A_i(x_1, x_2, \ldots, x_n) = a_i\}_{i=\overline{1,n}}$ разрешима однозначно. Система n-арных операций $A_1, A_2, \ldots, A_s$, определенных на множестве Q, где $s \geq n$, называется ортогональной если каждые n операций этой системы ортогональны. Для любого отображения $\theta : Q^n \to Q^n$ существуют n единственных n-арных операций $A_1, A_2, \ldots, A_n$, на Q, такие что $\theta((x_1^n)) = (A_1(x_1^n), A_2(x_1^n), \ldots, A_n(x_1^n))$, для любых $(x_1^n) \in Q^n$. Более того, отображение θ биективно тогда и только тогда, когда операции $A_1, A_2, \ldots, A_n$ ортогональны [5]. Операции $E_1, E_2, \ldots, E_n$, где $E_i(x_1, x_2, \ldots, x_n) = x_i$, для любых $x_1, x_2, \ldots, x_n \in Q$, называются n-арными селекторами на Q. n-арные квазигруппы, обладающие ортогональными n-ками парастрофов (главных парастрофов), называются парастрофно-ортогональными (самоортогональными).

Если $\Sigma = \{A_1, A_2, \ldots, A_n, E_1, E_2, \ldots E_n\}$ — ортогональная система, то систему $\{A_1\theta, A_2\theta, \ldots, A_n\theta, E_1\theta, E_2\theta, \ldots, E_n\theta\}$ обозначим через $\Sigma\theta$. Биективное отображение $\theta : Q^n \to Q^n$ называется паратопией системы Σ если $\Sigma\theta = \Sigma$.

Рассмотрим ортогональную систему $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$, где A_1, A_2, A_3 — тернарные квазигруппы определенные на непустом множестве Q и E_1, E_2, E_3 — тернарные селекторы на Q. Пусть $\theta : Q^3 \to Q^3$ — некоторое отображение, $\theta = (B_1, B_2, B_3)$, где B_1, B_2, B_3 являются тернарными операциями на Q и $\theta(x_1^3) = (B_1(x_1^3), B_2(x_1^3), B_3(x_1^3))$, для любых $(x_1^3) \in Q^3$. Если θ является паратопией системы Σ, то $\{A_1, A_2, A_3, E_1, E_2, E_3\} = \{A_1\theta, A_2\theta, A_3\theta, B_1, B_2, B_3\}$, следовательно паратопии системы Σ являются тройками операций Σ.

Мы находим необходимые и достаточные условия того, что тройка операций из Σ задает паратопию системы Σ. Так как селекторы E_1, E_2, E_3 фиксированны, мы рассматриваем тройки операций из Σ со всевозможным расположением селекторов: тройки без селекторов (один возможный случай), тройки с одним селектором и двумя квазигрупповыми операциями (9 возможных случаев, так как селектор E_i может появляться в каждой из трех позиций и $i = 1, 2, 3$), тройки с одной квазигрупповой операцией и двумя селекторами (18 возможных случаев, так как каждые два селектора могут появляться в каждых двух из трех позиций) и тройки из трех селекторов (6 возможных случаев).

Мы доказываем, что тройка операций из Σ задает паратопию системы Σ тогда и только тогда, когда квазигрупповые операции данной системы выражаются друг через друга (с помощью парастрофии и/или суперпозиции) и, в большинстве случаев, одна из квазигруп системы удолетворяет некоторому тождеству. Более того, некоторые из полученных тождеств влекут самоортогональность соответствующей тернарной квазигруппы или некоторых ее бинарных ретрастов.

Отметим что в бинарном случае существование паратопий влечет выполлнение некоторых минимальных тождеств, а именно трех из семи минимальных тождеств из классификации Белоусова-Беннетта [2]. Известно, что выполнение минимальных тождеств в бинарных квазигруппах влечет ортогональность некоторых пар парастрофов данных квазигрупп [2, 3, 6].

При исследовании необходимых и достаточных условий чтобы тройка операций из $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ задавала паратопию системы Σ, получено описание всех паратопий данной системы и найдены все ортогональные системы из трех тернарных квазигрупп и тернарных селекторов, обладающие по крайней мере одной нетривиальной паратопией.

Теорема. *Существует* 153 *ортогональных систем, состоящих из трех тернарных квазигрупп и тернарных селекторов* E_1, E_2, E_3, *обладающих по крайней мере одной нетривиальной паратопией.*

Следствие 1 [4]. *Любая тернарная квазигруппа* (Q, A) *удовлетворяющая одному из тождеств* $A(A,^{(132)} A,^{(123)} A) = E_2$ *или* $A(A,^{(132)} A,^{(123)} A) = E_3$, *является самоортогональной типа* $(\varepsilon, (132), (123))$.

Следствие 2. *Если тернарная квазигруппа* (Q, A) *удовлетворяет тождеству* $A(E_1, A,^{(23)} A) = E_3$ *то, для* $\forall a \in Q$, *его* 1*-ретракт* $B_a(x, y) = A(a, x, y)$ *является самоортогональным.*

Следствие 3. *Если тернарная квазигруппа* (Q, A) *удовлетворяет тождеству* $A(A, E_2, {}^{(13)}A) = E_3$ *то, для* $\forall a \in Q$, *его* 2*-ретракт* $B_a(x, y) = A(x, a, y)$ *вляется самоортогональным.*

Следствие 4. *Если тернарная квазигруппа* (Q, A) *удовлетворяет тождеству* $A(A, {}^{(12)}A, E_3) = E_2$ *то, для* $\forall a \in Q$, *его* 3*-ретракт* $B_a(x, y) = A(x, y, a)$ *вляется самоортогональным.*

Список литературы

1. Белоусов В. Д. Системы ортогональных операций // Матем. сборник. — 1968. — 77 (119). — С. 33–52.

2. Belousov V. Parastrofic-orthogonal quasigroups // Quasigroups and Related Systems. — 2005. — 14. — P. 3–51.

3. Bennett F.E. Quasigroups identities and Mendelsohn designs // Canad. J. Math. — 1989. — 41 (2). — P. 341–368.

4. Evans T. Latin cubes orthogonal to their transposes — a ternary analogue of Stein quasigroups // Aequationes Math. — 1973. — 9. P. 296–297.

5. Сырбу П.Н. Об ортогональных и самоортогональных n-арных операциях // Матем. исслед. — 1987. — 66. — С. 121–129.

6. Syrbu P., Ceban D. On π-quasigroups of type T_1 // Bul. Acad. Stiinte Repub. Mold. Mat. — 2014. — 2. — P. 36–43.

О КОМБИНАТОРНОМ ТОЖДЕСТВЕ HAJNAL—NAGY

С. П. Тарасов (Москва)

Решеточным путем называется путь из шагов $(1, 1), (1, -1)$ по целым точкам двумерной целочисленной решетки. Число шагов пути называется *длиной* пути. *Путем Дика* называется решеточный путь (четной длины), который стартует из начала координат, проходит только по точкам с неотрицательными ординатами и заканчивается на оси абсцисс (но не пересекает ее).

Назовем *профилем* любую конечную $\{0, 1\}$-последовательность. Будем говорить, что решеточный путь *согласован* с профилем $[b_0\, b_1 \ldots]$, $b_i \in \{0, 1\}$, если он не проходит через точки из множества $\{(2i, 0) \mid b_i = 0\}$.

Обозначим $\mathcal{P}[(1^k0^k)^n1] = \mathcal{P}[\underbrace{1^k0^k\ldots1^k0^k}_{n\text{ раз}}1]$ множество всех решеточных путей длины $4kn$, которые начинаются в начале координат и согласованы с профилем $(1^k0^k)^n1$. В [1] высказана гипотеза, что справедливо тождество $|\mathcal{P}[(1^k0^k)^n1]| = |\mathcal{P}[\underbrace{1^k0^k\ldots1^k0^k}_{n\text{ раз}}1]| = 4^{4kn-n}B_n$, где $B_n = \binom{2n}{n}$. Мы показываем справедливость этого тождества для небольших k. Для этого выписывается система уравнений относительно производящих функций соответствующих решеточных путей с ограничениями, которую удается решить для небольших значений k.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 14-01-00641.

Список литературы

1. P. Hajnal P., Nagy G.V. A bijective proof of Shapiro's Catalan convolution // The electronic journal of combinatorics. — 2014. — 21 (2). — P. 2–42.

О МИНИМАЛЬНОМ МНОГОЧЛЕНЕ МАТРИЦЫ ОГРАНИЧЕНИЙ МНОГОИНДЕКСНОЙ ТРАНСПОРТНОЙ ЗАДАЧИ

Е. Б. Титова, В. Н. Шевченко (Нижний Новгород)

Будем использовать следующие обозначения: $\mathbf{1}^{p\times q}$ — $p \times q$-матрица, каждый элемент которой равен 1, E_n — единичная матрица n-го порядка; A — целочисленная $m \times n$-матрица ($m \le n$), $r(A)$ — ее ранг, $A^\top$ — матрица, транспонированная к A, $A \times B$ — кронекерово произведение матриц A и B (определение и свойства см., например, в [1]).

Традиционная мера сложности для многоиндексных транспортных многогранников (Тр) — рост миноров в матрицах ограничений этих задач [2, 3]. Здесь делается попытка в качестве меры сложности рассматривать степень минимального многочлена этой матрицы.

Рассмотрим двухиндексный Тр, являющийся множеством неотрицательных решений системы линейных уравнений:

$$\sum_{j_1=1}^{n_1} x_{j_1 j_2} = b_{0 j_2},\ \sum_{j_2=1}^{n_2} x_{j_1 j_2} = b_{j_1 0}. \tag{1}$$

Ее можно обобщить на случай трехиндексного Тр двумя способами: в первом число суммирований $s = 1$ (планарный Тр) и

$$\sum_{j_1=1}^{n_1} x_{j_1 j_2 j_3} = b_{0 j_2 j_3},\ \sum_{j_2=1}^{n_2} x_{j_1 j_2 j_3} = b_{j_1 0 j_3},\ \sum_{j_3=1}^{n_3} x_{j_1 j_2 j_3} = b_{j_1 j_2 0},$$

во втором число суммирований $s = k - 1 = 2$ (аксиальный Тр) и

$$\sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2} x_{j_1 j_2 j_3} = b_{00 j_3},\ \sum_{j_1=1}^{n_1}\sum_{j_3=1}^{n_3} x_{j_1 j_2 j_3} = b_{0 j_2 0},\ \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3} x_{j_1 j_2 j_3} = b_{j_1 00}.$$

Используя кронекерово произведение систему (1) можно записать в виде:

$$T_{12}(n_1, n_2) = \begin{pmatrix} E_{n_1} \times \mathbf{1}^{1\times n_2} \\ \hline \mathbf{1}^{1\times n_1} \times E_{n_2} \end{pmatrix}.$$

Для матрицы $T_{12}(n_1, n_2)T_{12}^{\top}(n_1, n_2)$ характеристический многочлен имеет вид

$$\det(\lambda E_{n_1+n_2} - T_{12}T_{12}^{\top}) = \lambda(\lambda - n_1)^{(n_2-1)}(\lambda - n_2)^{(n_1-1)}(\lambda - (n_1 + n_2)),$$

для матрицы $T_{12}^{\top}(n_1, n_2)T_{12}(n_1, n_2)$ —

$$\det(\lambda E_{n_1 n_2} - T_{12}^{\top}T_{12}) = \lambda^{(n_1 n_2 - n_1 - n_2 + 1)}(\lambda - n_1)^{(n_2-1)}(\lambda - n_2)^{(n_1-1)}\cdot$$

$$\cdot(\lambda - (n_1 + n_2)),$$

а минимальный многочлен $\delta(\lambda, T_{12}(n_1, n_2))$ для обоих случев совпадает и при $n_1 \neq n_2$ имеет максимальную степень $d_{12}(n_1 \neq n_2) = 4$:

$$\delta(\lambda, T_{12}(n_1, n_2)) = \lambda(\lambda - n_1)(\lambda - n_2)(\lambda - (n_1 + n_2)),$$

при $n_1 = n_2 = n$ — минимальную степень $d_{12}(n_1 = n_2) = 3$:

$$\delta(\lambda, T_{12}(n)) = \lambda(\lambda - n)(\lambda - 2n).$$

При переходе к k индексам (широкий спектр прикладных задач, получаемых таким образом, см., например, в [4]) с неотрицательными переменными $x_J = x_{j_1 \ldots j_k}$ первый блок Тр с s суммированиями имеет вид

$$\sum_{j_1=1}^{n_1} \ldots \sum_{j_s=1}^{n_s} x_{j_1,\ldots,j_k} = b_{0\ldots 0 j_{s+1}\ldots j_k},$$

а соответствующая матрица ограничений имеет вид $T_{I_1}(n_1,\ldots,n_k) = \mathbf{1}^{1\times n_1}\times\ldots\times\mathbf{1}^{1\times n_s}\times E_{n_{s+1}}\times\ldots\times E_{n_k}$. Если рассмотреть все возможные варианты суммирования и лексикографически упорядочить индексы переменных $x_{j_1,\ldots,j_k}$ и правых частей уравнений, то матрица ограничений $T_{sk}(n_1,\ldots,n_k)$ k-индексной задачи с s суммированиями будет иметь следующее рекурсивное задание:

$$T_{s,k}(n_1,\ldots,n_k) = \left[\begin{array}{ccc} T_{s,k-1}(n_1,\ldots,n_{k-1}) & \times & E_{n_k} \\ \hline T_{s-1,k-1}(n_1,\ldots,n_{k-1}) & \times & \mathbf{1}^{1\times n_k} \end{array}\right].$$

Матрица $T_{sk}(n_1,\ldots,n_k)$ состоит из $\binom{k}{s}$ строчечных блоков, число ее столбцов $N = \prod_{i=1}^{k} n_i$, строк $M = \sigma_{k-s}(n_1,\ldots,n_k)$, ранг $r = \sum_{i=s}^{k}\sigma_{k-i}(n_1-1,\ldots,n_k-1)$. В [5] получен характеристический многочлен матрицы $T_{sk}(n_1,\ldots,n_k)^{\top}T_{sk}(n_1,\ldots,n_k)$. Отсюда при $n_1 = \ldots = n_k = n$ легко выписывается минимальный многочлен

$$\delta(\lambda, T_{sk}(n)) = \lambda\prod_{j=s}^{k}(\lambda - \binom{j}{s}n^s).$$

Утверждение 1. *Минимальная степень* $d_{sk}(n_1 = \ldots = n_k \geq 2) = k - s + 2$, *максимальная* $d_{sk}(n_1 \neq \ldots \neq n_k \neq 1) = 1 + \prod_{i=s}^{k}\binom{k}{s}$.

Матрицу T назовем α-модулярой, если в любой базисной системе столбцов все миноры порядка r равны $\pm\alpha$. В таком случае задача проверки пустоты транспортного многогранника имеет эффективный алгоритм. Для $T_{13}(n_1,n_2,n_3)$ свойство α-модулярности доказано в [6].

Утверждение 2. *Матрица* $T_{1k}(n_1,n_2,n_3,2\ldots,2)$ — α-*модулярна.*

Хорошо известно, что для матриц $T_{sk}(n_1,\ldots,n_k)$ при $s \geq 2$ утверждение 2 не верно [2].

Список литературы

1. Воеводин В. В., Кузнецов Ю. А. СМБ. Матрицы и вычисления. — М.: Наука, 1984.

2. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

3. Титова Е. Б., Шевченко В. Н. О минорах матрицы ограничений многоиндексных транспортных задач // Дискретная математика. — 2012. — Т. 24, вып. 4. — С. 147–157.

4. Раскин Л. Г., Кириченко И. О. Многоиндексные задачи линейного программирования. — М.: Радио и связь, 1982.

5. Шевченко В. Н. Характеристические многочлены многоиндексных транспортных задач // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 83–88.

6. Ильичёв А. П. Исследование многогранников многоиндексных транспортных задач: Автореферат дис. канд. физ.-мат. наук. — Горький, 1988.

О НЕЗАВИСИМЫХ СЕМЕЙСТВАХ МНОЖЕСТВ В ЗАДАЧЕ О ПОКРЫТИИ

И. П. Чухров (Москва)

Комбинаторная постановка задачи о покрытии конечного множества заключается в нахождении семейства допустимых подмножеств минимальной сложности, которое содержит все элементы множества.

Системой множеств называется пара $\langle X, Y\rangle$, где X — конечное множество элементов и $Y \subseteq 2^X$ — *семейство* различных множеств.

Множество элементов X, которые содержатся в произвольном семействе множеств $S \subseteq Y$, обозначим через X_S. Будем говорить, что семейство S *покрывает* множество элементов X_S.

Покрытием для системы множеств $\langle X, Y\rangle$ называется любое семейство $S \subseteq Y$, которое покрывает все множество X. Для существования покрытия семейство Y должно покрывать все множество X.

Сложность произвольного семейства множеств $S \subseteq Y$ определяется неотрицательным аддитивным функционалом $C\colon Y \to R^+$, который задает сложность множеств из Y, и соотношением $C(S) = \sum_{y\in S} C(y)$, определяющим сложность семейства S.

Стандартная задача о покрытии $Z = \langle X, Y, C\rangle$ заключается в нахождении семейства $S \subseteq Y$, которое является покрытием X и имеет

минимальную сложность $C(S)$. Сложность минимального покрытия в задаче $Z = \langle X, Y, C\rangle$ обозначим через $C(X, Y)$.

Если сложность любого множества равна 1 и сложность любого семейства равна его мощности, то функционал сложности называется *длиной* и обозначается через l.

Различные оптимизационные задачи для дискретных структур могут быть сформулированы как задачи о покрытии обобщенного вида. При этом может требоваться покрыть заданное подмножество элементов, а система множеств и функционал сложности могут удовлетворять ограничениям, которые порождаются свойствами структур, например, графа, булева куба и т. д. Следующие задачи обобщенного вида могут быть сведены к стандартной задаче о покрытии множества.

(i) Задача $Z_A = \langle A, X, Y, C\rangle$, где $A \subset X$, заключается в нахождении семейства $S \subseteq Y$ минимальной сложности, которое *покрывает* A, т. е. $A = X_S$.

(ii) Задача $\tilde{Z}_A = \langle A, X, Y, C\rangle$, где $A \subset X$, заключается в нахождении семейства $S \subseteq Y$ минимальной сложности, которое *содержит* A, т.е. $A \subseteq X_S$.

(iii) Задача $\tilde{Z}_{A,B} = \langle A, B, X, Y, C\rangle$, где $A \subset X$, $B \subset X$ и $A \cap B$ — пусто, заключается в нахождении семейства $S \subseteq Y$ минимальной сложности, для которого $A \subseteq X_S \subseteq A \cup B$.

Задача минимизации булевых функций относительно аддитивной меры сложности $\mathcal{L}$ в геометрической интерпретации [1] является задачей о покрытии для системы множеств $\langle B^n, G^n\rangle$, где B^n — множество вершин, G^n — множество граней n-мерного единичного куба и сложность комплекса граней равна сумме сложностей граней. Задаче минимизации всюду определенной булевой функции соответствует задача $Z_A = \langle N_f, B^n, G^n, \mathcal{L}\rangle$, а частично определенной булевой функции соответствует задача $\tilde{Z}_{A,B} = \left\langle N_f, N_{\tilde{f}}, B^n, G^n, \mathcal{L}\right\rangle$, где $A = N_f$ и $B = N_{\tilde{f}}$ — множества единичных и неопределенных вершин функции f в кубе B^n соответственно.

В обзорных статьях [2, 3] изложены различные алгоритмические вопросы и подходы к решению задачи о покрытии, которые характерны для многих трудных дискретных оптимизационных задач.

Предлагаемый метод получения нижних оценок длины и сложности минимальных покрытий основан на обобщении понятия независимого множества элементов.

Определение. *Независимым семейством множеств для системы множеств* $\langle X, Y\rangle$ *называется семейство* $\mathcal{A} = \{A \mid A \subset X\}$,

если любое множество $y \in Y$ пересекается не более чем с одним множеством $A \in \mathcal{A}$.

Независимое множество элементов является частным случаем независимого семейства множеств, в котором каждое множество состоит из одного элемента. Независимыми семействами множеств являются семейства, которые соответствуют компонентам связности или состоят из двух множеств: собственных элементов всех ядровых множеств и элементов, которые не содержатся в ядровых множествах.

Лемма 1. *Если $\mathcal{A}$ является независимым семейством для системы множеств $\langle X, Y\rangle$, то для любого аддитивного функционала сложности C выполняется $C(X,Y) \geq \sum\limits_{A\in\mathcal{A}} \tilde{C}(A,X,Y)$, где $\tilde{C}(A,X,Y)$ — сложность минимального покрытия для задачи $\tilde{Z}_A$.*

Лемма 2. *Для задачи $\tilde{Z}_A = \langle A, X, Y, C\rangle$ справедливы оценки*

$$\tilde{l}(A,X,Y) \geq \tilde{l}_{X,Y,A} = \lceil |A|/\Delta_{X,Y,A}\rceil,\ \tilde{C}(A,X,Y) \geq \tilde{C}_{X,Y,A},$$

где $\Delta_{X,Y,A}$ — максимальное число элементов множества A, которые содержатся в одном множестве семейства Y; $\tilde{C}_{X,Y,A}$ — сложность $\tilde{l}_{X,Y,A}$ множеств из Y, которые пересекаются с множеством A и имеют меньшую сложность.

Независимое семейство множеств может быть представлено в виде объединения независимого множества элементов, возможно пустого, и независимого семейства множеств среди которых нет независимых множеств элементов.

Теорема 1. *Если $\{Q\} \cup \mathcal{A}$ является независимым семейством для системы множеств $\langle X, Y\rangle$, где Q — независимое множество и в семействе $\mathcal{A}$ нет независимых множеств, то для аддитивного функционала сложности выполняется*

$$l(X,Y) \geq |Q| + \sum_{A\in\mathcal{A}} \lceil |A|/\Delta_{X,Y,A}\rceil,$$

$$C(X,Y) \geq \sum_{x\in Q} \tilde{C}_{X,Y,\{x\}} + \sum_{A\in\mathcal{A}} \tilde{C}_{X,Y,A}.$$

Оценки теоремы 1, в случае их достижимости, являются достаточными условиями минимальности покрытия и используются при доказательстве следующей теоремы.

Теорема 2. *Для задачи минимизации булевых функций*

(i) при $n \leq 3$ для всех функций длина кратчайшего покрытия совпадает с мощностью максимального независимого множества;

(ii) при $n \geq 5$ существуют функции, для которых длина кратчайшего покрытия больше мощности максимального независимого

множества.

Работа выполнена при финансовой поддержке РФФИ (проект 16-01-00593а).

Список литературы

1. Чухров И. П. О мерах сложности комплексов граней в единичном кубе // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 6. — С. 77–94.

2. Еремеев А. В., Заозерская Л. А., Колоколов А. А. Задача о покрытии: сложность, алгоритмы, экспериментальные исследования // Дискретный анализ и исследование операций. — 2000. — Серия 2, Т. 7, № 2. — С. 22–46.

3. Coudert O., Sasao T. Two-level logic minimization // Logic synthesis and verification — Norwell, MA, USA: Kluwer Academic Publishers — 2002. — P. 1–27.

ЦИКЛЫ В ЛИНЕЙНОМ И ЦЕЛОЧИСЛЕННОМ ЛИНЕЙНОМ ПРОГРАММИРОВАНИИ

В. Н. Шевченко (Нижний Новгород)

Будем использовать следующие бозначения: $\mathbf{Z}$ — кольцо целых чисел, $\mathbf{R}$ — поле вещественных чисел, если $M \subseteq \mathbf{R}$, то M^n — множество n-мерных столбцов x с координатами $x_j \in M$; при $x \in M^n, y \in M^n$ $x \leq y \Leftrightarrow x_j \leq y_j (j = 1, \ldots, n) \Leftrightarrow y \geq x$; $x < y \Leftrightarrow x_j < y_j (j = 1, \ldots, n) \Leftrightarrow y > x$. Аналогично определяется множество $M^{s \times t}$ матриц и отношения $''\geq''$ и $''>''$ на нем. Через $r(A)$ обозначим ранг матрицы A, а через A^T — матрицу, транспонированную к A.

Рассмотрим пару двойственных задач ЛП:

$$\begin{array}{ccccc} \max & & cx & & \\ x & \geq & 0 & \text{и} & \\ Ax & \leq & b & & \end{array} \qquad \begin{array}{ccccc} \min & & ub & & \\ uA & \geq & c & , & \\ u & \geq & 0 & & \end{array}$$

соответствующую этой паре кососимметрическую матрицу

$$K(A) = \begin{pmatrix} 0 & A^T \\ -A & 0 \end{pmatrix},$$

а также окаймляющие ее матрицы

$$K_{00}(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & A^T \\ 0 & -A & 0 \end{pmatrix}, \quad K_{01}(A) = \begin{pmatrix} 0 & c & 0 \\ -c^T & 0 & A^T \\ 0 & -A & 0 \end{pmatrix},$$

$$K_{10}(A) = \begin{pmatrix} 0 & 0 & -b^T \\ 0 & 0 & A^T \\ b & -A & 0 \end{pmatrix}, \; K_{11}(A) = \begin{pmatrix} 0 & c & -b^T \\ -c^T & 0 & A^T \\ b & -A & 0 \end{pmatrix}.$$

Положим при $\mu \in \{0,1\}$, $\nu \in \{0,1\}$ $r_{\mu\nu}(m,n) = r(K_{\mu\nu}(A))$. Хорошо известно [1], что для любой кососимметрической матрицы K множество $C(K) = \{z : z \geq 0, Kz \geq 0, z + Kz > 0\}$ не пусто и что [2] каждый из векторов $z \in C(K_{11})$ решает обе задачи линейного программирования. Отсюда следует, что задача линейного программирования и основная задача теории линейных неравенств — нахождение решения системы линейных неравенств или доказательство его отсутствия — имеют одинаковую сложность. Так же хорошо известно [2], что данный факт не верен для задач целочисленного линейного программирования. Если рассматриваемый вектор z единственный, то обозначим его $z_{opt} = (t; x; u)^T \in \mathbf{Z}^{(m+n+1)\times 1}$. Алгоритмы, вычисляющие $z_{opt}(K_{11})$ по известному $z_{opt}(K_{00})$, назовем циклическими. Будем считать далее, что $r_{00}(m,n)$ остался неизменным.

Для $d \times n$-матрицы B со столбцами b_j $(j = 1, 2, \ldots, n)$ обозначим через $B^{\angle} = \{\sum_{j=1}^{n} b_j y_j \; y_j \geq 0\}$ множество неотрицательных линейных комбинаций ее столбцов и предположим, что $B^{\angle}$ совпадает со множеством решений системы $\sum_{k=1}^{d} a_{ik} x_k \geq 0$ $(i = 1, \ldots, m)$.

Триангуляцией конуса K с узлами из множества B назовем множество $T(B) = \{S_1, \ldots, S_t\}$ таких S_τ, для которых выполнены следующие условия: 1) $S_\tau \subseteq \{1, \ldots, n\}$, 2) $|S_\tau| = r = \operatorname{rank} B(S_\tau)$, 3) $B^{\angle} = \bigcup_{\tau=1}^{t} B^{\angle}(S_\tau)$, 4) $B^{\angle}(S_\tau) \cap B^{\angle}(S_\sigma) = B^{\angle}(S_\tau \cap S_\sigma)$.

Множество $\triangle(T(B)) = \bigcup_{\tau=1}^{t} \Gamma(S_\tau)$ дает пример геометрической реализации d-мерного однородного симплициального комплекса (с. к.). Обозначим через $\triangle_k = \bigcup_{\tau=1}^{t} \Gamma_k(S_\tau)$ $(k = 0, \ldots, d)$ множество k-мерных граней с. к. $\triangle$, положим $f(\triangle) = (f_0(\triangle), \ldots, f_d(\triangle))$, $f_k(\triangle) = |\triangle_k|$ и $f(\lambda, \Delta) = \sum_{k=0}^{d} f_k(\Delta)\lambda^k$.

Следуя [3], представим многочлен $f(\lambda, \Delta)$ в виде

$$f(\lambda, \Delta) = \sum_{k \in \mathbf{Z}_+} \gamma_k(\Delta)\lambda^k (1+\lambda)^{d-k}$$

и назовем целочисленную последовательность $\gamma = (\gamma_0, \gamma_1, \dots)$ (d,n)-реализуемой, если $\gamma_k = \gamma_k(\Delta)$ при $k = 0, 1, \dots, d$ и $\gamma_k = 0$ при $k > d$.

Для любых натуральных чисел a и i существует единственное биномиальное i-разложение числа $a = \binom{a_i}{i} + \binom{a_{i-1}}{i-1} + \dots + \binom{a_j}{j}$, где $a_i > a_{i-1} > \dots > a_j \geq j \geq 1$. Тогда число $a^{<i>} = \binom{1+a_i}{1+i} + \dots + \binom{1+a_j}{1+j}$ называется i-й псевдостепенью числа a.

Теорема 1. 1. *Если найдется такое k, при котором $\gamma_{k+1} > \gamma_k^{<k>}$, то последовательность γ не реализуема ни при каком d.*

2. *Если $\gamma_{k+1} \leq \gamma_k^{<k>}$ при $k = 1, \dots, d-1$ (условия Маколея—Макмюллена—Стенли* [4]*), то последовательность γ — $(2d)$-реализуема.*

Следующая теорема позволяет находить минимальное d, при котором последовательность γ является d-реализуемой.

Теорема 2. *Для d-реализуемости целочисленной последовательности $\gamma = (\gamma_0, \gamma_1, \dots)$ необходимо и достаточно, чтобы выполнялись следующие условия:*
1) $\gamma_0 = 1$, $\gamma_i \geq 0$ *при* $i = 1, \dots, d$ *и* $\gamma_k = 0$ *при целых* $k \geq d$,
2) $\gamma_i \geq \gamma_{d-i} \leq \gamma_{d-i-1}$ *при* $i = 1, \dots, \lfloor \frac{d}{2} \rfloor$ *("овраг")*
3) $\gamma_{i+1} - \gamma_{j-i} \leq (\gamma_i - \gamma_{j+1-i})^{<i>}$ *при* $j = d, \dots, 2d$ *и* $i = 1, \dots, \lfloor \frac{j}{2} \rfloor$.

Следствие 1. $f(\lambda, \Delta) = \sum_{k=0}^{d+1} \gamma_k(\Delta) \lambda^k (1+\lambda)^{d+1-k}$, *где* $\gamma_k(\Delta) = |\{\tau \mid \dim J_\tau = k-1\}|$ — *целое неотрицательное число, не зависящее от порядка следования симплексов* $S_1, \dots, S_t$, $\gamma_0(\Delta) = 1$ *и* $\gamma_{d+1}(\Delta) = 0$.

Таким образом, $\partial\Delta = \bigcup_{i=1}^{m_1} \Gamma(F_i)$, а для остальных граней из Δ несложно доказать, что $\Delta \setminus \partial\Delta = \bigcup_{\tau=1}^{t} [\overline{J_\tau}, S_\tau]$, где объединение дизъюнктно и $\overline{J_\tau}$ — множество вершин симплекса S_τ, дополнительное к J_τ.

Следствие 2. $f(\lambda, \Delta \setminus \partial\Delta) = \sum_{k=0}^{d+1} \gamma_k(\Delta) \lambda^{d+1-k} (1+\lambda)^k$, $f(\lambda, \partial\Delta) = \sum_{k=0}^{\delta} (\gamma_k(\Delta) - \gamma_{d+1-k}(\Delta))(\lambda^k (1+\lambda)^{d+1-k} - \lambda^{d+1-k}(1+\lambda)^k)$.

При небольших d для любых n полученные условия легко проверяемы. То же верно при любых d, если n ограничено сверху полиномом от d. Этим удалось воспользоваться для формулировки следующей гипотезы.

Гипотеза. *Пусть $\Gamma(d,n)$ — множество γ-векторов d-мерных политопов с n вершинами, $\Gamma'(d,n)$ — аналогичное множество для симплициальных политопов, $\Gamma''(d,n)$ — аналогичное множество для простых политопов,* $\mathrm{conv}(M)$ — *выпуклая оболочка множе-*

ства M. Тогда

$$\Gamma(d,n) = \boldsymbol{Z}^d \bigcap \mathrm{conv}(\Gamma'(d,n) \bigcup \Gamma''(d,n)).$$

При $d = 3$ эта гипотеза доказана Штейницем [4].

Список литературы

1. Воеводин В. В., Кузнецов Ю. А. СМБ. Матрицы и вычисления. — М.: Наука, 1984.

2. Схрейвер А. Теория линейного и целочисленного программирования. — М.: Мир, 1991.

3. Шевченко В. Н. О разбиении политопа на симплексы без новых вершин. // Известия ВУЗ. Математика. — 1997. — №12 (427). — С. 89–99.

4. Ziegler G. Lectures on polytopes. — Berlin: Springer-Verlag, 1995.

5. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

Секция «Теория графов»

О ДИСТАНЦИОННЫХ КОДАХ ГРЕЯ

И. С. Быков, А. Л. Пережогин (Новосибирск)

Определим *n-мерный код Грея* как циклическую последовательность всех 2^n бинарных слов длины n такую, что два соседних слова отличаются ровно в одном символе. Любому n-мерному коду Грея соответствует гамильтонов цикл в графе Q_n. *Переходная последовательность* пути $v_1, v_2, \ldots, v_{m+1}$ в Q_n — это слово $T = (\tau_1, \tau_2, \ldots, \tau_m)$ над алфавитом $\{1, 2, \ldots, n\}$ такое, что τ_i — направление ребра (v_i, v_{i+1}) (в случае, если путь замкнутый, считаем слово T циклическим). Необходимое и достаточное условие того, что символьная последовательность является переходной последовательностью гамильтонова цикла (кода Грея) хорошо известно и приводится, например, в [1].

Коды Грея имеют многочисленные практические применения [2]. При этом возникают вопросы о существовании и построении кодов Грея, обладающих заданными свойствами. Одним из таких свойств является локальная равномерность переходной последовательности кода, которая обеспечивает равномерное изнашивание контактов в реальных устройствах, использующих эти коды [3]. Ранее рассматривались следующие параметры равномерности:

• $l_1(G)$ — такое максимальное число, что в каждом подслове длины $l_1(C)$ переходной последовательности кода C все буквы различны; наибольшее значение, которое параметр $l_1(C)$ принимает на множестве всех n-мерных кодов Грея обозначим $l_1(n)$;

• $l_2(G)$ — такое минимальное число, что в каждом подслове длины $l_2(C)$ переходной последовательности кода C встречаются все буквы из алфавита $\{1, 2, \ldots, n\}$; наименьшее значение, которое параметр $l_2(C)$ принимает на множестве всех n-мерных кодов Грея обозначим $l_2(n)$.

Лучшие известные оценки для $l_1(n)$ и $l_2(n)$ [4, 5]:

$$n - \lceil 2.001 \log n \rceil \le l_1(n) \le n - 1;$$

$$n+1 \le l_2(n) \le n+3\lceil \log n \rceil.$$

Другим возможным свойством кода Грея является антиподальность; n-мерный код Грея называется (n,t)-*антиподальным*, если противоположные двоичные слова находятся на расстоянии t в коде. Антиподальные коды Грея изучались в [6, 7]. В частности, в [7] показано, что для любого четного n существует $(n, 2^{n-1})$-антиподальный код Грея.

Рассмотрим класс кодов Грея, со свойством, в некотором смысле обобщающим понятие равномерности и антиподальности. Назовем n-мерный код $\langle d,k\rangle_n$-*дистанционным кодом Грея*, если расстояние Хэмминга между словами, находящимися в коде на расстоянии k, равно d. Далее для краткости такой код будем называть $\langle d,k\rangle_n$-кодом Грея. Справедливы следующие утверждения:

Утверждение. *Код C является $\langle d,d\rangle_n$-кодом тогда и только тогда, когда $l_1(C) \ge d$. В частности, код C является $\langle n-1,n-1\rangle_n$-кодом тогда и только тогда, когда $l_1(C) = n-1$.*

Утверждение. *Если для кода C выполнено $l_2(C) = n+1$, то код C является $\langle n-1,n+1\rangle_n$-кодом.*

Для существования $\langle d,k\rangle_n$-кода необходимо, чтобы d и k были одной четности, а также $d \le k$.

Утверждение. *При $1 < k < 2^n - 1$ не существует $\langle 1,k\rangle_n$-кода Грея.*

Утверждение. *$\langle n,k\rangle_n$-код Грея существует тогда и только тогда, когда n — четное число и $k = 2^{n-1}$.*

Теорема. *Следующие дистанционные коды Грея существуют:*
1) $\langle 2, 2^k - 2^t\rangle_n$ *при* $t < k \le n$;
2) $\langle d, 2^{t+d-1}\rangle_n$ *при четном* d *и* $n \ge d+t$;
3) $\langle d, 2^{t+d-1} - 2^t\rangle_n$ *при четном* d *и* $n \ge d+t$;
4) $\langle d, 2^t d\rangle_n$ *при четном* d *и* $d \le l_1(n-t)$;
5) $\langle d+1, 2^t d\rangle_n$ *при нечетном* d *и* $d \le l_1(n-t)$.

Для улучшения верхней оценки $l_1(n)$ и нижней оценки $l_2(n)$, которые являются тривиальными, особый интерес представляют дистанционные коды Грея при $d = n-1$:

Теорема. *Пусть n — четное число. $\langle n-1,k\rangle_n$-код Грея существует тогда и только тогда, когда существует $\langle n-1,k'\rangle_n$-код Грея, где $k \cdot k' \equiv 1 (\mathrm{mod}\ 2^n)$.*

Доказательство. Пусть $Q_n^{(n-1)}$ — граф на множестве двоичных слов длины n, в котором ребром соединены два слова, расстояние Хэмминга между которыми равно $n-1$. Заметим, что при четном n

существует изоморфизм $\varphi : Q_n^{(n-1)} \to Q_n$:

$$\varphi(v) = \begin{cases} v, \text{если вес } v \text{ четный} \\ \overline{v}, \text{иначе.} \end{cases}$$

Пусть $C = v_0, v_1, v_2, \ldots, v_{2^n-1}$ — $\langle n-1, k\rangle_n$-код Грея. Тогда цикл

$$C' = \varphi(v_0), \varphi(v_k), \varphi(v_{2k}), \ldots, \varphi(v_{(2^n-1)k})$$

является $\langle n-1, k'\rangle_n$-кодом Грея. Теорема доказана.

Следствие. *Пусть n — четное число. Если для некоторых k и k', удовлетворяющих $k \cdot k' \equiv 1(\mod 2^n)$, выполнено $k < n-1$, то $\langle n-1, k'\rangle_n$-код Грея не существует.*

Теорема. *Пусть $k = 2^p(2m+1)$ и $(2m+1) \cdot k' \equiv 1(\mod 2^{n-p})$. Если $\frac{n-2^p}{d} > k'$, то $\langle n-d, k\rangle_n$-код Грея не существует.*

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 14-01-00507).

Список литературы

1. Пережогин А. Л. Об автоморфизмах циклов в n-мерном булевом кубе // Дискретный анализ и исследование операций. — 2007. — Вып. 14. — С. 67–79.

2. Savage C. A Survey of Combinatorial Gray Codes // SIAM Review. — 1996. — Vol. 39. — P. 605–629.

3. Goddyn L., Lawrence G. M., Nemeth E. Gray codes with optimized run lengths // Utilitas Mathematica. — 1988. — Vol. 34. — P. 179–192.

4. Goddyn L., Gvozdjak P. Binary gray codes with long bit runs // The Electronic Journal of Combinatorics. — 2003. — Vol. 10.

5. Быков И. С. О равномерных кодах Грея // Дискретный анализ и исследование операций. — 2016. — Вып. 23. — С. 51–64.

6. Killian C., Savage C., Antipodal Gray Codes // Discrete Mathematics. — 2002. — Vol. 281. — P. 221–236.

7. Chang G. J., Eu S.-P., Yeh C.-H. On the (n, t)-antipodal Gray codes // Theoretical Computer Science. — 2007. — Vol. 374 (1–3). — P. 82–90.

МИНИМАЛЬНЫЕ НОСИТЕЛИ СОБСТВЕННЫХ ФУНКЦИЙ ГРАФОВ ХЭММИНГА

А. А. Валюженич (Новосибирск)

Расстоянием Хэмминга $d(x, y)$ между словами x, y из множества $\{0, 1, \ldots, q-1\}^n$ называется число позиций, в которых x и y различны. *Графом Хэмминга* называется граф, вершины которого — это все слова длины n над алфавитом $\{0, 1, \ldots, q-1\}$, а ребрами графа соединяются вершины на расстоянии Хэмминга 1. Обозначим граф Хэмминга через $H(n, q)$. Хорошо известно, что множество собственных значений матрицы смежности графа $H(n, q)$ — это $\{\lambda_m = n(q-1) - qm | m = 0, 1, \ldots, n\}$. Функция $f : H(n, q) \longrightarrow \mathbb{R}$ называется *собственной функцией* графа $H(n, q)$, отвечающей собственному значению λ, если $Af = \lambda f$, где A — матрица смежности $H(n, q)$. Пусть $f : H(n, q) \longrightarrow \mathbb{R}$. Множество $S(f) = \{x \in H(n, q) | f(x) \neq 0)\}$ называется *носителем функции* f. Для носителя собственной функции известна следующая нижняя оценка:

Теорема [1]. *Пусть* $f : H(n, q) \longrightarrow \mathbb{R}$ *— собственная функция, отвечающая собственному значению* λ_m *и* $f \not\equiv 0$. *Тогда*

$$|S(f)| \geq 2^m (q-2)^{n-m}$$

для $\frac{mq^2}{2n(q-1)} > 2$ *и*

$$|S(f)| \geq q^n (\frac{1}{q-1})^{m/2} (\frac{m}{n-m})^{m/2} (1 - \frac{m}{n})^{n/2}$$

для $\frac{mq^2}{2n(q-1)} \leq 2$.

Из результатов работы [2] следует, что для мощности носителя собственной функции $f : H(n, q) \longrightarrow \{-1, 0, 1\}$, отвечающей собственному значению $\lambda = q(n-m) - n$, выполнена нижняя оценка $|S(f)| \geq 2^m$.

В данной работе найдены минимальные носители собственных функций графов Хэмминга $H(n, q)$ с собственным значением $n(q-1) - q$. Кроме того, получена полная характеризация собственных функций, на которых достигается минимальное значение носителя.

Множество вершин x графа $H(n, q)$, у которых i-ая координата равна k, обозначим через $T_k(i, n)$. В работе доказывается следующая теорема:

Теорема. *Пусть* $f : H(n,q) \longrightarrow \mathbb{R}$ *— собственная функция, отвечающая собственному значению* λ_1*,* $q > 2$ *и* $f \not\equiv 0$*. Тогда* $|S(f)| \geq 2(q-1)q^{n-2}$*.*

Более того, если $|S(f)| = 2(q-1)q^{n-2}$*, то*

$$f(x) = \begin{cases} c, & \text{при } x \in T_k(i,n) \setminus T_m(j,n); \\ -c, & \text{при } x \in T_m(j,n) \setminus T_k(i,n); \\ 0, & \text{иначе;} \end{cases}$$

где $c \neq 0$ *— некоторая константа,* i, j, k, m *— некоторые числа, причем* $i \neq j$*.*

Исследование выполнено при финансовой поддержке Российского научного фонда (проект 14-11-00555).

Список литературы

1. Воробьев К. В, Кротов Д. С. Оценки мощности минимального 1-совершенного битрейда в графе Хэмминга // Дискретн. анализ и исслед. опер. — 2014. — Т. 21, вып. 6. — С. 6–10.

2. Potapov V. N. On perfect 2-colorings of the q-ary n-cube // Discrete Math. — 2012. — V. 312, is. 8. — P. 1269-1272.

ПРОСТАЯ ФОРМУЛА ДЛЯ ЧИСЛА ПОМЕЧЕННЫХ ВНЕШНЕПЛАНАРНЫХ k-ЦИКЛИЧЕСКИХ БЛОКОВ И ИХ АСИМПТОТИЧЕСКОЕ ПЕРЕЧИСЛЕНИЕ

В. А. Воблый (Москва)

Точкой сочленения связного графа называется его вершина, после удаления которой вместе с инцидентными ей ребрами граф становится несвязным. *Блок* — это связный граф без точек сочленения, а также максимальный связный нетривиальный подграф, не имеющий точек сочленения. *Цикломатическим числом* связного графа называется увеличенная на единицу разность между числом ребер графа и числом его вершин. Под k*-циклическим* графом понимается связный граф с цикломатическим числом равным k. *Планарный* граф – это граф, который можно уложить на плоскости без пересечения ребер. *Внешнепланарным* графом называется планарный граф,

если его можно уложить на плоскости так, что все его вершины принадлежат одной грани [1, с. 127, 131].

Теорема. *Для числа $OB(n,k)$ помеченных внешнепланарных k-циклических блоков с n вершинами при $k \geq 1$ и $n \geq k+2$ верна формула*

$$OB(n,k) = \frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!}. \tag{1}$$

Доказательство. В [2] при $k \geq 1$ и $n \geq 3$ выведена формула

$$OB(n,k) = \frac{(n-1)!}{4} \sum_{i=1}^{k} \binom{n+i-3}{2i-2} \frac{(-1)^{k-i}(2i)!}{(2i-1)i!i!}.$$

Выражая биномиальный коэффициент через факториалы и сокращая дробь, получим

$$OB(n,k) = \frac{(n-1)!}{2} \sum_{i=1}^{k} \frac{(-1)^{k-i}(n+i-3)!}{(n-i-1)!(i-1)!i!}.$$

Обозначим правую часть (1) через $f_k(n)$ и используем метод математической индукции.

При $k=1$ верно, что $OB(n,1) = (n-1)!/2 = f_1(n)$. Пусть (1) верна при некотором k, докажем, что она верна при $k+1$. Действительно, имеем

$$OB(n,k+1) = \frac{(n-1)!}{2} \sum_{i=1}^{k+1} \frac{(-1)^{k-i+1}(n+i-3)!}{(n-i-1)!(i-1)!i!} =$$

$$\frac{(n-1)!(n+k-2)!}{2k!(k+1)!(n-k-2)!} - \frac{(n-1)!}{2} \sum_{i=1}^{k} \frac{(-1)^{k-i}(n+i-3)!}{(n-i-1)!(i-1)!i!} =$$

$$\frac{(n-1)!(n+k-2)!}{2k!(k+1)!(n-k-2)!} - \frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!} =$$

$$\frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!} \Big(\frac{(n-1)(n-2)}{k(k+1)} - 1 \Big) =$$

$$\frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!} \frac{(n+k-1)(n-k-2)}{k(k+1)} = f_{k+1}.$$

Доказательство закончено.

Следствие. *Для числа $OB(n,k)$ помеченных внешнепланарных k-циклических блоков с n вершинами при фиксированном $k \geq 1$ и $n \to \infty$ верна асимптотическая формула*

$$OB(n,k) \sim n! \frac{n^{2k-3}}{2(k-1)!k!}.$$

Доказательство. При фиксированном $k \geq 1$ и $n \to \infty$ имеем

$$OB(n,k) = \frac{n!(n+k-2)(n+k-3)...(n-k-1)}{n(n-1)(n-2)2(k-1)!k!} \sim n! \frac{n^{2k-3}}{2(k-1)!k!}.$$

Список литературы

1. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977.

2. Воблый В. А. О числе помеченных внешнепланарных k-циклических блоков // Дискретная математика. — 2016. — Т. 28 (в печати).

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ПЛАНАРНЫХ ПОЛНОБЛОЧНО-КАКТУСНЫХ ГРАФОВ

В. А. Воблый, А. К. Мелешко (Москва)

Планарный граф — это граф, который можно уложить на плоскости без пересечения ребер. Кактусом называется связный граф, в котором нет ребер, лежащих более чем на одном простом цикле [1, с. 93]. Все блоки кактуса — ребра или простые циклы. Полноблочно-кактусный граф — связный граф, у которого все блоки или полные графы, или циклы. Два графа называются гомеоморфными, если их можно получить из одного графа с помощью последовательности подразбиений ребер.

Помеченные полноблочно-кактусные графы перечислены в [2].

Теорема 1. *Для числа PF_n помеченных планарных полноблочно-кактусных графов с n вершинами при $n \geq 3$ верна формула*

$$PF_n = \frac{(n-1)!}{n}[z^{n-1}] \exp\left(nz + \frac{nz^2}{2} + \frac{nz^3}{6} + \frac{nz^3}{2(1-z)}\right).$$

Доказательство. Пусть C_n — число помеченных связных графов с n вершинами, а B_n — число помеченных блоков с n вершинами. Введем производящую функцию: $B(z) = \sum\limits_{n=3}^{\infty} B_n \frac{z^n}{n!}$.

В работе [3] автором было получена формула

$$C_n = \frac{(n-1)!}{n}[z^{n-1}] \exp(nB'(z)), \tag{1}$$

где $[z^i]$ — коэффициентный оператор [4, с. 11].

Обозначая через $\bar{B}(z)$ экспоненциальную производящую функцию для числа блоков помеченных планарных полноблочно-кактусных графов, получим

$$PF_n = \frac{(n-1)!}{n}[z^{-1}] \exp(n\bar{B}'(z))z^{-n}.$$

Из теоремы Понтрягина-Куратовского следует, что граф планарен тогда и только тогда, когда он не содержит подграфов, гомеоморфных полному графу K_5 и $K_{3,3}$. Поэтому в рассматриваемых графах нет блоков-полных графов с числом вершин $n > 4$. Учитывая, что число помеченных циклов с n вершинами равно $(n-1)!/2$, найдем

$$\bar{B}(z) = \sum_{n=2}^{4} \frac{z^n}{n!} + \sum_{n=4}^{\infty} \frac{1}{2}(n-1)!\frac{z^n}{n!},$$

$$\bar{B}'(z) = nz + \frac{nz^2}{2} + \frac{nz^3}{6} + \frac{nz^3}{2(1-z)}. \tag{2}$$

Подставив (2) в (1), получим утверждение теоремы.

Теорема 2. *Для числа PF_n помеченных планарных полноблочно-кактусных графов с n вершинами при $n \to \infty$ верна асимптотическая формула*

$$PF_n \sim cn^{-5/2}a^n n!,$$

где $c \approx 0.1183273421$, $a \approx 4.2534965791$.

Доказательство. Используем теорему Флажоле-Седжвика [5; теорема VIII.8].

Имеем $PF_n = \frac{(n-1)!}{n}[z^n]\Big\{z\Big(\exp\Big(z + \frac{z^2}{2} + \frac{z^3}{6} + \frac{z^3}{2(1-z)}\Big)\Big)^n\Big\} =$

$$= \frac{(n-1)!}{n}F(N,n),$$

где $N = n$, $\lambda = 1$, $a(z) = z$, $b(z) = \exp\left(z + \frac{z^2}{2} + \frac{z^3}{6} + \frac{z^3}{2(1-z)}\right)$.

Очевидно, функции $a(z)$ и $b(z)$ аналитические в точке $z = 0$ и $b(0) = 1$. Функция $b(z)$ имеет положительные коэффициенты, так как $b(z) = \exp(\bar{B}(z))$ и $\bar{B}(z)$ — производящая функция для числа помеченных блоков частного вида. Поскольку $b_2 > 0, b_3 > 0$, имеем НОД$\{j|b_j > 0\} = 1$. Так как $z = 1$ — ближайшая к началу координат особая точка $b(z)$, радиус сходимости R функции $b(z)$ равен 1. Очевидно, $a(z)$ имеет бесконечный радиус сходимости. Таким образом, условия 1-3 теоремы Флажоле-Седжвика выполнены.

Найдем $T = \lim\limits_{x\to 1-0} \frac{xb'(x)}{b(x)} = \lim\limits_{x\to 1-0} \left(x + x^2 + \frac{x^3}{2} + \frac{3x^3}{2(1-x)} + \frac{x^4}{2(1-x)^2}\right) = +\infty$, $0 < \lambda < T$. Уравнение $r\frac{b'(r)}{b(r)} = \lambda$ имеет вид $r + r^2 + \frac{r^3}{2} + \frac{3r^3}{2(1-r)} + \frac{r^4}{2(1-r)^2} = 1$.

Решая это уравнение с помощью Wolfram Mathematica, получим единственный действительный корень $r \approx 0.4471957138$. Вычисляя величину $\sigma = \left(\frac{b'(r)}{b(r)}\right)' + \frac{\lambda}{r^2} = 1 + r + \frac{3r}{1-r} + \frac{3r^2}{(1-r)^2} + \frac{r^3}{(1-r)^3} + \frac{1}{r^2}$, получим $\sigma \approx 11.3671060792$. Также с помощью Wolfram Mathematica вычислим

$$c = \frac{a(r)}{r\sqrt{2\pi\sigma}} = \frac{1}{\sqrt{2\pi\sigma}} \approx 0.1183273421, \quad a = \frac{b(r)}{r} \approx 4.2534965791.$$

Окончательно при $n \to \infty$ имеем асимптотику

$$PF_n = \frac{(n-1)!}{n} F(N, n) \sim \frac{(n-1)!}{n} \frac{1}{\sqrt{2\pi\sigma}} n^{-1/2} \left(\frac{b(r)}{r}\right)^n \sim n! c n^{-5/2} a^n.$$

Доказательство закончено.

Следствие. *Почти все помеченные полноблочно-кактусные графы не являются планарными.*

Доказательство. Известно [2, теорема 3], что для числа F_n помеченных кактусов с n вершинами при $n \to \infty$ верна асимптотическая формула $F_n \sim c_1 n^{-5/2} a_1^n n!$, где $c_1 = 0.1178070871$, $a_1 = 4.261224133$. Следовательно, в силу теоремы 3 имеем

$$\lim_{n\to\infty} \frac{PF_n}{F_n} = \lim_{n\to\infty} \frac{c n^{-5/2} a^n}{c_1 n^{-5/2} a_1^n} = \lim_{n\to\infty} \frac{c}{c_1} \left(\frac{a}{a_1}\right)^n = 0,$$

то есть асимптотически почти все помеченные полноблочно-кактусные графы не являются планарными.

Список литературы

1. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977

2. Воблый В. А., Мелешко А. К. Перечисление помеченных полноблочно-кактусных графов //Дискретный анализ и исследование операций. — 2014. — Т. 21, вып. 2. — С. 24–32.

3. Воблый В. А. Об одной формуле для числа помеченных связных графов // Дискретный анализ и исследование операций. — 2012. — Т. 19, вып. 4. — С. 48–59.

4. Гульден Я., Джексон Д. Перечислительная комбинаторика. — М.: Наука, 1990.

5. Flajolet Ph., Sedgewick R., Analytic combinatorics. — Cambridge University Press, 2009.

ИЗБЫТОЧНОСТЬ КОНСТРУКТИВНЫХ ОПИСАНИЙ ГАМИЛЬТОНОВЫХ ГРАФОВ

М. А. Иорданский (Нижний Новгород)

Рассматриваются обыкновенные, конечные, неориентированные графы. Используется *конструктор* графов, содержащий потенциально бесконечный запас графов. К исходным графам, а также к графам, получаемым из них, применяются бинарные *операции склейки*. При выполнении этих операций производится отождествление изоморфных подграфов $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$ графов-операндов G_1 и G_2. Для результирующего графа G операции склейки графов G_1 и G_2 используется обозначение $G \Leftarrow (G_1 \circ G_2)\tilde{G}$, где $\tilde{G} \subseteq G$ — подграф, полученный в результате отождествления подграфов $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$, называемый *подграфом склейки* [1].

Конструктивные описания графов задаются суперпозициями операций склейки. В качестве исходных графов выбираются элементарные графы, обладающие заданным свойством. Для сохранения результирующими графами характеристического свойства на операции склейки накладывается система ограничений, включающая в себя, в общем случае, ограничения на вид отождествляемых подграфов,их выбор в графах-операндах и способ отождествления [2].

Возможность такого единообразного формулирования условий наследования различных характеристических свойств графов основывается на избыточности, вносимой операциями склейки в задание информации о графах при их конструктивных описаниях. При этом один и тот же граф может быть реализован суперпозициями, обладающими различной избыточностью.

Вершинная избыточность оценивается по формуле

$$I_v^s(G) = \frac{\sum_{i=0}^{q} |V(\tilde{G}_i)|}{|V(G)|},$$

где q — число операций склейки в суперпозиции s, реализующей граф G, $\tilde{G}_i$-подграф склейки i-й операции.

Для оценки реберной избыточности используется формула

$$I_e^s(G) = \frac{\sum_{i=0}^{q} |E(\tilde{G}_i)|}{|E(G)|}.$$

Вершинная избыточность конструктивных описаний эйлеровых графов и (r, s)-деревьев рассматривалась соответственно в работах [3, 4]. В [5] получена оценка реберной избыточности для конструктивных описаний гамильтоновых планарных графов.

В данной работе найдены оценки реберной избыточности конструктивных описаний обыкновенных гамильтоновых графов на основе трех способов, рассмотренных в [6].

Для сохранения свойства гамильтоновости на операции склейки накладываются следующие ограничения.

Лемма. *Если G_1 и G_2 — гамильтоновы графы, то граф $G \Leftarrow (G_1 \circ G_2)\tilde{G}$ также будет гамильтоновым при выполнении любого из следующих условий:*
1) *отождествляемый подграф хотя бы одного из графов-операндов содержит все его вершины;*
2) *каждый отождествляемый подграф содержит концевые вершины гамильтоновых цепей графов-операндов.*

Исходными графами являются простые циклы C_p, $p \geq 3$. Ребра произвольного гамильтонова графа G, $|V(G)| = n$, $|E(G)| = m$ разбиваются на два подмножества: ребра,принадлежащие гамильтонову циклу, и ребра-хорды, не принадлежащие гамильтонову циклу. Хордальное ребро называется *разделяющим*, если его концевые вершины образуют разделяющее множество графа G.

В первом способе синтеза сначала строятся графы $(C_{n_1} \circ C_{n_2})K_2$, $n_1 + n_2 = n$, $n_1, n_2 \geq 3$, каждый из которых реализует гамильтонов

цикл $C_n, n \geq 4$ с одной хордой. Эти графы затем склеиваются в нужном количестве по гамильтонову циклу.

Во втором способе гамильтонов цикл $C_n, n \geq 4$, последовательно склеивается с циклами $C_q, q \geq 3$, по $L_q, q \geq 3$, добавляя к текущему гамильтонову графу по одной хорде.

В третьем способе вначале с помощью операций склейки по K_2 строится n — вершинный гамильтонов граф, все хордальные ребра которого являются разделяющими. Затем полученный граф последовательно склеивается по $(L_{n'} \circ L_{n''})O_0, n', n'' \geq 2$ с циклами $C_p, p \geq 4$, добавляющими в G по две хорды, не являющиеся разделяющими в подграфе, порожденном этими хордами и гамильтоновым циклом.

В каждом методе синтеза, очевидно, используются операции, удовлетворяющие условиям леммы и, следовательно, сохраняющие гамильтоновость графов-операндов.

Пусть $\Im_n$ множество n-вершинных обыкновенных гамильтоновых графов; S_i множестве всех суперпозиций s, реализующих граф $G \in \Im_n$ с использованием i-го способа синтеза, $i \in \overline{1,3}$.

Рассматриваются функции шенноновского типа, характеризующие величину реберной избыточности:

$$\min_{s \in S_i} I_e^s(G) = I_e^i(G), \ \max_{G \in \Im_n} I_e^i(G) = I_e^i(\Im_n), \ i \in \overline{1,3}.$$

Теорема. *Справедливы неравенства*

$$I_e^1(\Im_n) < n - 1, \quad I_e^2(\Im_n) < n/2 - 1,$$

$$I_e^3(\Im_n) \preceq n/4 \quad \textit{при} \quad n \to \infty.$$

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, №4. — С. 35–63.

2. Иорданский М. А. Конструктивная классификация графов // Моделирование и анализ информационных систем. — 2012. — Т. 19, №4. — С. 144–153.

3. Иорданский М. А. Избыточность конструктивных описаний эйлеровых графов // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество. — 2014. — С. 115–116.

4. Иорданский М. А. Избыточность конструктивных описаний (r, s)-деревьев //Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20-22 мая 2015 г. — М.: МАКС Пресс, 2015. — С. 90–91.

5. Иорданский М. А. Избыточность конструктивных описаний гамильтоновых планарных графов // Мат-лы XI международного семинара «Дискретная математика и ее приложения» (МГУ, 18–22 июня 2012 г.) — М. : Изд-во механико-математического ф-та МГУ. — 2012. — С. 285–288.

6. Иорданский М. А. Конструктивные описания гамильтоновых графов //Вестник Нижегородского государственного университета. Математика. — 2012. — №3 (1). — С. 137–140.

АЛГОРИТМ ПОСТРОЕНИЯ AOE-ЦЕПИ В ПЛОСКОМ СВЯЗНОМ 4-РЕГУЛЯРНОМ ГРАФЕ

Т. А. Макаровских, А. В. Панюков (Челябинск)

Для плоского графа G далее через $E(G)$ будем обозначать множество его ребер, представляющих плоские жордановы кривые с попарно непересекающимися внутренностями, гомеоморфные отрезкам. Через $V(G)$ обозначим множество граничных точек этих кривых. Топологическое представление плоского графа $G = (V, E)$ на плоскости S с точностью до гомеоморфизма определяется заданием для каждого ребра $e \in E$ следующих функций [1]: $v_k(e)$, $k = 1, 2$ – вершины, инцидентные ребру e; $l_k(e)$, $k = 1, 2$ – ребра, полученные вращением ребра e против часовой стрелки вокруг вершины $v(k)$; $r_k(e)$, $k = 1, 2$ – ребра, полученные вращением ребра e по часовой стрелке вокруг вершины $v(k)$. Далее будем считать, что все рассматриваемые плоские графы представлены указанными функциями. Пространственная сложность такого представления будет $O(|E| \cdot \log_2 |V|)$.

Определение 1. *Графом переходов* [2] $T_G(v)$ вершины $v \in V(G)$ будем называть граф, вершинами которого являются ребра, инцидентные вершине v, т.е. $V(T_G(v)) = E_G(v)$, а множество ребер – разрешенные переходы между ребрами.

Определение 2. *Системой переходов* [3] T_G будем называть множество $\{T_G(v) \mid v \in V(G)\}$, $T_G(v)$ – граф переходов в вершине v.

Определение 3. Путь $P = v_0, e_1, v_1, ..., e_k, v_k$ в G называется T_G-*совместимым*, если $\{e_i,\ e_{i+1}\} \in E(T_G(v_i))$, $1 \le i \le k-1$.

Определение 4. Пусть для цепи $T = v_0, k_1, v_1, \ldots, k_n, v_n, v_n = v_0$ в графе $G = (V, E)$ в каждой вершине $v \in V$ задан циклический порядок $O^{\pm}(v)$, определяющий систему переходов $A_G(v) \subset O^{\pm}(v)$. В случае, когда $\forall v \in V(G)\ A_G(v) = O^{\pm}(v)$, систему переходов $A_G(v)$ будем называть *полной системой переходов*.

Определение 5. Эйлерову цепь T будем называть A-*цепью* тогда и только тогда, когда она является A_G-совместимой цепью. Таким образом, последовательные ребра в цепи T (инцидентные вершине v) являются соседями в циклическом порядке $O^{\pm}(v)$.

В работе [3] определены некоторые классы графов, для которых распознавание наличия A-цепи требует полиномиального времени.

Рассмотрим плоскость S. Пусть на ней задан плоский эйлеров граф $G = (V, E)$. Пусть f_0 – внешняя грань графа G. Для любого подмножества $H \subset S$ определим $\mathrm{Int}(H)$ как подмножество S, являющееся объединением всех связных компонент множества $S \backslash H$, не содержащих внешней грани f_0. Так, $\mathrm{Int}(G)$ будет представлять объединение всех внутренних граней графа G. Для плоского графа в качестве цикла $O^{\pm}(v)$ далее будем рассматривать соседей при вращении текущего ребра e по или против часовой стрелки относительно вершины v.

Определение 6. Будем говорить, что цикл $C = v_1 e_1 v_2 e_2 \ldots v_k$ в эйлеровом графе G имеет *упорядоченное охватывание* (является OE-цепью), если для любой его начальной части $C_i = v_1 e_1 v_2 e_2 \ldots e_i$, $i \le |E(G)|$ выполнено условие $\mathrm{Int}\,(C_i) \cap G = \emptyset$.

Определение 7. Будем говорить, что цепь является AOE-*цепью*, если она одновременно является OE-цепью и A-цепью.

Теорема 1. *Если в плоском графе G графе существует A-цепь, то существует и AOE-цепь.*

Теорема 2. *В плоском связном 4-регулярном графе G существует AOE-цепь.*

Определение 8. *Рангом ребра* $e \in E(G)$ будем называть значение функции $\mathrm{rank}(e) : E(G) \to N$, определяемую рекурсивно: пусть $E_1 = \{e \in E : e \subset f_0\}$ – множество ребер, ограничивающих внешнюю грань f_0 графа $G(V, E)$, тогда $(\forall e \in E_1)\,(\mathrm{rank}(e) = 1)$; пусть $E_k(G)$ – множество ребер ранга 1 графа $G_k \left(V, E \backslash \left(\bigcup_{l=1}^{k-1} E_l \right) \right)$,

тогда $(\forall e \in E_k)\,(\mathrm{rank}(e) = k)$.

Различные способы вычисления значений функции $\mathrm{rank}(e)$ приведены в работах [1, 4]. Вычислительная сложность определения ранга для всех ребер графа не превосходит $O(|E| \log_2 |V|)$.

Определение 9. Сураф G_k графа G, для которого $E(G_k) = \{e \in E(G) : \mathrm{rank(e)} \geq \mathrm{k}\}$ назовем *суграфом ранга* k.

Предложение 1. *Вершина, инцидентная четырем ребрам, смежным внешней грани, является точкой сочленения.*

Предложение 2. *Внешняя грань суграфа G_k является объединением всех граней ранга k в графе G.*

Из предложений 1 и 2 следует, что в любом плоском графе G можно найти точки сочленения для любого суграфа G_k, $k = 1, 2, ...$ и провести расщепление в этих вершинах таким образом, чтобы в G_k не появились новые грани. В результате получим граф, в котором любой сураф G_k не имеет точек сочленения.

Приведем описание алгоритма, который позволяет построить AOE-цепь в любом плоском связном 4-регулярном графе G, любой сураф G_k которого не имеет точек сочленения.

Алгоритм *AOE*-TRAIL. Вход: $G = (V, E)$; начальная вершина $v \in V(f_0)$. Вывод: $ATrail$ – выходной поток, содержащий построенную алгоритмом AOE-цепь.

`Initiate(`G`, `v_0`);` // Инициализация
`Ranking(`G`);` // Ранжирование
$e = \arg\max_{e \in E(v)} \mathrm{rank}(e)$; $v = v_1(e)$;
`do` {
  `if` $(v \neq v_1(e))$ REPLACE(e);
  $ATrail$ << v << e;
  $\mathrm{mark}(e) =$ `false`; counter++; $v = v_2(e)$;
  `if` $(\mathrm{rank}(r_2(e)) \geq \mathrm{rank}(l_2(e)))$ `then`
    `if` $\mathrm{mark}(r_2(e))$ `then` $e = r_2(e)$ **else** $e = l_2(e)$;
  `else if` $\mathrm{mark}(l_2(e))$ `then` $e = l_2(e)$ `else` $e = r_2(e)$;
} `while(counter` $< |E(G)|$`);`
`Stop`

Теорема 3. *Алгоритм AOE-TRAIL строит AOE-цепь в плоском связном 4-регулярном графе G за время $O(|E(G)| \cdot \log_2 |V(G)|)$.*

Список литературы

1. Панюкова Т. А. Обходы с упорядоченным охватыванием в плоских графах // Дискретный анализ и исследование операций. Сер. 2. — 2006. — Т. 13, № 2. — С. 31–43.

2. Szeider S. Finding paths in graphs avoiding forbidden transitions // Discrete Applied Mathematics. — 2003. — 126. — P. 261–273.

3. Фляйшнер Г. Эйлеровы графы и смежные вопросы. — М.: Мир, 2002.

4. Савицкий Е. А. Использование алгоритма поиска в ширину для определения уровней вложенности ребер плоского графа // Информационные технологии и системы: тр. Третьей междунар. науч. конф. / Челябинск: Изд-во ЧелГУ, 2014. — С. 43–45.

ГРАНИЧНЫЕ КЛАССЫ ГРАФОВ В ЗАМКНУТЫХ СЕМЕЙСТВАХ КЛАССОВ ГРАФОВ

Д. С. Малышев (Нижний Новгород)

В настоящей работе мы рассматриваем только *обыкновенные графы*, т. е. непомеченные неориентированные графы без петель и кратных ребер. Класс графов называется *наследственным*, если он замкнут относительно удаления вершин. Любой наследственный класс может быть задан множеством своих запрещенных порожденных подграфов. Если наследственный класс может быть задан конечным множеством запрещенных порожденных подграфов, то он называется *конечно определенным*. Помимо семейства $\mathbb{H}$ всех наследственных классов мы рассматриваем два его подсемейства. Первое из них — семейство $\mathbb{SH}$ всех *сильно наследственных* классов, т.е. классов, замкнутых относительно удаления вершин и ребер. Второе — семейство $\mathbb{M}$ всех *минорно замкнутых* классов, т.е. сильно наследственных классов, замкнутых еще и относительно стягивания ребер. Любой класс из $\mathbb{SH}$ может быть задан множеством своих запрещенных подграфов. Очевидно, что класс из $\mathbb{SH}$ может быть задан конечным множеством запрещенных подграфов тогда и только тогда, когда он является конечно определенным. Поэтому термин «конечно определенный класс» имеет в семействе $\mathbb{SH}$ такое же значение, что и в семействе $\mathbb{H}$. Согласно известной теореме Н. Робертсона и П. Сеймура [1], любой минорно замкнутый класс может быть задан конечным множеством своих запрещенных миноров.

Пусть Π — какая-либо задача на графах. Наследственный класс с полиномиально разрешимой задачей Π называется Π-*простым*. Наследственный класс с NP-полной задачей Π называется Π-*сложным*. Понятие граничного класса было введено в работе [2] применительно к задаче о независимом множестве и обобщено в работе [3] на случай произвольной задачи на графах из класса NP. Ранее это понятие рассматривалось только в рамках семейства $\mathbb{H}$. Здесь мы распространяем это понятие на другие семейства. Пусть $\mathbb{F} \in \{\mathbb{H}, \mathbb{SH}, \mathbb{M}\}$. Класс $\mathcal{X}$ называется $(\Pi, \mathbb{F})$-*предельным*, если существует такая бесконечная последовательность $\mathcal{X}_1 \supseteq \mathcal{X}_2 \supseteq \ldots$ из Π-сложных классов, каждый из которых принадлежит $\mathbb{F}$, что $\mathcal{X} = \bigcap\limits_{i=1}^{\infty} \mathcal{X}_i$. Минимальный по включению $(\Pi, \mathbb{F})$-предельный класс называется $(\Pi, \mathbb{F})$-*граничным*. Значение этого понятия раскрывает следующая теорема, которая может быть доказана точно также, как и соответствующие утверждения из [2, 3]:

Теорема 1. *Пусть* $\mathbb{F} \in \{\mathbb{H}, \mathbb{SH}\}$. *Конечно определенный класс из* $\mathbb{F}$ *является* Π-*сложным тогда и только тогда, когда он включает какой-нибудь* $(\Pi, \mathbb{F})$-*граничный класс. Минорно замкнутый класс является* Π-*сложным тогда и только тогда, когда он включает какой-нибудь* $(\Pi, \mathbb{M})$-*граничный класс.*

Таким образом, по теореме 1 знание всех граничных классов приводит к полной классификации всех конечно определенных классов (или всех минорно замкнутых) по сложности решения данной задачи. Однако, применительно к семейству $\mathbb{H}$, вопрос получения описания всех граничных классов оказывается сложным для многих задач Π, на настоящее время известен только один пример полного описания множества граничных классов [4]. В работе [5] было доказано, что для реберной задачи о 3-раскраске (задачи 3-PP) совокупность $(3\text{-PP}, \mathbb{H})$-граничных классов является континуальной, что, по-видимому, свидетельствует о принципиальной невозможности получения полного описания множества граничных классов для этой задачи. В семействе $\mathbb{SH}$ вопрос полного описания граничных классов оказывается более простым. Пусть $\mathcal{T}$ — класс всех лесов, каждая компонента связности которых имеет не более трех листьев. Для некоторых задач на графах (например, для задач НМ и ДМ о независимом и о доминирующем множествах) класс $\mathcal{T}$ является единственным граничным в семействе $\mathbb{SH}$ [2, 6]. Однако, совокупность всех $(3\text{-PP}, \mathbb{SH})$-граничных классов остается континуальной [6]. Из теоремы Робертсона—Сеймура следует, что для любой задачи Π множество всех $(\Pi, \mathbb{M})$-граничных классов является не более чем счетным.

Множество планарных графов $\mathcal{P}lanar$ для семейства $\mathbb{M}$ является аналогом класса $\mathcal{T}$ для семейства $\mathbb{SH}$. Именно, для многих задач на графах (например, для задач НМ и ДМ) класс $\mathcal{P}lanar$ является единственным граничным в семействе $\mathbb{M}$ [6].

Было бы интересным найти такие классическую задачу на графах П и (П, $\mathbb{M}$)-граничный класс, что не известны ни (П, $\mathbb{H}$)-граничные, ни (П, $\mathbb{SH}$)-граничные классы. *Нумерацией графа* G называется произвольное инъективное отображение $f_G : V(G) \longrightarrow \overline{1, |V(G)|}$. *Ленточной шириной графа* G называется число $b(G) = \min \max_{(u,v)\in E(G)} |f_G(u) - f_G(v)|$, где минимум берется по всевозможным нумерациям f_G графа G. *Задача о ленточной ширине графа* (кратко, *задача ЛШ*) для заданного графа G состоит в вычислении $b(G)$. *Задача ЛШ*$_{+2}$ для заданного графа G состоит в вычислении такого числа $p(G)$, что $b(G) \leq p(G) \leq b(G) + 2$. Задача ЛШ — классическая NP-трудная задача на графах, задача ЛШ$_{+2}$ также NP-трудна. *Циклическая 1-гусеница* — граф, получаемый добавлением к простому циклу попарно несмежных вершин (возможно, ни одной), каждая из которых смежна ровно с одной из вершин цикла. Минорное замыкание множества всех циклических 1-гусениц обозначается через 1-$\mathcal{C}Caterpillar$.

Теорема 2. *Класс* 1-$\mathcal{C}Caterpillar$ *является* (*ЛШ*$_{+2}$, $\mathbb{M}$)*-граничным.*

Отметим, что на настоящее время для задач ЛШ и ЛШ$_{+2}$ в семействах $\mathbb{H}$ и $\mathbb{SH}$ граничные классы не известны.

Работа выполнена при финансовой поддержке РФФИ (проект 16-31-60008-мол-а-дк), гранта Президента РФ МК-4819.2016.1, лаборатории алгоритмов и технологий анализа сетевых структур, Национальный исследовательский университет «Высшая школа экономики».

Список литературы

1. Robertson N., Seymour P. Graph minors XX: Wagner's conjecture // Journal of Combinatorial Theory, Series B. — 2004. — V. 92, No 2. — P. 325–357.

2. Alekseev V. E. On easy and hard hereditary classes of graphs with respect to the independent set problem // Discrete Applied Mathematics. — 2003. — V. 132, No. 1–3. — P. 17–26.

3. Alekseev V. E., Boliac R., Korobitsyn D. V., Lozin V. V. NP-hard graph problems and boundary classes of graphs // Theoretical Computer Science. — 2007. — V. 389, No 1–2. — P. 219–236.

4. Малышев Д. С. Критические классы графов для задачи о реберном списковом ранжировании // Дискретный анализ и исследование операций. — 2013. — Т. 20, вып. 6. — С. 59–76.

5. Малышев Д. С. Континуальные множества граничных классов графов для задач о раскраске // Дискретный анализ и исследование операций. — 2009. — Т. 16, вып. 5. — С. 41–51.

6. Малышев Д. С. Критические элементы в комбинаторно замкнутых семействах классов графов // Дискретный анализ и исследование операций. — 2016 (направлено в журнал).

О ДИФФЕРЕНЦИАЦИИ ГРАФОВ НА ОСНОВЕ БЫСТРО ВЫЧИСЛЯЕМЫХ ИНВАРИАНТОВ

Б. Ф. Мельников, Н. П. Чурикова (Самара)

Настоящая статья посвящена некоторым частным вопросам, связанным с проблемой построения алгоритмов определения (не) изоморфности двух заданных графов. После нескольких десятилетий работы над данной проблемой многих научных групп недавно (в самом конце 2015 г.) было объявлено об окончании разработки квазиполиномиального (псевдо-полиномиально-временно́го) алгоритма; однако стоит отметить, что публикаций этого алгоритма пока не появилось, вся информация пока ограничивается научно-популярными сайтами вроде [1] с примерно следующим текстом:

> Математик Ласло Бабай из Чикагского университета в США разработал теоретический алгоритм, позволяющий существенно ускорить сравнение графов друг с другом ... Бабай изложил основные моменты своей работы в двух лекциях, а присутствующие на них эксперты в области теории графов пока не нашли ошибок в рассуждениях ученого. Между тем окончательной верификации в математическом сообществе его работа пока не получила.

Итак, информации о возможности практического применения данного алгоритма пока нет. На практике применяются более простые процедуры, от которых ожидается хорошая работа в большинстве случаев. Например, используются эвристики для доказательства, что два графа не изоморфны ([2] и многие другие). Для этого используют различные инварианты, и, как только обнаруживаются два различных значения одного и того же инварианта, приходят к заключению, что графы не изоморфны. В [2] одним из авторов настоящей статьи был предложен один из вариантов проверки двух заданных графов на неизоморфность — а именно, эвристический алгоритм определения конкретной последовательности поверки инвариантов.

В настоящей работе кратко описывается решение одной из задач, необходимых для осуществления этого подхода. Мы рассматриваем два инварианта, для которых ранее были неизвестны такие примеры графов, для которых эти инварианты дают разную дифференциацию (т. е. когда *ровно один* из этих инвариантов показывает их неизоморфность). А именно, мы, во-первых, рассматриваем индекс Рандича — величину

$$\sum_{(v_i,v_j)\in E} \frac{1}{\sqrt{d(v_i)d(v_j)}},$$

где v_i и v_j — две вершины, образующие ребро множества E. Во-вторых, мы также рассматриваем вектор степеней 2-го порядка, определённый и исследованный в [2]. (При этом важно отметить, что, согласно доступной об алгоритме Бабая информации, в этом алгоритме, по-видимому, используются аналогичные инварианты.)

Эвристические алгоритмы, работавшие со случайно сгенерированными графами, содержащими по 10 вершин, не дали ни одного примера, для которых упомянутые нами инварианты дают разную дифференциацию. Однако нами найден пример (по-видимому, ранее подобных примеров опубликовано не было), когда разную дифференциацию для упомянутых нами инвариантов дают два графа, содержащие по 12 вершин; приведём этот пример.

Для графа G_1 матрица смежности следующая:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

При этом приближённое значение индекса Рандича графа G_1 есть 5.79870219113. Вектор степеней второго порядка сначала запишем по порядку вершин графа:

$$[[3,5,7,3],[4,7,3],[4,5,7,5,3],[4,5,3,7,5,3,4],[4,7,7],[3,7,3,3,5,3,4],$$
$$[3,7,5],[5,5,5],[4,5,3,7,3],[4,5,7,3,3],[5,7,7],[5,5,7,7]],$$

после чего проведём сортировку [2]:

$$[[7,5,5,4,4,3,3],[7,5,4,3,3,3,3],[7,5,5,4,3],[7,5,4,3,3],[7,5,4,3,3],$$
$$[7,7,5,5],[7,5,3,3],[7,7,5],[7,7,4],[7,5,3],[7,4,3],[5,5,5]].$$

Для графа G_2 матрица смежности следующая:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

При этом значение индекса Рандича *в точности совпадает* с вычисленным для графа. Вектор степеней второго порядка сразу запишем в отсортированном виде:

$$[[7,5,5,4,3,3,3],[7,5,4,4,3,3,3],[7,5,5,4,3],[7,5,4,3,3],[7,5,4,3,3],$$
$$[7,7,5,3],[7,5,5,3],[7,7,5],[7,5,5],[7,7,3],[7,4,3],[5,5,4]].$$

Как мы видим, он не совпадает с аналогичным вектором графа G_1.

Подробное описание эвристических алгоритмов получения подобных пар графов мы приведём в следующей публикации.

Список литературы

1. Graph-theory breakthrough tantalizes mathematicians // Электронный ресурс: `http://www.nature.com/news/graph-theory-breakthrough-tantalizes-mathematicians-1.18801` (дата публикации 19.11.2015, дата обращения 17.04.2016).

2. Мельников Б. Ф., Сайфуллина Е. Ф. Применение мультиэвристического подхода для случайной генерации графа с заданным вектором степеней // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2013. — № 3 (27). — С. 70–83.

О РАВЕНСТВЕ ЧИСЕЛ УПАКОВКИ И ПОКРЫТИЯ ОТНОСИТЕЛЬНО P_4 В РАСЩЕПЛЯЕМЫХ ГРАФАХ И ИХ РАСШИРЕНИЯХ

Д. Б. Мокеев (Нижний Новгород)

В статье используются традиционные обозначения для простых путей, циклов и полных графов: P_n, C_n, K_n.

Пусть $\mathcal{X}$ — множество графов. Множество попарно непересекающихся порождённых подграфов графа G, изоморфных графам из $\mathcal{X}$, называется $\mathcal{X}$-*упаковкой* G. Множество вершин графа G, покрывающее все порождённые подграфы графа G, изоморфные графам из $\mathcal{X}$, называется $\mathcal{X}$-*покрытием*. Граф называется *кёниговым* относительно $\mathcal{X}$, если в любом его порождённом подграфе наибольшая мощность $\mathcal{X}$-упаковки равна наименьшей мощности $\mathcal{X}$-покрытия [1]. Класс всех кёниговых графов относительно множества $\mathcal{X}$ обозначаем через $\mathcal{K}(\mathcal{X})$. Если множество $\mathcal{X}$ состоит из единственного графа H, то будем говорить об H-упаковках, H-покрытиях и кёниговых графах относительно H.

Класс $\mathcal{K}(\mathcal{X})$ при любом $\mathcal{X}$ является наследственным и, следовательно, может быть описан множеством запрещенных графов (минимальных по отношению «быть порожденным подграфом» графов, не принадлежащих $\mathcal{X}$). Для P_2 такую характеризацию даёт теорема Кёнига вместе с известным критерием двудольности. Кроме этой

классической теоремы автору известны следующие результаты такого рода для обыкновенных графов: в [2] описаны все запрещённые подграфы для класса $\mathcal{K}(\mathcal{C})$, где $\mathcal{C}$ — множество всех простых циклов, в [1, 3] описаны все запрещённые подграфы для классов $\mathcal{K}(P_3)$ и $\mathcal{K}(\{P_3, C_3\})$, а также дано конструктивное описание обоих классов. В [4] описано несколько семейств запрещённых графов для класса $\mathcal{K}(P_4)$ и высказано предположение, что объединение этих семейств образует полное множество запрещенных графов для данного класса.

Граф называется расщепляемым, если существует разбиение множества его вершин на клику и независимое множество. Класс расщепляемых графов также является наследственным. Множество его минимальных запрещённых подграфов составляют $2P_2$, C_4 и P_5.

Цель настоящей работы — дать описание пересечения класса $\mathcal{K}(P_4)$ с классом графов, полученных из расщепляемых с помощью замены вершин кографами. Даётся описание множества минимальных запрещённых графов для этого класса, а так же его структурная характеризация.

Далее порождённый подграф, изоморфный P_4 будем называть *квартетом*.

Обозначим $V(G)$ множество вершин графа G. Окрестность вершины v будем обозначать $N(v)$.

Кографом называется граф, не содержащий квартетов.

Определение. Операция *замены графом H вершины x* состоит в том, что эта вершина удаляется из графа, к графу добавляется несколько новых вершин, соединённых между собой так, что они порождают подграф, изоморфный H. Каждая новая вершина соединена ребром со всеми вершинами $N(x)$ в исходном графе.

Определение. Будем говорить, что граф G является *расширением* графа H, если он может быть получен из H заменой некоторых его вершин произвольными кографами.

Граф *rising sun* — это расщепляемый граф, клика которого состоит из 4 вершин, а независимое множество — из 3 вершин. Каждая вершина независимого множества смежна ровно с двумя вершинами клики. Две вершины клики имеют степень 4, а остальные две имеют степень 5. Граф *co-rising sun* является дополнением графа *rising sun*.

Граф *net* — это расщепляемый граф, клика и независимое множество которого состоят из 3 вершин. Каждая вершина клики смежна ровно с одной вершиной независимого множества, каждая вершина независимого множества смежна ровно с одной вершиной клики. Граф S_3 является дополнением графа *net*.

Граф A получен из графа C_4 добавлением двух несмежных вершин. Каждая из них смежна с одной вершиной цикла, причём вершины их окрестностей являются смежными. Граф *co-A* является дополнением A.

Граф *parapluie* получен из графа P_4 заменой одной из его вершин степени 2 графом P_4. Граф *parachute* является дополнением графа *parapluie*.

Определение. Пусть H — расщепляемый граф со следующими свойствами:
1) $V(G) = K_1 \cup K_2 \cup L_1 \cup L_2$;
2) $K_1 \cup K_2$ формирует клику в G, а $L_1 \cup L_2$ является независимым множеством G;
3) для любого $t \in \{1, 2\}$ для любых $x, y \in K_t$ выполняется $N(x) \subseteq N(y)$ или $N(y) \subseteq N(x)$;
4) для любого $t \in \{1, 2\}$ для любых $x, y \in L_t$ выполняется $N(x) \subseteq N(y)$ или $N(y) \subseteq N(x)$.

Будем называть такой граф зеркально-расщепляемым.

Теорема. *Следующие утверждения равносильны для связного графа G:*
1) *G является расширением некоторого зеркально-расщепляемого графа;*
2) *G является расширением расщепляемого графа, не содержащего порождённых подграфов rising sun, co-rising sun, S_3, net;*
3) *G не содержит порождённых подграфов C_5, P_5, $\overline{P_5}$, rising sun, co-rising sun, S_3, net, A, co-A, parapluie, parachute, $2P_4$, $\overline{2P_4}$;*
4) *G принадлежит множеству $\mathcal{K}(P_4)$ и является расширением расщепляемого графа.*

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 16-31-00109-мола, 16-01-00599-а), гранта Президента РФ МК-4819.2016.1 и Лаборатории алгоритмов и технологий анализа сетевых структур НИУ ВШЭ, грант правительства РФ (договор 11.G34.31.0057).

Список литературы

1. Алексеев В. Е., Мокеев Д. Б. Кёниговы графы относительно 3-пути // Дискретный анализ и исследование операций. — 2012. — Т. 19, вып. 4. — С. 3–14.

2. Ding G., Xu Z., Zang W. Packing cycles in graphs II // Journal of Combinatorial Theory. Ser. B. — 2003. — Vol. 87. — P. 244–253.

3. Alekseev V. E., Mokeev D. B. König graphs for 3-paths and 3-cycles // Discrete Applied Mathematics. — 2016. — Vol. 204. — P. 1–5.

4. Mokeev D. König Graphs for 4-paths // Models, Algorithms and Technologies for Network Analysis. — 2014. — P. 93–103.

ОБ ОДНОМ ТЕОРЕТИКО-ГИПЕРГРАФОВОМ ПОДХОДЕ РЕШЕНИЯ ЗАДАЧИ О КЛИКАХ

В. А. Перепелица (Запорожье), Д. А. Тамбиева (Черкесск)

Известно, что задача о покрытии графа кликами относится к классу NP-полных (NP-трудных) задач [1]. В этой связи ее решения в научных публикациях ограничивается статистически эффективными и асимптотически точными алгоритмами. В настоящей работе предлагается алгоритм α выделения множества допустимых решений покрытия графа типовыми подграфами различной конфигурации, базирующийся на методологии теории гиперграфов. Для описания обобщенной математической модели указанной задачи используем термин «функциональная единица», под которой понимаем минимальную значимую единицу соответствующую подструктуре некоторой сложной системы.

В структуре системы имеется n функциональных единиц. В теоретико-графовой модели рассматриваемой задачи строим граф $G = (V,\ E)$, в котором $V = \{v_1, v_2,\ ...,\ v_n\}$ — множество вершин, каждая вершина v_i, $i = 1,\ 2,\ ...,\ n$ взаимнооднозначно соответствует i-ой функциональной единице, а $E = \{e_{ij}\}$, $(i,\ j = 1,\ 2,\ ...,\ n)$ — множество ребер, где наличие ребра $e_{ij} = (v_i,\ v_j) \in E$ соответствует вертикальным и/или горизонтальным связям системы между i-ой и j-ой функциональными единицами. Требуется выделить множество допустимых решений покрытия графа $G = (V,\ E)$ типовыми подграфами заданной конфигурации.

Рассмотрим указанный алгоритм для решения задачи покрытия графа 3-кликами (трисочетаниями).

На первом шаге алгоритма осуществляется переход от исходного графа $G = (V,\ E)$ к гиперграфу $H\,(W,\ I)$, на базе которого проводятся все дальнейшие вычисления.

Принцип построения гиперграфа $H\,(W,\ I)$ следующий: вершины графа $G = (V,\ E)$, соответствующие типовому подграфу заданной конфигурации, стягиваются в одну гипервершину гиперграфа

$H(W,\, I)$. Ребро гиперграфа $H(W,\, I)$ строится между двумя гипервершинами в том случае, если пересечение множеств вершин графа $G = (V,\ E)$ образующих эти гипервершины гиперграфа $H(W,\, I)$ пусто.

Условимся, что множество вершин $V = \{v\}$ представляет собой множество натуральных чисел $v = 1,\, 2,\, ...,\, i,\, ...,\, n$. Тогда гипервершины $w \in W$ представляют собой упорядоченные (по возрастанию) тройки $w = (v_1,\, v_2,\, v_3)$, где $v_1 < v_2 < v_3$. Упорядочив множество W этих троек лексикографически, получим последовательность (упорядоченное множество)

$$W = \{w_1,\, w_2,\, ...,\, w_\mu,\, ...,\, w_M\}\,,\ M = |W|\,. \tag{1}$$

Последовательность (1) разбиваем на подпоследовательности $W_1, W_2, ..., W_l, ..., W_L$ следующим образом. Сначала рассмотрим последовательность

$$\left\{v_1^1,\, v_1^2,\, ...,\, v_1^\mu,\, ...,\, v_1^M\right\} \tag{2}$$

первых компонент v_1^μ в гипервершинах $w_\mu = (v_1^\mu,\, v_2^\mu,\, v_3^\mu)$ последовательности (1), т.е. между элементами упорядоченных последовательностей (1) и (2) существует взаимнооднозначное соответствие. Далее заметим, что последовательность (2) состоит из подпоследовательностей одинаковых по значению элементов. Выбрав из каждой такой подпоследовательности по одному представителю, получим упорядоченную по возрастанию последовательность, состоящую из этих представителей:

$$\bar{V} = \{1,\, i_2,\, ...,\, i_l,\, ...,\, i_L\}\,. \tag{3}$$

С учетом обозначения $i_1 = 1$, ряд чисел (3) определяет собой разбиение последовательности (1) на подпоследовательности

$$W_l = \left\{w_\mu = (v_1^\mu,\, v_2^\mu,\, v_3^\mu) : v_1^\mu = i_l,\ i_l \in \bar{V}\right\},\ l = 1,\, L.$$

Этот процесс заканчивается тогда, когда сформируется такая доля W_L, на которой полностью исчерпывается множество гипервершин W, т.е. является пустым подмножество $W \setminus (W_1 \cup W_2 \cup ... \cup W_L) = \emptyset$.

Результат построения гиперграфа $H(W,\, I)$ представляется в виде матрицы смежности A^1 гипервершин $w \in W$.

На втором шаге реализуется специальная процедура отсеивания неперспективных гипервершин, суть которой на первом шаге итерации определяется тем свойством, что всякая гипервершина $w \in W_\chi$, принадлежащая допустимому решению имеет степень $\deg w = n_0 - 1$,

где $n_0 = n/3$. Поэтому если общее количество входящих и исходящих дуг оказывается меньшим, чем приведенная выше оценка, то такую гипервершину будем считать «неперспективной» и «вычеркивается» из матрицы A^1. Последующие шаги процедуры отсеивания предполагает последовательное удаление всех «неперспективных» гипервершин и реализуется на базе матриц преобразования: A^i, B^i, C^i, где i=1, ..., t – шаг итерации.

Последовательность шагов алгоритма α:

$$G(V,E) \to H(W,I) \to \underbrace{A^1 \to B^1 \to C^1}_{1\text{-}я\ итерация} \to \ldots \to$$

$$\to \underbrace{A^{(t-1)} \to B^{(t-1)} \to C^{(t-1)}}_{(t-1)\text{-}я\ итерация} \to \underbrace{A^{(t)} \to B^{(t)} \to C^{(t)}}_{t\text{-}я\ итерация}, \ldots$$

Если $C^{(t-1)} = C^t$, то достигли неподвижной точки, соответствующей множеству допустимых решений задачи о покрытии графа трисочетаниями.

Лемма 1. *Если данный граф содержит единственное допустимое решение, то алгоритм α гарантирует нахождение неподвижной точки размерности n_0, однозначно определяющей это решение. Трудоемкость нахождения допустимого решения в этом случае ограничена сверху полиномом от n.*

Лемма 2. *При выполнении условий леммы 1 на каждой итерации (кроме последней) удаляется хотя бы одно ребро или вершина соответствующего гиперграфа.*

Лемма 3. *Если исходный граф полный, то начальная матрица A^1 представляет собой неподвижную точку.*

Лемма 4. *Если в исходном графе некоторый треугольник принадлежит хотя бы одному допустимому решению, то соответствующая ему гипервершина не будет удалена ни на какой итерации.*

Лемма 5. *Для всякого исходного графа неподвижная точка достигается алгоритмом не более чем за полиномиальное число итераций.*

Лемма 6. *Нижняя оценка размерности неподвижной точки является полином порядка $O\left(n^3\right)$.*

Пусть m — размерность матрицы A^1, тогда с учетом леммы 2 справедлива

Лемма 7. *Для всякой матрицы A^1 количество итераций для достижения неподвижной точки задачи о трисочетаниях не превосходит $O(n^9)$.*

Отметим, что подробное описание алгоритма α и доказательства представленных лемм можно найти в [2].

Список литературы:

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

2. Перепелица В. А., Тамбиева Д. А. Системы с иерархической структурой управления: разработка экономико–математических и инструментальных методов. — М.: Финансы и статистика, 2009.

БУЛЕВО-МАТРИЧНЫЕ ИДЕМПОТЕНТЫ

В. Б. Поплавский (Саратов)

Пусть $\langle \mathbf{B}_{m\times n}, \cup, \cap, ', O, I\rangle$ есть булева алгебра $m \times n$ матриц с элементами из некоторой булевой алгебры $\langle \mathbf{B}, \cup, \cap, ', 0, 1\rangle$. Операции объединения $\cup$, пересечения $\cap$, дополнения $'$ и, следовательно, отношение частичного порядка $\subseteq$ определяются для матриц поэлементно. Матрицы O и I, образованные целиком из нулей 0 и единиц 1 соответственно, дают нуль и единицу такой вторичной булевой алгебры.

Матрицу $C = A \sqcap B \in \mathbf{B}_{m\times k}$ с элементами $C^i_j = \bigcup_{t=1}^{n}(A^i_t \cap B^t_j)$ назовём *конъюнктным произведением* матриц согласованных размеров $A = (A^i_j) \in \mathbf{B}_{m\times n}$ и $B = (B^i_j) \in \mathbf{B}_{n\times k}$. *Дизъюнктное произведение* $A \sqcup B$ определяется дуальным образом: $A \sqcup B = (A' \sqcap B')'$.

Рассмотрим $\mathbf{M}^n(\mathbf{B}) = \bigcup_{m,n\in\langle 1,..,n\rangle} \mathbf{B}_{m\times n}$ - множество булевых матриц всевозможных размеров, начиная с 1×1 по $n \times n$. Пары $\langle \mathbf{M}^n(\mathbf{B}), \sqcap\rangle$ и $\langle \mathbf{M}^n(\mathbf{B}), \sqcup\rangle$ образуют частичные полугруппы относительно частичных, то есть определенных не для каждых пар матриц, бинарных операций. При этом неравенство $A \subseteq B$ влечёт $A \sqcap C \subseteq B \sqcap C$, $C \sqcap A \subseteq C \sqcap B$ и $A \sqcup C \subseteq B \sqcup C$, $C \sqcup A \subseteq C \sqcup B$. Дополнение булевых матриц , в силу равенств $(A \sqcap B)' = A' \sqcup B'$ и $(A \sqcup B)' = A' \sqcap B'$, является изоморфизмом частичных полугрупп $\langle \mathbf{M}^n(\mathbf{B}), \sqcap\rangle$ и $\langle \mathbf{M}^n(\mathbf{B}), \sqcup\rangle$.

Пусть A^T означает транспонирование матрицы A. Заметим, что $(A \sqcap B)^T = B^T \sqcap A^T$ и $(A \sqcup B)^T = B^T \sqcup A^T$. Здесь и далее полагаем, что $A'^T = (A^T)' = (A')^T$.

Символом E будем далее обозначать квадратные единичные матрицы с единицами на главной диагонали и нулями на остальных местах. При этом соответствующий контексту размер матрицы E указывать не будем.

Определение 1. Матрица A называется *первичным* $\sqcap$-*идемпотентом*, если $E \nsubseteq A = A \sqcap A$, и *вторичным* $\sqcap$-*идемпотентом* частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, если $E \subseteq A = A \sqcap A$.

Для частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcup \rangle$ первичные и вторичные $\sqcup$-идемпотенты определяются дуальным образом, то есть матрица $A = A \sqcup A$ называется *первичным* $\sqcup$-*идемпотентом*, если $A \nsubseteq E'$, и *вторичным* $\sqcup$-*идемпотентом*, если $A \subseteq E'$.

Любая булева матрица произвольного размера порождает *вторичные идемпотенты правого типа*: $A^{\mathcal{R}} = A \sqcup A'^T$, $A_{\mathcal{R}} = (A^{\mathcal{R}})'^T = A \sqcap A'^T$ и *левого типа*: $A^{\mathcal{L}} = A'^T \sqcup A$, $A_{\mathcal{L}} = (A^{\mathcal{L}})'^T = A'^T \sqcap A$. Причём матрицы $A^{\mathcal{R}}$ и $A^{\mathcal{L}}$ являются вторичными $\sqcap$-идемпотентами, а $A_{\mathcal{R}}$ и $A_{\mathcal{L}}$ являются вторичными $\sqcup$-идемпотентами [1, 2].

Теорема 1. *Пусть A — идемпотент частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$. Матрица A является первичным $\sqcap$-идемпотентом тогда и только тогда, когда $A \subsetneqq A^{\mathcal{R}}$ и $A \subsetneqq A^{\mathcal{L}}$, и является вторичным $\sqcap$-идемпотентом тогда и только тогда $A = A^{\mathcal{R}} = A^{\mathcal{L}}$.*

Теорема 2. *Если матрицы A и B порождают один и тот же правый главный идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$ (или полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcup \rangle$) то $A^{\mathcal{R}} = B^{\mathcal{R}}$, что равносильно равенству $A_{\mathcal{R}} = B_{\mathcal{R}}$. Если матрицы A и B порождают левый идеал, то это влечет совпадение вторичных идемпотентов левого типа: $A^{\mathcal{L}} = B^{\mathcal{L}}$, $A_{\mathcal{L}} = B_{\mathcal{L}}$.*

Следующие равенства указывают свойства вторичных идемпотентов.

$$A^{\mathcal{L}} = (A_{\mathcal{L}})'^T = (A'^T)^{\mathcal{R}}) = A^{\mathcal{L}} \sqcup A_{\mathcal{L}} = A_{\mathcal{L}} \sqcup A^{\mathcal{L}} =$$
$$= (A^{\mathcal{L}})^{\mathcal{L}} = (A^{\mathcal{L}})^{\mathcal{R}} = (A_{\mathcal{L}})^{\mathcal{L}} = (A_{\mathcal{L}})^{\mathcal{R}},$$
$$A^{\mathcal{R}} = (A_{\mathcal{R}})'^T = (A'^T)^{\mathcal{L}}) = A^{\mathcal{R}} \sqcup A_{\mathcal{R}} = A_{\mathcal{R}} \sqcup A^{\mathcal{R}} =$$
$$= (A^{\mathcal{R}})^{\mathcal{R}} = (A^{\mathcal{R}})^{\mathcal{L}} = (A_{\mathcal{R}})^{\mathcal{R}} = (A_{\mathcal{R}})^{\mathcal{L}}.$$

Свойства $A_{\mathcal{L}}$ и $A_{\mathcal{R}}$ записываются аналогично двойственным образом.

Известно, что вторичные идемпотенты играют главную роль в вопросах разрешимости простейших матричных уравнений, делимости, регулярности матриц, порождаемости односторонних идеалов, поиска транзитивно-рефлексивных замыканий и пр. [1, 2].

Частичная полугруппа $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$ разбивается на непересекающиеся $\mathbf{D}$-классы Грина двусторонних идеалов. В следующем утверждении обсуждается взаимное расположение вторичных $\sqcap$- и $\sqcup$-идемпотентов в двусторонних идеалах ($\mathbf{D}$-классах) частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$.

Теорема 3. *Пусть $A_{\mathcal{L}}$ и $A^{\mathcal{L}}$ порождают один и тот же двусторонний идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, тогда матрицы A и A'^T порождают тот же двусторонний идеал. Причём,если $A_{\mathcal{L}}$ и $A^{\mathcal{L}}$ порождают один и тот же левый идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, то матрица A порождает тот же левый идеал идеал, и, если $A_{\mathcal{L}}$ и $A^{\mathcal{L}}$ порождают один и тот же правый идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, то матрица A'^T порождает тот же правый идеал.*

Аналогичное утверждение можно сформулировать для $A_{\mathcal{R}}$ и $A^{\mathcal{R}}$, меняя местами слова "левый"и "правый".

Заметим, что, учитывая теорему 2, в каждом левом или правом идеале частичной полугруппе $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$ может находиться только один вторичный $\sqcap$-идемпотент, либо $\sqcup$-идемпотент.

Вторичные $\sqcap$- и $\sqcup$-идемпотенты располагаются достаточно "плотно"в множестве $\mathbf{M}^n(\mathbf{B})$. Так каждый левый или правый идеал частичной полугруппы $\langle \mathbf{M}^3(\{0,1\}), \sqcap \rangle$ порождается либо вторичным $\sqcap$-идемпотентом, либо вторичным $\sqcup$-идемпотентом. Это означает , что любая матрица $\{0,1\}$-матрица (размера с 1×1 по 3×3) может только лишь "элементарными"преобразованиями строк (или столбцов) быть приведена либо к $\sqcap$-идемпотентной матрице с единицами на главной диагонали, либо к $\sqcup$-идемпотентной матрице с нулями на главной диагонали.

Список литературы

1. Поплавский В. Б. О приложениях ассоциативности дуальных произведений алгебры булевых матриц // Фундаментальная и прикладная математика. — 2011/2012. — Т. 17, вып. 4. — С. 181–192.

2. Поплавский В. Б. Об идемпотентах алгебры булевых матриц // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. — 2012. — Т. 12, вып. 2. — С. 26–33.

О ТРАНЗИЕНТНЫХ ВЗВЕШИВАНИЯХ БЕСКОНЕЧНЫХ СИЛЬНО СВЯЗНЫХ ОРГРАФОВ

С. В. Савченко (Черноголовка)

Пусть $\mathcal{D}$ — счетный орграф и w — его *взвешивание*, т.е. положительная функция на его дугах. Для *взвешенного орграфа* $(\mathcal{D}, w)$ обозначим через $A_w(\mathcal{D})$ его *весовую матрицу смежности*. По определению $A_w(\mathcal{D})(u, v) = w(u, v)$, если (u, v) — дуга в $\mathcal{D}$, и $A_w(\mathcal{D})(u, v) = 0$ в противном случае. Таким образом, если w тождественно равно 1 на дугах $\mathcal{D}$, то $A_w(\mathcal{D})$ совпадает с обычной матрицей смежности орграфа $\mathcal{D}$. Определим ее *"внутренний"спектральный радиус* $\lambda(\mathcal{D}, w)$ как супремум спектральных радиусов конечных главных подматриц в $A_w(\mathcal{D})$ (или, то же самое, весовых матриц смежности конечных взвешенных подорграфов в $(\mathcal{D}, w)$). Мы будем рассматривать только случай, когда $\lambda(\mathcal{D}, w) < \infty$. Тогда, очевидно, будет конечен и супремум $\lambda^{(n)}(\mathcal{D}, w)$ спектральных радиусов главных подматриц порядка n в $A_w(\mathcal{D})$ (или, то же самое, весовых матриц смежности взвешенных подорграфов порядка n в $(\mathcal{D}, w)$). Очевидно, последовательность $\lambda^{(n)}(\mathcal{D}, w)$ не убывает (по n) и сходится к $\lambda(\mathcal{D}, w)$. В работе исследуется поведение величины

$$\Delta^{(n)}(\mathcal{D}, w) = n\big(\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w)\big)$$

и даются ответы на некоторые вопросы, впервые поставленные в [1].

В дальнейшем мы всегда будем считать, что исходный орграф $\mathcal{D}$ является *сильно связным*. В этом случае он содержит по крайней мере один (ориентированный) *цикл* (т.е. сильно связный подорграф, из каждой вершины которого выходит ровно одна дуга) и, следовательно, $\lambda(\mathcal{D}, w) > 0$ для любого взвешивания w, определенного на $\mathcal{D}$. Мы скажем, что множество W вершин в $\mathcal{D}$ является *цикловой трансверсалью*, если орграф $\mathcal{D} - W$ (полученный удалением всех вершин подмножества W из $\mathcal{D}$ вместе с инцидентными им дугами) вообще не имеет никаких циклов.

Взвешивание w назовем *транзиентным*, если бесконечный ряд $\sum\limits_{m=0}^{\infty} A_w^m(\mathcal{D})\lambda(\mathcal{D}, w)^{-m}$ сходится (поэлементно). Множество всех таких взвешиваний орграфа $\mathcal{D}$ обозначим через $\mathcal{T}(\mathcal{D})$. Если ряд расходится, то взвешивание w называется *рекуррентным*. Для конечного орграфа любое его взвешивание рекуррентно. Таким образом, транзиентность w означает, что взвешенный орграф $(\mathcal{D}, w)$ далек по своим рекуррентным (аналитическим) свойствам от конечного

случая. Можно было бы ожидать, что при $w \in \mathcal{T}(\mathcal{D})$ разность $\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w)$ убывает к нулю достаточно медленно. Однако, оказывается, что в классе $\mathcal{T}(\mathcal{D})$ для величины $\Delta^{(n)}(\mathcal{D}, w)$ всегда справедлива следующая альтернатива.

Теорема 1. *При фиксированном $\mathcal{D}$ или для любой положительной функции $g(n)$ найдется взвешивание $w \in \mathcal{T}(\mathcal{D})$ такое, что $\Delta^{(n)}(\mathcal{D}, w) < g(n)$ при каждом $n \geq 1$, или для любого $w \in \mathcal{T}(\mathcal{D})$ существует положительная константа c_w, независящая от n, такая, что $\Delta^{(n)}(\mathcal{D}, w) > c_w$. Последняя альтернатива имеет место тогда и только тогда, когда $\mathcal{D}$ допускает конечную цикловую трансверсаль.*

Заметим, что во втором случае мы также неявно считаем, что орграф $\mathcal{D}$ содержит цикл какой угодно большой длины: иначе в силу теоремы Ван Кира, доказанной в [2], множество $\mathcal{T}(\mathcal{D})$ пусто и, следовательно, и говорить не о чем. Пока мы не в состоянии доказать, что для любого $\mathcal{D}$ с конечной цикловой трансверсалью существует $w \in \mathcal{T}(\mathcal{D})$ такое, что $\Delta^{(n)}(\mathcal{D}, w) < C_w$ при некоторой $C_w > 0$. Однако, можно довольно просто показать, что для любой положительной функции $g(n)$ с $\limsup g(n) = \infty$ всегда найдутся $\mathcal{D}$, все циклы которого проходят через одну вершину, и $w \in \mathcal{T}(\mathcal{D})$ такие, что $\Delta^{(n)}(\mathcal{D}, w) < g(n)$ при бесконечно многих n. Это, в частности, показывает, что для справедливости теоремы 1 множитель n в $\Delta^n(\mathcal{D}, w)$ нельзя, вообще говоря, заменить на n^α, где $0 < \alpha < 1$.

В силу теоремы 1 только при наличии конечной цикловой трансверсали у $\mathcal{D}$ мы можем всегда быть уверенными в том, что достаточно быстрая сходимость $\lambda^{(n)}(\mathcal{D}, w)$ к $\lambda(\mathcal{D}, w)$ влечет хорошие рекуррентные свойства w.

Следствие. *Предположим, что $\mathcal{D}$ допускает конечную цикловую трансверсаль и $\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w) = o(n^{-1})$. Тогда взвешивание w является рекуррентным.*

В приложениях (особенно в теории вероятностей) наиболее важным является понятие *положительной рекуррентности*. По определению, она имеет место тогда и только тогда, когда последовательность $A_w^m(\mathcal{D})\lambda(\mathcal{D}, w)^{-m}$ не сходится к нулю. Замечательно, что в этом случае оба уравнения $A_w(\mathcal{D})\vec{\xi} = \lambda(\mathcal{D}, w)\vec{\xi}$ и $A_w^\top(\mathcal{D})\vec{\eta} = \lambda(\mathcal{D}, w)\vec{\eta}$ имеют положительные решения, скалярное произведение которых конечно.

Гипотеза. *Предположим, что $\mathcal{D}$ допускает конечную цикловую трансверсаль и $\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w) = o(n^{-2})$. Тогда взвешивание w является положительно рекуррентным.*

В отличие от рекуррентного случая для транзиентного w матрица $A_w(\mathcal{D})$ не обязана иметь положительные собственные векторы. Для того, чтобы предъявить достаточное условие на $\mathcal{D}$, при котором это справедливо при каждом $w \in \mathcal{T}(\mathcal{D})$, нам понадобится новое определение. Скажем, что последовательность различных вершин $\{v_m\}_{m=0}^{\infty}$ образует *бесконечный вперед путь*, если при любом $m \geq 0$ пара (v_m, v_{m+1}) является дугой в $\mathcal{D}$. Используя идеи доказательства теоремы 1 из [3], можно показать справедливость следующего утверждения.

Предложение. *Пусть $\mathcal{D}$ не содержит бесконечного вперед пути. Тогда для любого $w \in \mathcal{T}(\mathcal{D})$ весовая матрица смежности $A_w(\mathcal{D})$ не имеет положительного собственного вектора.*

Таким образом, как ни странно, транзиентность взвешивания w и наличие у $\mathcal{D}$ некоторых важных свойств конечного орграфа (существование конечной цикловой трансверсали, отсутствие бесконечного вперед пути) влекут плохие спектральные свойства матрицы $A_w(\mathcal{D})$ (достаточно медленная сходимость $\lambda^{(n)}(\mathcal{D}, w)$ к своему пределу $\lambda(\mathcal{D}, w)$, отсутствие положительных собственных векторов). На данный момент мы не имеем простого объяснения этого достаточно противоречивого факта.

Список литературы

1. Seneta E. Finite approximations to infinite non-negative matrices // Mathematical Proceedings of the Cambridge Philosophical Society. — 1967. — V. 63. — P. 983–992.

2. Cyr V. Countable Markov shifts with transient potentials // Proceedings of the London Mathematical Society. — 2011. — V. 103. — P. 923–949.

3. Harris T. E. Transient Markov chains with stationary measures // Proceedings of the American Mathematical Society. — 1957. — V. 8. — P. 937–942.

О КЛИКОВЫХ ПОКРЫТИЯХ РЕБЕР В ГРАФАХ С ОГРАНИЧЕНИЯМИ СТЕПЕНЕЙ ВЕРШИН

С. Н. Селезнева, М. В. Мельник (Москва)

В работе найден критерий единственности тупикового кликового покрытия ребер для графов, в которых степени всех вершин не превышают четырех.

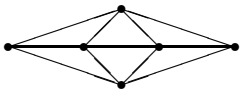
Графом G назовем пару множеств (V, E), где V — множество вершин, E — множество ребер, причем каждому ребру $e \in E$ поставлена в соответствие неупорядоченная пара (v, w) различных вершин, и разным ребрам сопоставлены различные пары вершин. *Степенью* вершины $v \in V$ в графе $G = (V, E)$ назовем величину $d_G(v) = |\{(v, w) \mid w \in V, (v, w) \in E\}|$. Пусть $\Delta(G) = \max\limits_{v \in V} d_G(v)$ обозначает наибольшую степень вершин в графе G.

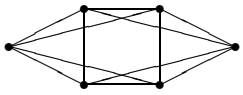
Если $K \subseteq V$, то множество K называется *кликой* в графе $G = (V, E)$, если из $v, w \in K$, $v \neq w$, следует $(v, w) \in E$. Клика K называется *максимальной*, если из $u \in V \setminus K$ следует, что множество $K \cup \{u\}$ не является кликой. Множество максимальных клик $T = \{K_1, \ldots, K_m\}$ называется *кликовым покрытием ребер* (КПР) в графе $G = (V, E)$, если из $(v, w) \in E$ следует, что найдется такой номер j, $1 \leq j \leq m$, что $v, w \in K_j$. КПР называется *тупиковым* КПР (ТКПР), если при удалении из него любой клики оставшееся множество не является КПР. ТПКР называется *кратчайшим*, если оно содержит наименее возможное число клик.

Задача о существовании в произвольном графе $G = (V, E)$ КПР мощности, не превосходящей M, где число M подается на вход алгоритма вместе с графом G, является NP-полной [1].

В работе рассматриваются графы, в которых степени всех вершин не превосходят четырех.

Пусть Γ_α и Γ_β — графы, изображенные ниже.

Γ_α : 

Γ_β : 

Если $G = (V, E)$, и $V' \subseteq V$, то граф $G' = (V', E')$, где $E' = \{(v, w) \in E \mid v, w \in V'\}$, назовем *порожденным* подграфом графа G.

Теорема 1. *В графе $G = (V, E)$ с $\Delta(G) \leq 4$ ТКПР единственно тогда и только тогда, когда этот граф не содержит порожденных подграфов, изоморфных Γ_α или Γ_β.*

Следствие. *В графе $G = (V, E)$ с $\Delta(G) \leq 3$ ТКПР единственно.*

Теорема 2. *Существует полиномиальный алгоритм, который в произвольном графе $G = (V, E)$ с $\Delta(G) \leq 4$ находит его кратчайшее ТКПР.*

Работа частично поддержана РФФИ, грант 16–01–00593-а.

Список литературы

1. Kou L. T., Stockmeyer L. J., Wong C. K. Covering edges by cliques with regard to keyword conflicts and intersection graphs // Comm. ACM. — 1978. — V. 21. — P. 135–138.

ГРАФЫ, НЕ ДОПУСКАЮЩИЕ (a, d)-ДИСТАНЦИОННУЮ АНТИМАГИЧЕСКУЮ РАЗМЕТКУ

М. Ф. Семенюта (Кировоград)

За последние 20 лет появилось большое количество разных типов и подтипов разметок, с которыми можно ознакомится в электронном журнале Д. Галлиана [1]. Будем рассматривать конечные неориентированные графы без кратных ребер и петель. Под весом $w(u)$ вершины u графа $G = (V, E)$, при вершинной разметке f, понимаем сумму меток вершин, смежных с u, то есть $w(u) = \sum_{v \in N(u)} f(v)$, где $v \in V(G)$, а $N(u)$ — множество смежности вершины u.

Будем называть (a, d)-дистанционной антимагической разметкой графа $G = (V, E)$ порядка n такую биекцию $f : V(G) \to \{1, 2, \ldots, n\}$, для которой множество всех вершинных весов образует арифметическую прогрессию a, $a+d$, $a+2d$, $\ldots$, $a+(n-1)d$ с первым членом a и разностью d, где a, d — фиксированные неотрицательные целые числа и $a \geq 1$, $d \geq 0$. Граф G, допускающий такую разметку, называют (a, d)-дистанционным антимагическим графом.

С. Арумугам и Н. Камачи, предложившие данную разметку, получили несколько базовых результатов [2]. Установили необходимое условие существования (a, d)-дистанционной антимагической разметки графа, доказали, что цикл C_n будет (a, d)-дистанционным антимагическим графом только при нечетном n и $d = 1$, а граф C_{2n}^{+} является $(2n + 2, 1)$-дистанционным антимагическим графом. Следующий шаг сделан в работе [3], где исследуются на дистанционную антимагичность цепи P_n при $2 \leq n \leq 15$, дизъюнктивное объединение изоморфных копий цикла C_n и графы с порядком меньшим 6. Для (a, d)-дистанционного антимагического графа множества смежности любых двух вершин не должны быть равными [2]. Это дает

возможность установить те типы графов, которые не допускают данной разметки. К ним относятся некоторые мультидольные графы, также графы, содержащие не меньше двух висячих ребер, смежных одной и той же вершине. Следующие теоремы расширяют семейство таких графов.

Теорема 1. *Если граф G содержит цикл $abcd$ с $\deg a = \deg c = 2$, то G не является (a, d)-дистанционным антимагическим графом.*

Доказательство. В графе G множества смежности $N(a) = \{b, d\}$ и $N(c) = \{b, d\}$ совпадают. Из этого следует, что для него не существует (a, d)-дистанционной антимагической разметки. Теорема доказана.

Теорема 2. *Если $a \leq 2$, то корона $P_n \circ P_1$ не допускает $(a, 1)$-дистанционной антимагической разметки для $n \geq 2$.*

Доказательство. Обозначим $V(P_n \circ P_1) = \{u_1, u_2, u_3, \ldots, u_n, v_1, v_2, \ldots, v_n\}$ множество вершин короны $P_n \circ P_1$, где $\{u_1, u_2, \ldots, u_n\}$ и $\{v_1, v_2, \ldots, v_n\}$ — множество вершин копии P_n и n копий P_1, соответственно. Допустим, что существует (a, d) - дистанционная антимагическая разметка f короны $P_n \circ P_1$. Запишем веса вершин, полученные при наличии разметки f

$$w(v_i) = f(u_i),$$

$$w(u_1) = f(v_1) + f(u_2),\ w(u_2) = f(v_2) + f(u_1) + f(u_3),\ \ldots,$$

$$w(u_n) = f(v_n) + f(u_{n-1}),$$

где $i = 1, 2, \ldots, n$.

Найдем суму весов всех вершин:

$$\sum_{i=1}^{n} w(u_i) + \sum_{i=1}^{n} w(v_i) = 2an + dn(2n - 1)$$

или

$$2\sum_{i=1}^{n} f(u_i) + n(2n + 1) - (f(u_1) + f(u_n)) = 2an + dn(2n - 1)$$

(d не может принимать значения 1 или 2.)

Пусть $d = 1$, тогда

$$2\sum_{i=1}^{n} f(u_i) = 2an - 2n + (f(u_1) + f(u_n)).$$

Так как $f(u_1) + f(u_n) \leq 4n - 1$, получим

$$2\sum_{i=1}^{n} f(u_i) \leq 2an + 2n - 1.$$

С другой стороны $2\sum_{i=1}^{n} f(u_i) \geq n(n+1)$. Таким образом, должно выполняться двойное неравенство:

$$n(n+1) \leq 2\sum_{i=1}^{n} f(u_i) \leq 2an + 2n - 1.$$

Это, в свою очередь, означает, что $n(n+1) \leq 2an + 2n - 1$ или $n(n-2a-1) \leq -1$. Последнее неравенство может быть верным только при $n < 2a + 1$.

Случай, когда $a = 1$ не рассматриваем, так как граф может быть (1, 1)-дистанционным антимагическим только если каждая его компонента является изоморфным образом P_2 [1]. Пусть $a = 2$, тогда n может принимать значения 2, 3, 4.

Если $n = 2$ и $V(P_2 \circ P_1) = \{u_1, u_2, v_1, v_2\}$, тогда метку 2 можно присвоить только одной из вершин u_1 или u_2. Предположим, что $f(u_1) = 2$, получим уравнение $2f(u_2) + f(v_1) + f(v_2) = 6$, не имеющее решений на множестве $\{1, 3, 4\}$.

Если $n = 3$ и $V(P_3 \circ P_1) = \{u_1, u_2, u_3, v_1, v_2, v_3\}$, тогда метку 2 можно присвоить только одной из вершин u_1, u_2 или u_3. Без потери общности, предположим $f(u_1) = 2$, получим уравнение $3f(u_2) + 3f(u_3) + f(v_1) + f(v_2)f(v_3) = 17$, не имеющее решений на множестве $\{1, 3, 4, 5, 6\}$. Аналогично для $n = 4$, уравнение

$$3f(u_2) + 3f(u_3) + 2f(u_4) + f(v_1) + f(v_2)f(v_3) + f(v_4) = 32$$

не имеет решений на множестве $\{1, 3, 4, 5, 6, 7, 8\}$. Таким образом, корона $P_n \circ P_1$ не допускает $(a, 1)$-дистанционной антимагической разметки, если $a \leq 2$. Теорема доказана.

Список литературы

1. Gallian J. A. A dynamic survey of graph labeling // The electronic journal of combinatorics. — 2015. — 18. — P. 157–163.

2. Arumugam S., Kamatchi N. On $(a; d)$-distance antimagic graphs // Australasian journal of combinatorics. — 2012. — Vol. 54. — P. 279–287.

3. Nalliah M. Antimagic labelings of graphs and digraphs: Ph. D. thesis. — The National Centre for Advanced Research in Discrete Mathematics, University of Kalasalingam, 2014.

О НЕКОТОРЫХ КОНСТРУКЦИЯХ *SD*-ГРАФОВ

З. А. Шерман (Киев)

Данная работа посвящена квадратной разностной разметке графа, которая впервые была введена в 2012 году Аджифа, Принси, Локеш и Ранжини [1].

Под графом понимаем конечный неориентированный граф без петель и кратных ребер. Пусть $G = (V, E)$ — граф с множеством вершин $V(G)$ и множеством ребер $E(G)$. Будем считать, что $|V(G)| = p$, $|E(G)| = q$.

Функцию f называют квадратной разностной разметкой графа G с p вершинами, если f — биекция из $V(G)$ на множество $\{0, 1, 2, ..., p-1\}$ и индуцируемая ею реберная разметка $f^*(u, v) = |[f(u)]^2[f(v)]^2|$ является инъекцией из $E(G)$ в множество натуральных чисел. Граф, допускающий квадратную разностную разметку, называется квадратным разностным графом или *SD графом*.

Исследуются на наличие квадратной разностной разметки такие типы графов как цепное соединение циклов и дизъюнктивное объединение звезд. Так же доказано существование квадратной разностной разметки дизъюнктивного объединения любого SD графа с цепью.

Теорема 1. *Произвольное цепное соединение n копий цикла C_3 является квадратным разностным графом для любого натурального n.*

Теорема 2. *Дизъюнктивное объединение звезд K_{1,n_i} , где $i = 1, 2, ..., m$ допускает квадратную разностную разметку для любых натуральных m и n_i.*

Теорема 3. *Дизъюнктивное объединение любого SD графа G с цепью P_k, является квадратным разностным графом для любого k.*

Список литературы

1. Ajitha V., Princy K. L., Lokesha V. and Ranjini P. S. On square difference Graphs // Int. J. of Mathematical Combinatorics — 2012. — Vol. 1, i. 1. — P. 31–40.

Секция «Математическая теория интеллектуальных систем»

К ВОПРОСУ О ВОССТАНОВЛЕНИИ ТРЕХМЕРНОГО ТЕЛА ПО ЕГО ПЛОСКИМ ПРОЕКЦИЯМ

Д. В. Алексеев (Москва)

В данной работе рассматривается задача восстановления тела по двум плоским проекциям. В работах [3, 4] описан процесс восстановления тела по плоским проекциям с точностью до аффинной эквивалентности. В [1, 2] описаны оптимизированные алгоритмы решения этой задачи. В указанных работах не приводится критерия возможности восстановления тела, т.е. условия, позволяющие по двум наборам точек определить, являются ли они проекциями одного и того же трехмерного тела. В данной работе такой критерий приводится в теореме 1.

Также рассматривается более сложная задача восстановления трехмерного тела с точностью до метрической эквивалентности проекции. Задача состоит в том, что надо построить трехмерное тело и задать две плоскости и два направления проектирования так, чтобы проекции были равны данным (как геометрические фигуры). Эта задача решается в теореме 2.

Определение 1. Будем называть *изображением* (двумерным) произвольный занумерованный набор (непустое конечное множество) точек на плоскости.

Определение 2. Будем называть *телом* произвольный занумерованный набор (непустое конечное множество) точек в трехмерном пространстве (с указанием порядка).

Определение 3. Пусть дано двухмерное изображение, состоящее из n точек $\mathcal{A} = (A_1, \ldots, A_n)$. Кроме того, пусть задан вектор $\bar{p}$ и прямая l, не параллельная вектору $\bar{p}$. Будем называть такие прямые (не параллельные $\bar{p}$) *допустимыми*. Рассмотрим прямые a_i, проходящие через соответствующие точки A_i параллельно вектору $\bar{p}$ $(i = 1, \ldots, n)$. Проекцией изображения $\mathcal{A}$ по направлению $\bar{p}$ на прямую l называется изображение $\mathcal{A}' = A'_1, \ldots, A'_n$, в котором A'_i есть точка пересечения прямых a_i и l $(i = 1, \ldots, n)$. Пусть на

прямой l введена система координат, тогда вектор координат точек $X(A'_1), \ldots, X(A'_n)$ будем называть *отпечатком* множества $\mathcal{A}$ и обозначать $F_{l,p}(\mathcal{A})$.

Определение 4. Пусть дано 3-мерное изображение, состоящее из n точек $\mathcal{A} = (A_1, \ldots, A_n)$. Кроме того, пусть задан вектор $\bar{p}$ и плоскость Π, не параллельная вектору $\bar{p}$. Рассмотрим прямые a_i, проходящие через соответствующие точки A_i, $i = 1, \ldots, n$, параллельно вектору $\bar{p}$. *Проекцией* изображения $\mathcal{A}$ по направлению $\bar{p}$ на плоскость Π называется изображение $\mathcal{A}' = A'_1, \ldots, A'_n$, в котором A'_i есть точка пересечения прямой a_i с плоскостью Π $(i = 1, \ldots, n)$.

В работе рассматриваются следующие задачи:

Задача 1. Пусть даны два плоских изображения. Построить трехмерное тело и указать плоскости и направления проектирования, такие, что проекции указанного тела на эти плоскости аффинно эквивалентны данным плоским изображениям.

Задача 2. Пусть даны два плоских изображения. Построить трехмерное тело и указать плоскости и направления проектирования, такие, что проекции указанного тела на эти плоскости метрически эквивалентны данным плоским изображениям. Т.е. существуют изометрические преобразования, переводящие проекции в данные изображения.

Определение 5. *Условие коллинеарности двух проекций.* Пусть заданы изображения $\mathcal{A}' = (A'_1, \ldots, A'_n)$ и $\mathcal{A}'' = (A''_1, \ldots, A''_n)$. Пусть в изображениях $\mathcal{A}'$ и $\mathcal{A}''$ точки $A'_{i_1}, A'_{i_2}, A'_{i_3}$ не лежат на одной прямой и $A''_{i_1}, A''_{i_2}, A''_{i_3}$ не лежат на одной прямой. Рассмотрим аффинное отображение $\mathcal{T}$, которое переводит $\mathcal{T} : A'_{i_1} \mapsto A''_{i_1}$, $\mathcal{T} : A'_{i_2} \mapsto A''_{i_2}$, $\mathcal{T} : A'_{i_2} \mapsto A''_{i_2}$. Будем говорить, что изображения $\mathcal{A}'$ и $\mathcal{A}''$ *коллинеарны* относительно точек i_1, i_2, i_3, если все векторы $\mathcal{T}(A'_i)A''_i$ попарно взаимно коллинеарны (нулевой вектор коллинеарен любому). Будем это обозначать как $\mathcal{A}' \|_{i_1,i_2,i_3} \mathcal{A}''$.

Теорема 1. *Пусть заданы изображения* $\mathcal{A}' = (A'_1, \ldots, A'_n)$ *и* $\mathcal{A}'' = (A''_1, \ldots, A''_n)$. *Пусть в изображениях* $\mathcal{A}'$ *и* $\mathcal{A}''$ *выбраны по* 4 *соответствующие точки (не ограничивая общности можно считать, что их индексы* $1, 2, 3, 4$*), обладающие следующими свойствами: a) Первые три* A'_1, A'_2, A'_3 *не лежат на одной прямой и* A''_1, A''_2, A''_3 *не лежат на одной прямой. b) Изображения* $A'_1A'_2A'_3A'_4$ *и* $A''_1A''_2A''_3A''_4$ *не являются аффинно-эквивалентными. Тогда необходимым и достаточном условием существования решения Задачи* 1 *(восстановления с точностью до аффинной эквивалентности) является условие коллинеарности изображений* $\mathcal{A}'$ *и* $\mathcal{A}''$ *относитель-*

но тройки A_1, A_2, A_3.

Теорема 2. *Пусть заданы изображения* $\mathcal{A}' = (A'_1, \ldots, A'_n)$ *и* $\mathcal{A}'' = (A''_1, \ldots, A''_n)$. *Пусть в изображениях* $\mathcal{A}'$ *и* $\mathcal{A}''$ *выбраны по* 4 *соответствующие точки* (*не ограничивая общности, можно считать, что их индексы равны* $1, 2, 3, 4$)*, обладающие следующими свойствами: a*) *Первые три точки* A'_1, A'_2, A'_3 *не лежат на одной прямой и точки* A''_1, A''_2, A''_3 *не лежат на одной прямой. b*) *Изображения* $A'_1A'_2A'_3A'_4$ *и* $A''_1A''_2A''_3A''_4$ *не являются аффинно-эквивалентными. Тогда необходимым и достаточном условием существования решения Задачи* 2 (*восстановления с точностью до метрической эквивалентности*) *является условие коллинеарности изображений* $\mathcal{A}'$ *и* $\mathcal{A}''$ *относительно тройки* A_1, A_2, A_3.

Автор выражает благодарность проф. В. Н. Козлову за ценные замечания и внимание к работе.

Список литературы

1. Алексеев Д. В. Использование метода В. Н. Козлова в образовательном процессе на кафедре МаТИС // Интеллектуальные системы — 2013. — Т. 17, № 1–4. — С. 16–20.

2. Алексеев Д. В. К вопросу о восстановлении тела по плоским проекциям // Интеллектуальные системы. Теория и приложения — Т. 18, № 3. — С. 47–60.

3. Козлов В. Н. Элементы математической теории зрительного восприятия. — М.: Изд-во ЦПИ при мех.-мат. ф-те МГУ, 2001.

4. Kozlov V. Mathematical model of reconstructing a three-dimensional image from plane projections // Pattern Recognition and Image Analysis. — 2011. — Vol. 2. — P. 279–282.

5. Kozlov V. Conclusiveness and heuristics in visual recognition // Pattern Recognition and Image Analysis. — 2014. — Vol. 24, iss. 4. — P. 1–7.

ТОЧНАЯ ПАРАМЕТРО-ЭФФЕКТИВНАЯ РАСШИФРОВКА ЛИНЕЙНЫХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

А. В. Быстрыгова (Ташкент)

Точную расшифровку функции можно наглядно представлять как игру между учеником и учителем, когда учитель загадал функцию из некоторого класса, известного ученику, а ученик, задавая

запросы учителю, должен полностью восстановить вектор значений загаданной функции.

Под параметро-эффективной расшифровкой понимают расшифровку функций, существенно зависящих от малого числа переменных.

Пусть $\Psi(k)$ — некоторый класс функций k-значной логики ($k \geqslant 2$). Под *запросом на значение* к функции $f \in \Psi(k)$ будем понимать вектор (набор) $a \in E^n, E = \{0, 1, \ldots, k-1\}$. Под *ответом на запрос на значение* будем понимать значение $f(a)$.

Под *запросом на сравнение* к функции $f \in \Psi(k)$ будем понимать пару (a, b), $a, b \in E^n$, $E = \{0, 1, \ldots, k-1\}$. Под *ответом на запрос на сравнение* будем понимать значение

$$\operatorname{sign}(f(a) - f(b)) = \begin{cases} 1 & \text{если } f(a) > f(b) \\ 0 & \text{если } f(a) = f(b) \\ -1 & \text{если } f(a) < f(b) \end{cases}$$

В данной работе рассматривается точная параметро-эффективная расшифровка запросами на значение и запросами на сравнение функций вида $f(x_0, x_1, \ldots, x_{n-1}) = c_0x_0 + c_1x_1 + \ldots + c_{n-1}x_{n-1}$, $c_i, x_i \in \{0, 1, 2, \ldots, k-1\}$, $|\{i : c_i \neq 0\}| = p$, где «+» — операция сложения по модулю k.

При рассмотрении расшифровки запросами на значение будем в обозначениях дописывать индекс $_V$, запросами на сравнение — $_C$.

Под *алгоритмом расшифровки* будем понимать условный эксперимент, который последовательно генерирует запросы к функции в зависимости от ответов на предыдущие запросы. Будем говорить, что *алгоритм расшифровывает функцию* f, если значения функции на наборах, сгенерированных условным экспериментом, однозначно определяют таблицу значений функции f. Обозначим множество алгоритмов расшифровки класса $\Psi(k)$ через $\mathcal{A}(\Psi(k))$.

Пусть $A \in \mathcal{A}(\Psi(k))$, $f \in \Psi(k)$, тогда обозначим через $\varphi(A, f)$ число запросов на значение функции, требуемое алгоритму A для расшифровки функции f. Будем называть $\varphi(A, f)$ *сложностью алгоритма* A *на функции* f. Положим

$$\varphi(k, n, p) = \min_{A \in \mathcal{A}(\Psi(k))} \max_{f \in \Psi^{p,n}(k)} \varphi(A, f).$$

В работе [1] получены получены оценки сложности расшифровки запросами на значение линейных булевых функций для случаев $p = 2$ и $p = 3$, отличающиеся от точного значения не более чем на 2.

В работе [2] была рассмотрена задача точной расшифровки линейных булевых функций запросами на значение, получена верхняя оценка сложности $p \log n + p$.

В данной работе получены верхние и нижние оценки сложности параметро-эффективной расшифровки запросами на значение и запросами на сравнение линейных функций k-значной логики с нулевым свободным членом. При стремлении числа переменных к бесконечности получен порядок сложности расшифровки для обоих типов запросов.

Теорема 1. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k > 2)$ *имеет место следующее неравенство*

$$\varphi_V(k, n, p) \leqslant 1 + (p-1) \cdot (\rceil \log_2 (k-1) \lceil + \rceil \log_2 (n-1) \rceil) + p \rceil \log_2 n \lceil.$$

Теорема 2. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k \geqslant 2)$ *имеют место следующие неравенства:*

$$\begin{aligned} \varphi_C(k, n, p) \quad \leqslant \quad & 1 + (p-1) \cdot (\rceil \log_2 (k-1) \lceil + \rceil \log_2 (n-1) \rceil) + \\ & p \rceil \log_2 n \lceil + p \cdot \rceil \log_2 k \lceil, \text{ если } k > 2; \end{aligned}$$

$$\varphi_C(2, n, p) \leqslant 1 + (p-1) \cdot \rceil \log_2 (n-1) \lceil + p \rceil \log_2 n \lceil.$$

Теорема 3. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k \geqslant 2)$ *имеет место следующее неравенство*

$$\varphi_V(k, n, p) \geqslant p \log_2 (k-1) + p \cdot \log_2 (n-p+1) - \log_2 p.$$

Теорема 4. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k \geqslant 2)$ *имеет место следующее неравенство*

$$\varphi_C(k, n, p) \geqslant p \log_2 (k-1) + p \cdot \log_2 (n-p+1) - \log_2 p.$$

Из теорем 1–4 получаем следующее

Следствие. $\varphi_V(k, n, p) = \varphi_C(k, n, p) = O(p \log n)$ *при* $n \longrightarrow \infty$.

Автор выражает благодарность научному руководителю, д.ф.-м.н. профессору Э. Э. Гасанову за постановку задачи и помощь в работе.

Список литературы

1. Быстрыгова А. В. Сложность расшифровки линейных булевых функций // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 101–126.

2. Hofmeister T. An application of codes to attribute-efficient learning // EuroCOLT'99 Proceedings of the 4th European Conference on Computational Learning Theory, 1999.

О СТАБИЛИЗАЦИИ АВТОНОМНОЙ МОДЕЛИ МИГРАЦИОННЫХ ПРОЦЕССОВ

Д. И. Васильев (Москва)

В работе рассматривается модель, предсказывающая миграцию населения внутри страны в зависимости от уровня зарплат. В качестве сети городов рассматривается граф, вершинам которого приписано текущее число людей в нём, максимальное число людей, которое может в нем находиться и невозрастающая по количеству людей функция зарплаты. На каждом шаге выбирается пара городов, и, если это выгодно, один из работников переезжает из одного города в другой. Формализуем это следующим образом:

Если $m \in N$, то обозначим $N_m = \{0, 1, \ldots, m\}$.

Пусть $G = (V, E)$ — полный граф без петель с n вершинами, т. е. $V = \{1, 2, \ldots, n\}$, $E = \{\{v_1, v_2\} : v_1, v_2 \in V, v_1 \neq v_2\}$. Пусть каждой вершине графа приписана тройка: (m_i, q_i, f_i), где $m_i \in N$, $q_i \in N_{m_i}$, $f_i : N_{m_i} \to N$, причем f_i невозрастающая функция, т.е. для любых $a, b \in N_{m_i}$ если $a \geqslant b$, то $f_i(a) \leqslant f_i(b))$, $i \in \{1, 2, \ldots, n\}$.

Обозначим $Q(G) := \{q = (q_1, q_2, \ldots, q_n) : q_i \in N_{m_i}, i \in \{1, 2, \ldots, n\}\}$, $\mathcal{G}^n$ — множество всех таким образом нагруженных полных графов без петель с n вершинами.

В дальнейшем для удобства восприятия вершины графа будем интерпретировать как города, для каждого города $i \in \{1, 2, \ldots, n\}$ число m_i будет восприниматься как максимально возможное число людей в городе, q_i — текущее число людей в городе, f_i — функция зарплат в i-м городе в зависимости от числа проживающих в городе людей. Вектор $q = (q_1, q_2, \ldots, q_n)$ будем называть *состоянием* графа G.

Рассмотрим автомат без выходов $A^G = (E, Q(G), \varphi, q_0)$, где E — входной алфавит, $Q(G)$ — алфавит состояний, $\varphi : Q(G) \times E \to Q(G)$ — функция переходов, q_0 — начальное состояние. Автомат A^G задается канонической системой

$$\begin{cases} q(1) = q_0, \\ q(t+1) = \varphi(q(t), v(t)), \end{cases}$$

где для $q = (q_1, q_2, \ldots, q_n)$, $v = \{v_1, v_2\}$,

$$\varphi(q, v) = \begin{cases} q', \text{ если } f_{v_2}(q_{v_2} + 1) > f_{v_1}(q_{v_1}), q_{v_2} < m_{v_2}, q_{v_1} > 0, \\ q'', \text{ если } f_{v_1}(q_{v_1} + 1) > f_{v_2}(q_{v_2}), q_{v_1} < m_{v_1}, q_{v_2} > 0, \\ q \text{ в остальных случаях,} \end{cases} \quad (1)$$

$$q' = (q_1, \ldots, q_{v_1-1}, q_{v_1} - 1, q_{v_1+1}, \ldots, q_{v_2-1}, q_{v_2} + 1, q_{v_2+1}, \ldots, q_n),$$

$$q'' = (q_1, \ldots, q_{v_1-1}, q_{v_1} + 1, q_{v_1+1}, \ldots, q_{v_2-1}, q_{v_2} - 1, q_{v_2+1}, \ldots, q_n).$$

В нашей интерпретации функция переходов устроена таким образом, что для пары городов v_1, v_2, если зарплата в городе v_2 после увеличения числа жителей на единицу больше, чем зарплата в городе v_1, то из города v_1 один человек переезжает в город v_2.

Через E^* будем обозначать множество всех слов в алфавите E. Через E^∞ будем обозначать множество всех сверхслов в алфавите E.

Расширим функцию φ на $Q(G) \times E^*$, а именно, если $\alpha \in E^*$, $v \in E$, то индуктивно определим

$$\varphi(q, \alpha v) = \varphi(\varphi(q, \alpha), v).$$

Пусть $\alpha \in E^\infty$, α_t — первые t символов сверхслова α. Определим

$$A^G(\alpha) = \begin{cases} \lim\limits_{t \to \infty} \varphi(q_0, \alpha_t), \text{ если такой предел существует,} \\ * \text{ — в противном случае.} \end{cases}$$

Теорема. *Для любого графа G из $\mathcal{G}^n$, любого сверхслова α из E^∞ имеем $A^G(\alpha) \neq *$.*

Пусть граф G находится в состоянии q и пусть в этом состоянии в городах s различных значений зарплат f_1,f_2,...,f_s, причём $f_1 < f_2 < ... < f_s$. Пусть r_i это количество городов, зарплата в которых равна f_i, $i = 1, 2, ..., s$. Понятно, что $\sum\limits_{i=1}^{s} r_i = n$. Сопоставим состоянию q вектор пар $ord_G(q) = ((f_1, r_1), \ldots, (f_s, r_s))$.

Введём на парах (f_i, r_i) следующий линейный порядок:

- если $f^i > f^j$, то $(f^i, r^i) > (f^j, r^j)$ независимо от r^i и r^j;
- если $f^i = f^j$, то $(f^i, r^i) > (f^j, r^j)$ точно тогда, когда $r^i < r^j$.

Введём лексикографический порядок на множестве всех векторов, состоящих из таких пар.

Лемма. *Для любых $G \in \mathcal{G}^n$, $q \in Q$, $\{a, b\} \in E$ если $\varphi(q, \{a, b\}) \neq q$, то $ord_G(\varphi(q, \{a, b\})) > ord_G(q)$.*

Для определённости будем считать, что мигранты переезжают из города a в город b, то есть $f_a(q_a) < f_b(q_b + 1)$, $q_b < m_b$, $q_a > 0$. Пусть количество городов с зарплатой $f_a(q_a)$ равно r_a, а количество городов с зарплатой $f_b(q_b)$ равно r_b. Пусть $(f_a(q_a), r_a)$ является i-ым элементом вектора $ord_G(q)$, а $(f_b(q_b), r_b)$ является j-ым элементом этого вектора. Поскольку $f_b(q_b + 1) \leqslant f_b(q_b)$, то $f_a(q_a) < f_b(q_b)$ и значит $i < j$. Обозначим пару, являщуюся $i+1$-м элементом вектора $ord_G(q)$, через (f_c, r_c). Возможно $f_c = f_b$, тогда $r_c = r_b$ и $j = i + 1$.

Обозначим через r' число городов, зарплата в которых равна $f_b(q_b + 1)$, если таких городов нет, то $r' = 0$. Обозначим $q^+ = \varphi(q, \{a, b\})$.

Когда один мигрант переезжает в город b, зарплата там становится $f_b(q_b+1)$, то есть в $ord_G(q^+)$ появляется пара $(f_b(q_b+1), r'+1)$. Поскольку $f_b(q_b+1) > f_a(q_a)$, то позиция этой пары в $ord_G(q^+)$ будет не меньше чем i, причём эта пара окажется в i-ой позиции вектора только если $r_a = 1$ и $f_b(q_b + 1) \leq f_c$. Равенство $r_a = 1$ означает, что после отъезда одного мигранта из города a, не останется городов с зарплатой $f_a(q_a)$, и следовательно, на i-ю позицию переместится пара со значением зарплаты $\min(f_a(q_b + 1), f_c)$, которое больше, чем $f_a(q_a)$.

Если же $r_a > 1$, то после отъезда одного мигранта из города a число городов с зарплатой $f_a(q_a)$ уменьшится как минимум на 1, а зарплата в городе a останется прежней, либо возрастёт, то есть на i-ой позиции вектора $ord_G(q^+)$ окажется пара со значением зарплаты $\min(f_a(q_a - 1), f_c)$, которое больше чем $f_a(q_a)$.

Следовательно, $ord_G(q)$ и $ord_G(q^+)$ совпадают до $(i-1)$-й позиции включительно, а в i-й позиции в $ord_G(q^+)$ стоит большая пара, то есть $ord_G(q^+) > ord_G(q)$.

Докажем теорему. Предположим, что значение функции $q(t)$ изменяется бесконечное число раз с ростом t. . Тогда по доказанной лемме $ord_G(q(t))$ неограниченно возрастает, что невозможно, так как множество различных векторов $ord_G(q)$ конечно. Значит, значение $q(t)$ может меняться конечное число раз. Теорема доказана.

ЧАСТИЧНОЕ ПРОГНОЗИРОВАНИЕ ОБЩЕРЕГУЛЯРНЫХ СВЕРХСОБЫТИЙ В МНОГОЗНАЧНОМ АЛФАВИТЕ

И. К. Ведерников (Москва)

В статье А. Г. Вереникина и Э. Э. Гасанова [1] были введены прогнозирующие автоматы — конечные автоматы, предсказывающие сверхслово или множество сверхслов. Автомат прогнозирует сверхслово, если через некоторое конечное время после начала подачи сверхслова, он начинает угадывать каждый следующий символ, то есть на выходе в момент времени t выдавать элемент входной последовательности под номером $t+1$.

В работе [2] А. А. Мастихиной было введено понятие частичного прогнозирования, а в работе [3] для общерегулярных сверхсобытий в двоичном алфавите получен критерий прогнозируемости.

В данной работе исследуется частичная прогнозируемость в многозначных алфавитах, получен критерий.

Введем основные определения.

Определение. Пусть $E_k = \{0, 1, \ldots, k-1\}$ — конечный алфавит. Через E_k^* и E_k^∞ обозначим соответственно множество всех слов конечной длины и множество всех сверхслов в алфавите E_k. По определению будем считать, что пустое слово Λ принадлежит E_k^*. Подмножества E_k^* называются *событиями*, а подмножества E_k^∞ — *сверхсобытиями*.

Определение. Если R_1 — событие и R_2 — событие или сверхсобытие, то через R_1R_2 обозначим их *произведение*, то есть все слова (сверхслова) вида $\alpha\beta$, где $\alpha \in R_1, \beta \in R_2$.

Определение. Если R — событие, то R^* — *итерация* события R, то есть $R^* = R \cup R^2 \cup R^3 \cup \ldots \cup R^i \ldots$, а R^∞ — *сверхитерация* события R, $R^\infty = \{\alpha_1\alpha_2\alpha_3 \ldots | \ \alpha_i \in R, i = 1, 2, 3 \ldots\}$.

Если α — сверхслово в алфавите E_k, n — натуральное число, то n-ую букву сверхслова α будем обозначать $\alpha(n)$, а через $\alpha]_n$ обозначим префикс длины n сверхслова α, т.е. $\alpha]_n = \alpha(1)\alpha(2)\ldots\alpha(n)$.

В работе рассматриваются конечные инициальные автоматы $V = (E_k, Q, E_k, \varphi, \psi, q_0)$, где $E_k = \{0, 1, \ldots, k-1\}$ — входной и выходной алфавит, Q — множество состояний, которое является конечным подмножеством некоторого фиксированного счетного множества, $\varphi : Q \times E_k \to Q$ — функция переходов, $\psi : Q \times E_k \to E_k$ — функция выходов, q_0 — начальное состояние.

Функции φ и ψ естественно расширяются на $Q \times E_k^*$, а именно, если $\alpha \in E_k^*$, $a \in E_k$, то индуктивно определим $\varphi(q, \alpha a) =$

$\varphi(\varphi(q,\alpha),a)$, $\psi(q,\alpha a) = \psi(\varphi(q,\alpha),a)$. Введем также обозначения $\overline{\varphi}(q,\alpha) = \varphi(q,\alpha]_1)\varphi(q,\alpha]_2)\dots\varphi(q,\alpha)$, если α — слово, а если α — сверхслово, то $\overline{\varphi}(q,\alpha) = \varphi(q,\alpha]_1)\varphi(q,\alpha]_2)\dots\varphi(q,\alpha]_n)\dots$. Аналогичные обозначения вводятся для функции выходов.

Определение. Если α — сверхслово в алфавите A, то *пределом* сверхслова α назовем такое множество $A' \subseteq A$, что в сверхслове α бесконечное число раз встречаются символы из A' и только они. Этот факт будем обозначать через $A' = \lim\alpha$.

Определение. Сверхсобытие R *представимо* автоматом $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ с помощью семейства F, $F \subseteq 2^Q$, тогда и только тогда, когда для любого $\alpha \in R$, существует $Q' \in F$, такое, что $\lim\overline{\varphi}(q_0,\alpha) = Q'$.

Определение. Будем говорить, что символ $\alpha(t+1)$ сверхслова $\alpha = \alpha(1)\alpha(2)\dots\alpha(t+1)\dots$ *угадан* автоматом $V = (A, Q, B, \varphi, \psi, q_0)$, если $\psi(q,\alpha]_t) = \alpha(t+1)$.

Определение. Пусть $\alpha \in E_k^\infty$, обозначим $\sigma_\alpha = \underline{\lim}_{n\to\infty} N/n$, где N — количество угаданных автоматом V символов в слове $\alpha]_n$. Будем говорить, что σ_α – *степень прогнозирования* слова α автоматом V.

Считаем, что множество слов *частично прогнозируемо*, если существует такой автомат, что степень прогнозирования для каждого сверхслова множества строго больше нуля.

Определение. *Регулярное событие* над алфавитом E_k.

1. $\varnothing, \{a\}, a \in E_k$, — регулярные события.

2. Пусть R_1, R_2 являются регулярными событиями. Тогда события $R_1R_2, R_1 \cup R_2, R_1^*$ также регулярны.

Определение. *Общерегулярное сверхсобытие* над алфавитом E_k.

1. Если R — регулярное событие над алфавитом E_k, то R^* — общерегулярное сверхсобытие над алфавитом E_k.

2. Если R_1 — регулярное событие над алфавитом E_k, R_2 — общерегулярное сверхсобытие над алфавитом E_k, то R_1R_2 — общерегулярное сверхсобытие над алфавитом E_k.

3. Если R_1, R_2 — общерегулярные сверхсобытия над алфавитом E_k, то $R_1 \cup R_2$ — общерегулярное сверхсобытие над алфавитом E_k.

Определение. *Сильно связным множеством* назовем такое множество состояний C, $C \subseteq Q$, автомата $V = (E_k, Q, E_k, \varphi, \psi, q_0)$, что для любых $q', q'' \in C$ найдется такое слово α из E_k^*, что $\varphi(q',\alpha) = q''$ и $\overline{\varphi}(q',\alpha) \in C^*$, т.е. по слову α автомат переходит из состояний q' в состояние q'', проходя только состояния из C. Множество, состоящее из одного состояния, по определению считается сильно связным.

Определение. Любое сильно связное множество состояний мощности более одного назовем *автоматным циклом*. Одноэлементное множество состояний $C = \{q\}$ является *автоматным циклом* только если существует символ a из E_k, что $\varphi(q, a) = q$. *Длиной автоматного цикла* назовем число состояний в автоматном цикле.

Определение. *Состоянием выхода* для автоматного цикла C назовем такое состояние q, что существует единственное a, $a \in E_k$, такое, что $\varphi(q, a) \in C$.

Теорема. *Общерегулярное сверхсобытие, представимое конечным инициальным автоматом $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ с помощью некоторого семейства F, $F \subset 2^Q$, частично прогнозируемо, тогда и только тогда, когда для любого $Q' \in F$ и для любого автоматного цикла C, $C \subseteq Q'$, существует состояние выхода.*

Автор выражает благодарность профессору Э. Э. Гасанову и доценту А. А. Мастихиной за постановку задачи и помощь в работе.

Список литературы

1. Вереникин А. Г., Гасанов Э. Э. Об автоматной детерминизации множеств сверхслов // Дискретная математика. — 2006. — Т. 18, вып. 2. — С. 84–97.

2. Мастихина А. А. О частичном угадывании сверхслов // Интеллектуальные системы. — 2007. — Т. 11, вып. 1–4. — С. 561–572.

3. Мастихина А. А. Критерий частичного предвосхищения общерегулярных сверхсобытий // Дискретная математика. — 2011. — Т. 23, вып. 4 — С. 103–114.

РЕКОНФИГУРИРУЕМЫЙ НА ЛЕТУ АППАРАТНЫЙ БЧХ ДЕКОДЕР

Э. Э. Гасанов, П. А. Пантелеев (Москва)

Бинарные БЧХ коды представляют собой мощный класс помехоустойчивых кодов. Они имеют широкий диапазон применений в системах оптической и беспроводной связи, в магнитной записи и т.д.

Рассмотрим алгоритм декодирования БЧХ. Вход БЧХ декодера есть кодовое слово $(c_{n-1}, \ldots, c_0)$, где каждый символ $c_i \in \{0, 1\}$. Кодовое слово будем также задавать полиномом $c(x) = c_{n-1}x^{n-1} +$

$\ldots + c_1 x + c_0$. Этот полином используется модулем вычисления синдромов (Syndrome Calculation, SC), который вычисляет $2t$ синдромов $S_1, S_2, \ldots, S_{2t}$ следующим образом: $S_i = c(\alpha^i)$, $i = 1, 2, \ldots, 2t$, где t — максимальное число ошибок, которое БЧХ код может исправить, а α — примитивный элемент поля расширения $GF(2^m)$, связанного с этим кодом БЧХ. В этом случае длина кодового слова равна $n = 2^m - 1$. Затем эти синдромы приходят к модулю решения ключевых уравнений (Key Equation Solver, KES), который вычисляет полином локаторов ошибок $\Lambda(x)$, корнями которого являются позиции ошибок. Затем модуль коррекции ошибок (Error Correction, EC), используя $\Lambda(x)$, корректирует позиции ошибок в кодовом слове, сохраняемом в специальном модуле FIFO (очередь).

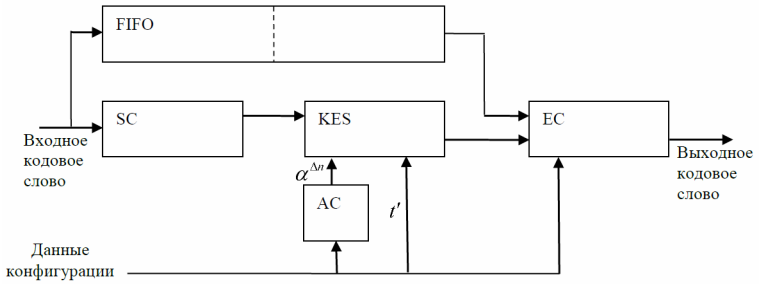


Рис. 4: Схема конфигурируемого БЧХ декодера

Большинство реализаций БЧХ декодеров не позволяют пользователю изменять параметры БЧХ кода, такие как максимальное число ошибок и длина кодового слова. Однако современные приложения кодов БЧХ в контроллерах твердотельных дисков (solid-state disk, SSD) делают необходимым изменение этих параметров во время функционирования. При этом, чтобы достичь быстрой скорости, время изменения конфигурации такого контроллера должно быть как можно меньше. Поэтому реконфигурируемые декодеры должны иметь специальный вход (см. рис.1) под названием "Данные конфигурации". Он состоит из пары (n', t'), где n' — текущая длина кодового слова, t' — текущее максимальное число исправляемых ошибок.

В данной работе мы предлагаем новую реконфигурируемую на лету аппаратную схему БЧХ декодера. Это означает, что изменение конфигурации в этой конструкции может быть сделано за константное число тактов, независящее от длины кодового слова и числа исправляемых ошибок.

Не трудно изменить схему 1 так, чтобы она могла обрабатывать БЧХ коды с числом ошибок $t' < t$. Единственное отличие состоит в том, что KES блок должен выполнять $2t'$ итераций вместо $2t$. Но если мы хотим использовать БЧХ код с другой длиной $n' < n$, то мы должны использовать усеченные коды БЧХ. Это означает, что вместо кодового слова полной длины $(c_{n-1}, \ldots, c_0)$ на вход БЧХ декодера будет поступать усеченное кодовое слово $(c_{n'-1}, \ldots, c_0)$, которое можно рассматривать как кодовое слово полной длины $(c_{n'-1}, \ldots, c_0, 0 \ldots, 0)$ или в полиномиальной форме $c(x) = x^{\Delta n} c'(x)$, где $c'(x) = c_{n'-1}x^{n'-1} + \ldots + c_1 x + c_0$ и $\Delta n = n - n' = 2^m - 1 - n'$. Следовательно, если мы будем использовать стандартную схему для вычисления синдромов, то она вместо синдромов $S_i = c(\alpha^i) = \alpha^{i\Delta n} c'(\alpha^i)$, $i = 1, 2, \ldots, 2t$ произведет значения $S'_i = c'(\alpha_i)$. Так что, если мы хотим получить правильные значения синдромов $S_1, S_2, \ldots, S_{2t}$, то мы должны сначала вычислить значения $S'_1, S'_2, \ldots, S'_{2t}$, а затем использовать формулу $S_i = \alpha^{i\Delta n} S'_i$, $i = 1, 2, \ldots, 2t$. Основная проблема состоит в том, что Δn зависит от параметра конфигурации n' — текущей длины кодового слова, и значение $\alpha^{\Delta n}$ не может быть вычислено за небольшое фиксированное число тактов, поскольку величина Δn может быть очень большой.

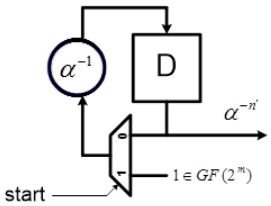


Рис. 5: Схема Альфа Калькулятора

Основная идея данной работы заключается в вычислении значения $\alpha^{\Delta n}$ одновременно с вычислением синдромов $S'_1, S'_2, \ldots, S'_{2t}$. Для того, чтобы упростить вычисление $\alpha^{\Delta n}$, заметим, что $\alpha^{\Delta n} = \alpha^{2^m - 1 - n'} = \alpha^{-n'}$ так как $\alpha^{2^m - 1} = 1$ в поле $GF(2^m)$. Так что для того, чтобы вычислить $\alpha^{-n'}$, мы можем использовать константный умножитель в поле $GF(2^m)$, который выполняет умножение на α^{-1}. Модуль, который выполняет эти вычисления, называется Альфа Калькулятором (Alpha Calculator, AC) и реализован, как показано на рис.2. Если сигнал start $= 1$, то вычисления запускаются. Модуль

AC работает одновременно с модулем SC (см. рис.1) и в конце вычислений он производит значение $\alpha^{-n'}$.

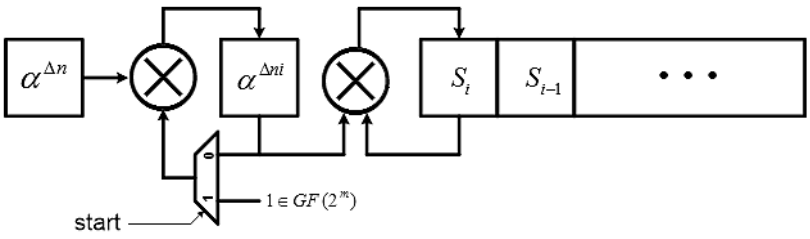


Рис. 6: Схема обновления синдромов

После того, как значение $\alpha^{-n'}$ получено, оно подается на KES блок (см. рис.1). В нашей реализации модуля KES значения синдромов $S_1, S_2, \ldots, S_{2t}$ используются последовательно. На первой итерации используется только S_1, на второй — только S_1, S_2, и т.д. Поэтому, мы имеем достаточно времени, чтобы вычислить все значения $S_1 = \alpha^{\Delta n} S'_1, S_2 = \alpha^{2\Delta n} S'_2, \ldots, S_{2t} = \alpha^{2t\Delta n} S'_{2t}$, используя только два умножителя в поле $GF(2^m)$, как показано на рис.3. На этом рисунке сигнал "start" выводится из блока SC и если start = 1, то это означает, что модули SC и AC закончили свои расчеты и модуль KES должен начать работать.

Список литературы

1. Panteleev P. A., Gasanov E. E., Neznanov I. V., Sokolov A. P., Shutkin Yu. A. Reconfigurable BCH decoder. United States Patent: 8,621,329, December 31, 2013.

СВОЙСТВА АФИННО ЭКВИВАЛЕНТНЫХ ПЛОСКИХ ИЗОБРАЖЕНИЙ

В. Н. Козлов (Москва)

Изображение — это конечное множество точек на плоскости. Кодом изображения A называем пару $\langle M_A, T_A \rangle$, в которой M_A — множество номеров точек изображения, T_A — множество всех чисел вида $\rho_{mnu,ksp} = S_{mnu}/S_{ksp}$, где S_{mnu} и S_{ksp} — площади треугольников с

вершинами в точках соответственно m, n, u и k, s, p. При $S_{ksp} = 0$ полагаем $\rho_{mnu,ksp}$ неопределенным. Изображения A и B с кодами $\langle M_A, T_A\rangle$ и $\langle M_B, T_B\rangle$ называем эквивалентными, если существует такая биекция $\psi : M_A \to M_B$, что $\rho_{mnu,ksp} = \rho_{\psi(m)\psi(n)\psi(u),\psi(k)\psi(s)\psi(p)}$. Если все точки изображения не лежат на одной прямой или двух параллельных прямых, то изображение называем плоским.

Теорема 1 [2]. *Два плоских изображения эквивалентны тогда и только тогда, когда они аффинно эквивалентны.*

Содержательно теорема 1 означает, в частности, что код изображения задает его с точностью до аффинных преобразований.

Пусть B есть часть изображения A. Если код для A есть $\langle M_A, T_A\rangle$, то, очевидно, код $\langle M_B, T_B\rangle$ можно получить, если собрать в M_B номера из M_A всех точек, вошедших в B, и собрав в T_B все те $\rho_{mnu,ksp}$ из T_A, для которых m, n, u, k, s, p вошли в M_B. Говорим в этом случае, что код $\langle M_B, T_B\rangle$ есть часть кода $\langle M_A, T_A\rangle$.

Известно, что для построения изображения A по коду $\langle M_A, T_A\rangle$ достаточно таких элементов $\rho_{mnu,ksp}$ из T_A, у которых тройки mnu и ksp разнятся только одним номером. Возникает вопрос: какова может быть роль других элементов $\rho_{mnu,ksp}$ в коде?

Назовем изображения A и B эквидистантными, если существует такая биекция $\psi : M_A \to M_B$, при которой для любых точек с номерами m, n, u из M_A (не лежащих на одной прямой), число $\rho_{mnu,\psi(m)\psi(n)\psi(u)}$ есть константа, не зависящая от выбора точек m, n, u.

Название «эквидистантные изображения» объясняется следующей аналогией с более простым случаем. Пусть A и B есть изображения, совместимые параллельным переносом. Тогда, очевидно, существует биекция $\psi : M_A \to M_B$ такая, что все расстояния $r(a, \psi(a))$ между соответствующими точками двух изображений одинаковы. Отрезки $r(a, \psi(a))$ для всех a из M_A в этом случае не только равны, но и параллельны. Очевидно, имеет место и обратное: если все эти отрезки равны и параллельны, то A и B совместимы параллельным переносом.

Теорема 2. *Два плоских изображения эквидистантны тогда и только тогда, когда они аффинно эквивалентны.*

Доказательство. Пусть A и B аффинно эквивалентны. Тогда существует такая биекция $\psi : M_A \to M_B$, что B переводится в B', совмещенное с A, т. е. при этом каждая точка a из A совмещена с точкой $\psi(a)$. Ясно, что при этом для каждой тройки m, n, u из A (не лежащих на одной прямой) и соответствующей тройки k', s', p' из B' (здесь $k' = \psi(m)$, $s' = \psi(n)$, $p' = \psi(u)$) имеем $\rho_{mnu,k's'p'} =$

$S_{mnu}/S_{k's'p'} = q$. Вернем теперь обратным преобразованием B' в B. При этом площадь каждого треугольника с вершинами $k's'p'$ из B' при переводе в треугольник ksp с вершинами из B умножится на одну и ту же для всех треугольников величину q. Следовательно $\rho_{mnu,ksp} = S_{mnu}/S_{ksp} = S_{mnu}/(qS_{k's'p'}) = 1/q$.

Пусть теперь A и B эквидистантны. Если B' получено из B аффинным преобразованием, то нетрудно видеть, A и B' тоже эквидистантны. Выберем некоторые три точки (не на одной прямой) m, n, u на A, и пусть преобразованное B' таково, что его точки k', s', p', соответствующие точкам m, n, u, совпали с ними, т. е. площади треугольников mnu и $k's'p'$ равны. Но тогда, с учетом эквидистантности, должны быть равны площади и всех остальных соответствующих друг другу треугольников из A и B'. Однако это значит, что коды $\langle M_A, T_A\rangle$ и $\langle M_{B'}, T_{B'}\rangle$ эквивалентны, и, значит, в силу теоремы 1, изображения A и B' аффинно эквивалентны. Но тогда аффинно эквивалентны и изображения A и B. Теорема доказана.

Таким образом, нами прояснена роль элементов $\rho_{mnu,ksp}$ кода с полностью различными тройками mnu и ksp. Роль элементов с двумя различиями в этих тройках пока не ясна.

Список литературы

1. Крушинский Л. В., Кудрявцев В. Б., Козлов В. Н. О некоторых результатах применения математики к моделированию в биологии // Математические вопросы кибернетики. Вып. 1. — 1988. — С. 52–88.

2. Козлов В. Н. Введение в математическую теорию зрительного восприятия. — М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2007.

ВЫДЕЛЕНИЕ ОБЩЕЙ ПОДФОРМУЛЫ ФОРМУЛ ИСЧИСЛЕНИЯ ПРЕДИКАТОВ ДЛЯ РЕШЕНИЯ РЯДА ЗАДАЧ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Т. М. Косовская (Санкт-Петербург)

Рассматриваются задачи искусственного интеллекта при логико-предметном подходе в следующей постановке. Исследуемый объект является конечным множеством $\omega = \{\omega_1, \ldots, \omega_t\}$. На элементах ω

задан набор предикатов $p_1, \ldots, p_n$, характеризующих свойства и отношения между элементами объекта ω. Задано разбиение множества Ω всех исследуемых объектов на K (возможно пересекающихся) классов $\Omega = \bigcup_{k=1}^{K} \Omega_k$. Логическим описанием класса Ω_k называется бескванторная формула в ДНФ $A_k(\overline{x})$, такая что если $A_k(\overline{\omega})$ (где $\overline{\omega}$ – некоторая перестановка элементов из ω), то $\omega \in \Omega_k$. Логическим описанием $S(\omega)$ объекта ω называется набор всех истинных постоянных атомарных формул вида $p_i(\overline{\tau})$ или $\neg p_i(\overline{\tau})$, выписанных для всех возможных частей τ объекта ω. В рамках логико-предметного подхода основными задачами являются следующие.

Задача идентификации. Проверить, принадлежит ли объект ω или его часть классу Ω_k.

$$S(\omega) \Rightarrow \exists \overline{x}_{\neq} A_k(\overline{x})$$

Задача классификации. Найти все такие номера классов k, что $\omega \in \Omega_k$.

$$S(\omega) \Rightarrow \vee_{k=1}^{K} A_k(\overline{\omega}).$$

Задача анализа сложного объекта.

$$S(\omega) \Rightarrow \vee_{k=1}^{K} \exists \overline{x_k}_{\neq} A_k(\overline{\omega}).$$

В [1, 2] доказаны экспоненциальные оценки числа шагов алгоритмов, решающих сформулированные задачи. В зависимости от алгоритма (алгоритм полного перебора и алгоритмы, основанные на доказательстве выводимости в исчислении предикатов) в показателе экспоненты стоит либо число аргументов в описании класса, либо количество атомарных формул в описании класса. Там же доказана NP-трудность рассматриваемых задач.

Для уменьшения числа шагов решения рассматриваемых задач в [3] предложено понятие многоуровневого описания классов, заключающееся в выделении достаточно «коротких» общих с точностью до имён переменных подформул у элементарных конъюнкций, составляющих описания классов. Такие подформулы являются обобщёнными признаками объектов, присущих многим объектам из одного класса. Там же доказаны оценки уменьшения числа шагов для рассматриваемых алгоритмов.

До последнего времени не было алгоритма, позволяющего выделять такие подформулы, но эвристически найденные подформулы показывали существенное уменьшение числа шагов.

Для задачи распознавания объектов с неполной информацией в [4] было предложено понятие неполной выводимости. Это понятие

оказалось удобным для выделения «коротких» общих с точностью до имён переменных подформул у элементарных конъюнкций, составляющих описания классов [5].

Автоматическое выделение требуемых подформул позволило разработать понятие самокорректирующейся предикатной сети, в которой имеется два блока: обучающий («долго» работающий) блок, в котором автоматически по обучающей выборке строятся многоуровневые описания классов, и распознающий («быстро» работающий) блок, в котором распознаются новые объекты. Если распознавание было ошибочным, то возможно дообучение сети с помощью обучающего блока. При этом структура (количество уровней и количество проверяемых формул в уровне) сети может измениться.

Выделение максимальных общих с точностью до имён аргументов подформул позволяет рассмотреть и решить следующую задачу мультиагентного описания объекта.

Имеется m агентов $a_1, \ldots, a_m$, которые могут измерить некоторые значения признаков на некоторых элементах объекта ω (то есть определить свойства некоторых элементов исследуемого объекта и некоторые отношения между этими элементами). Каждый из агентов $a_1, \ldots, a_m$ обладает информацией $I_1, \ldots, I_m$ соответственно. Информация, которой обладает каждый агент, абсолютно достоверна.

Требуется построить описание объекта ω в виде конъюнкции атомарных формул или их отрицаний, задающих свойства элементов заданного объекта и отношения между этими элементами при условии, что агент a_j может не знать реального количества элементов в объекте ω и предполагать, что он имеет дело с объектом $\omega^j = \{\omega_1^j, ...\omega_{t_j}^j\}$ (нумерация элементов у каждого агента своя, например, агенты рассматривают один и тот же объект с разных сторон).

Результатом применения алгоритма выделения максимальной общей подформула является не только сама подформула, но и унификаторы для этой подформулы и тех формул, из которых она выделена. Тем самым обеспечивается выделение общей (с точностью до имён элементов) информации, собранной разными агентами.

Оценка числа шагов работы алгоритма мультиагентного описания объекта составляет $O(t^t \cdot ||I|| \cdot m^2)$ «шагов» для алгоритма полного перебора, где t и $||I||$ — максимальные количества аргументов и атомарных формул в I_i $(i = 1, \ldots m)$ соответственно и $O(s^{||I||} \cdot ||I||^3 \cdot m^2)$ для алгоритма, основанного на поиске вывода исчислении предикатов, где s — максимальное количество атомарных формул с одним и тем же предикатом в каждой элементарной конъюнкции I_i.

Работа выполнена при финансовой поддержке РФФИ (проект № 14-08-01276).

Список литературы

1. Косовская Т. М. Доказательства оценок числа шагов решения некоторых задач распознавания образов, имеющих логические описания // Вестн. С.-Петербург. ун-та. Сер. 1. —2007. — Вып. 4. — С. 82–90.

2. Косовская Т. М. Некоторые задачи искусственного интеллекта, допускающие формализацию на языке исчисления предикатов, и оценки числа шагов их решения // Труды СПИИРАН. — 2010. — Вып. 14. — С. 58–75.

3. Косовская Т. М. Многоуровневые описания классов для уменьшения числа шагов решения задач распознавания образов, описываемых формулами исчисления предикатов // Вестн. С.-Петербург. ун-та. Сер. 10. — 2008. — Вып. 1. — С. 64–72.

4. Косовская Т. М. Частичная выводимость предикатных формул как средство распознавания объектов с неполной информацией // Вестн. С.-Петербург. ун-та. Сер. 10. — 2009. — Вып. 1. — С. 74–84.

5. Косовская Т. М. Подход к решению задачи построения многоуровневого описания классов на языке исчисления предикатов // Труды СПИИРАН. —2014. — Вып. 34. — С. 204–217.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА ДОРОГАХ

А. А. Лыков, В. А. Малышев, М. В. Меликян (Москва)

Проблеме описания и организации транспортных потоков посвящено множество работ, см. глобальный обзор [2]. Условно эти работы можно разделить на два класса: 1) макроподход, где основным является понятие потока, аналогичное потоку жидкости в трубах [1]; 2) микроподход, где основные объекты — отдельные машины и взаимодействия между ними. В микроподходе в основном это работы вероятностного характера, не касающиеся вопросов искусственного интеллекта, в которых исследуется случайность в разных ее проявлениях, даже для случайного движения машин. Детерминированному движению машин посвящено существенно меньше работ. Наша

работа лежит в рамках последнего подхода, однако отличается конкретностью модели, где можно получить явное описание областей устойчивости, как в смысле безопасности, так и эффективности.

Обозначения. Поток машин по однополосной дороге представляется точками прямой R

$$... < x_i(t) < ... < x_1(t) < x_0(t),$$

где $x_i(t)$ — координата переднего бампера машины с номером i, $v_i(t) > 0$ — скорость машины i. Машина с номером 0 (лидер) едет произвольным образом в зависимости от препятствий на дороге и от возможностей водителя. Машина с нолером i должна выдерживать расстояние до машины $i-1$.

Пусть $D(v)$ — минимально безопасное расстояние между соседними машинами. Предполагается, что оно известно и является обязательным для всех машин, то есть должно быть (для всех t и i)

$$x_{i-1}(t) - x_i(t) > D(v_i) + d_{i-1},$$

где d_i — длина машины i. Можно взять $d_i = 0$ (добавляя максимально возможное значение d_i к $D(v)$), то есть считать машины точечными частицами.

Если скорость $v_0(t) = v$ постоянна, дорога не имеет перекрестков и если все машины могут двигаться с той же скоростью, то плотность может быть $D^{-1}(v)$.Препятствия к такому движению может быть только изменение скорости впереди идущей машины. Мы разберем два случая причин такого изменения: наличие перекрестков и флуктуации движения лидера.

Перекрестки. Управление движением на перекрестках может быть двух видов: 1) светофоры, то есть циклическая остановка некоторых потоков — им посвящено максимальное число исследований, 2) без остановки движения путем уменьшения скорости и увеличения расстояния между машинами. Остановимся сначала на этом случае одного перекрестка n дорог. Пусть есть n дорог $k = 1, \ldots, n$, причем с одинаковыми расстояниями и скоростями $d_k = d, v_k = v$. Тогда существует безопасный режим движения с плотностью машин $\rho_{critical} = \frac{1}{nD(v)}$, но не существует безопасного режима с большей плотностью. Тот же результат имеет место для любого числа дорог и перекрестков при условии, что граф дорог не имеет циклов. В этом случае под n понимается максимальная из кратностей перекрестков.

Если же все n скоростей v_k и расстояний d_k допускаются различными, то определим поток машин на дороге k как

$$J_k = \rho_k v_k = \frac{v_k}{d_k}.$$

Возникает естественный вопрос: для каких v_k, d_k возможно движение такое что $d_k \geq D(v_k)$ для некоторого $D(v_k)$? А также, какими должны быть v_k, d_k, чтобы средний поток

$$J = \frac{1}{m}\sum_{k=1}^{m} J_k$$

был максимальным (здесь m общее количество дорог). Например, ответ на данный вопрос для случая двух дорог, когда $D(v_k) = D_0,\ k = 1, 2$ для некоторого D_0, имеет следующий вид.

1. Если $\frac{J_1}{J_2}$ иррационально, то такого движения не существует.

2. Пусть $\frac{J_1}{J_2} = \frac{n_1}{n_2}$, где n_1, n_2 целые такие, что $(n_1, n_2) = 1$. Тогда движение существует тогда и только тогда, когда

$$\frac{n_2}{d_1} + \frac{n_1}{d_2} < \frac{1}{D_0}. \tag{1}$$

Пусть теперь v_1, v_2 и D_0 фиксированы. Пусть $\Sigma(v_1, v_2, D_0)$ - множество всех пар (d_1, d_2), для которых существует движение. Тогда для максимального потока имеет место

$$\sup_{(d_1,d_2)\in\Sigma(v_1,v_2,d)} J(d_1, d_2) = \frac{\hat{v}}{2D_0},$$

где $\hat{v} = \frac{2}{\frac{1}{v_1}+\frac{1}{v_2}}$ — гармоническое среднее v_1 и v_2.

Если граф дорог имеет циклы, ситуация существенно более сложная, и требует более подробного описания.

Переменное движение в одном потоке. Рассматривается простейший локальный алгоритм управления, основанный на физическом принципе взаимодействия в цепочке молекул [7]. Однако, система ОДУ в нашей модели не является гамильтоновой. Каждая машина знает только свою скорость и расстояние до впереди идущей машины, однако с малым запаздыванием по времени (реакция измерительных приборов). Таким образом, выполнена система $N \leq \infty$

уравнений Ньютона с гармонической силой, удерживающей расстояние близким к d, а также (абсолютно необходимая) диссипативная сила

$$\frac{d^2x_k}{dt^2} = \omega^2(x_{k-1}(t-\epsilon_1) - x_k(t-\epsilon_1) - d) - \alpha v_k(t-\epsilon_2).$$

Обозначая расстояния между машинами $r_k(t) = z_{k-1}(t) - z_k(t)$, мы получаем для величин

$$I = \inf_{k\geqslant 1}\inf_{t\geqslant 0} r_k(t), \quad S = \sup_{k\geqslant 1}\sup_{t\geqslant 0} r_k(t)$$

большие нуля оценки снизу для I и конечные оценки сверху для S.

Выделены три области на плоскости параметров $\omega, \alpha > 0$, которые для случая $\epsilon_1 = \epsilon_2 = 0$ имеют вид: 1) $\alpha > 2\omega$, где имеет место устойчивость, 2) $\alpha < \sqrt{2}\omega$, где имеет место неустойчивость, 3) $\sqrt{2}\omega \leq \alpha \leq 2\omega$, где устойчивость имеет место только для более узкого класса начальных условий и движения лидера.

Список литературы

1. Prigogine I., Herman R. Kinetic theory of vehicular traffic. — N.Y.: Elsevier, 1971.

2. Helbing D. Traffic and related self-driven many particle systems // Rev. Mod. Phys. — 2001. — 73. — P. 1067–1141.

О НОВОЙ ВЕРСИИ АЛГОРИТМА ПОСТРОЕНИЯ БАЗИСНОГО КОНЕЧНОГО АВТОМАТА

А. А. Мельникова (Димитровград)

В статье приводится новая версия одного из возможных алгоритмов построения базисного конечного автомата, определённого и исследованного в [1] и др. Алгоритм является некоторым изменением алгоритма, приведённого в [2, 3].

Применяемые далее обозначения согласованы с [2, 4]. Дуги автоматов $\widetilde{L}$ и $\widetilde{L^R}$ будем обозначать заглавными греческими буквами,

не совпадающими по написанию с латинскими — до буквы Ξ для автомата $\widetilde{L}$ и начиная с буквы Π для автомата $\widetilde{L^R}$, а также для зеркального к последнему автомата $\left(\widetilde{L^R}\right)^R$. Для некоторой конкретной дуги Γ, идущей из вершины A в вершину B и имеющей пометку $a \in \Sigma$, будем писать $\alpha^a(\Gamma) = A$ и $\beta^a(\Gamma) = B$. Проделаем для каждой буквы a алфавита Σ следующую процедуру. Пусть δ_π^a — помеченные буквой a дуги автомата $\widetilde{L}$ (т.е. элементы множества δ_π), а δ_ρ^a — помеченные буквой a дуги автомата $\widetilde{L^R}$ (т.е. элементы множества δ_ρ). Аналогично сказанному выше, будем таким же образом обозначать соответствующее множество дуг автомата $\left(\widetilde{L^R}\right)^R$.

Рассмотрим бинарное отношение $\#^a \subseteq \delta_\pi^a \times \delta_\rho^a$, определённое следующим образом. Для некоторых $\Gamma \in \delta_\pi^a$ и $\Omega \in \delta_\rho^a$ полагаем $\Gamma \#^a \Omega$ тогда и только тогда, когда для некоторого слова $w \in L$ имеем представление $w = uav$, и при этом:

$$\begin{aligned} &u \in \mathcal{L}^{in}_{\widetilde{L}}(\alpha^a(\Gamma))\,,\ u \in \mathcal{L}^{in}_{\left(\widetilde{L^R}\right)^R}(\alpha^a(\Omega))\,,\\ &v \in \mathcal{L}^{out}_{\widetilde{L}}(\beta^a(\Gamma))\,,\ v \in \mathcal{L}^{out}_{\left(\widetilde{L^R}\right)^R}(\beta^a(\Omega))\,. \end{aligned} \tag{1}$$

Приведённое нами определение отношения $\#^a$ с помощью (1) можно рассматривать как *алгоритм* его построения.

Теорема. *Пусть $\Gamma \in \delta_\pi$ и $\Omega \in \delta_\rho$ — некоторые дуги канонических автоматов для языков L и L^R соответственно. Тогда в базисном автомате $\mathcal{BA}(L)$ имеется дуга*

$$\delta_T\Big(\big(\alpha^a(\Gamma), \alpha^a(\Omega)\big), a\Big) \ni \big(\beta^a(\Gamma), \beta^a(\Omega)\big) \tag{2}$$

тогда и только тогда, когда $\Gamma \#^a \Omega$.

Рассмотрим пример построения базисного автомата с помощью описанного здесь алгоритма. Для этого сначала приведём графы переходов автоматов $\widetilde{L}$ (исходного) и $<L>$ (соответствующего ему); они вместе с обозначениями дуг заглавными греческими буквами даны на рисунках 1 и 2 соответственно:

Теперь рассмотрим букву $a \in \Sigma$ и построим отношение $\#^a$. Наличие восьми элементов этого отношения можно показать с помощью таблицы 1.

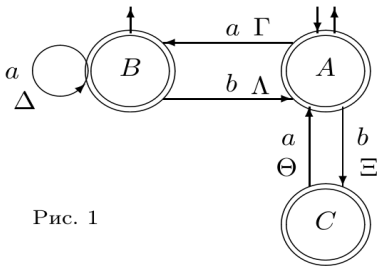


Рис. 1

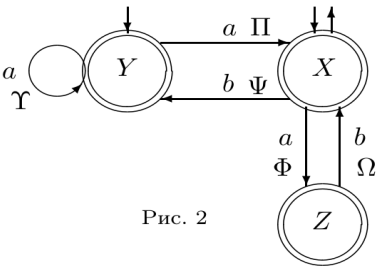


Рис. 2

$\#^a$	Π	Υ	Φ
Γ	a	$\underline{a}a$	ab
Δ	$a\underline{a}$	$a\underline{a}a$	$a\underline{a}b$
Θ	ba	$b\underline{a}a$	

Таб. 1

В таблице 1 парам дуг автоматов $\widetilde{L}$ и $<L>$ поставлены в соответствие слова рассматриваемого языка, и при этом — в случае, когда в слове более одной буквы a, — подчёркнута та буква a этого слова, читая которую автоматы (они оба — однозначные, "unambiguous automata") проходят по этим дугам. (В клетки таблицы можно вписать и другие слова рассматриваемого языка; нами выбраны минимальные по длине.)

Рассмотрим следующую таблицу 2, в которой в клетке, соответствующей паре дуг автоматов $\widetilde{L}$ и $<L>$, запишем дугу базисного автомата согласно (2):

$\#^a$	Π	Υ	Φ
Γ	$(A,Y)\to(B,X)$	$(A,Y)\to(B,Y)$	$(A,X)\to(B,Z)$
Δ	$(B,Y)\to(B,X)$	$(B,Y)\to(B,Y)$	$(B,X)\to(B,Z)$
Θ	$(C,Y)\to(A,X)$	$(C,Y)\to(A,Y)$	

Таб. 2

Для $b\in\Sigma$ построенная аналогичным образом таблица 2×2 отношения $\#^b$ содержит следующие 3 элемента:

$\#^b$	Ψ		Ω	
Λ	aab	$(B,X)\to(A,Y)$	ab	$(B,Z)\to(A,X)$
Ξ	b	$(A,X)\to(C,Y)$		

Таб. 3

Оставшиеся операции, необходимые для окончания построения базисного автомата, выполняются очевидным образом.

Список литературы

1. Vakhitova A. The basis automaton for the given regular language // The Korean Journal of Computational and Applied Mathematics. — 1999. — Vol. 6, No. 3. — P. 617–624.

2. Melnikov B., Melnikova A. A new algorithm of constructing the basis finite automaton // Informatica (Lithuania). — 2002. — Vol. 13, No. 3. — P. 299–310.

3. Мельников Б., Мельникова А. Новый алгоритм построения базисных конечных автоматов // Тезисы докладов XIII Межд. науч. конф. «Проблемы теоретической кибернетики». — 2002. — М.: Изд-во МГУ. — С. 124.

4. Мельникова А. Некоторые свойства базисного автомата // Вестник Воронежского государственного университета. Серия «Физика. Математика». — 2012. — № 2. — С. 184–189.

О СИНТАКСИЧЕСКОМ АНАЛИЗЕ НОРМАТИВНЫХ АКТОВ

Е. М. Перпер (Москва)

Под *синтаксическим анализом* текста будем понимать процесс, который по набору токенов, соответствующих словам предложения, создаёт набор синтаксических отношений между этими словами.

Токен представляет собой тройку, в которую входят: слово; *лемма* — каноническая форма слова (например, для существительного это будет то же слово, но в именительном падеже и единственном числе); набор *морфологических характеристик* (для существительного это род, падеж, число и т.д., для глагола это вид, время и т.д). Процесс построения токенов для всех слов текста называется *морфологическим анализом* текста.

Синтаксическое отношение — это отношение между парой слов предложения. Одно из слов считается в этом отношении главным, а другое — зависимым. У каждого синтаксического отношения есть название, определяемое по частям речи слов, участвующих в отношении, их морфологическим характеристикам и т.д. Например,

отношение между словами «высокое» и «дерево» называется *определительным*. Полный список синтаксических отношений приведён в [1]. Если каждому слову предложения сопоставить вершину графа, а каждому синтаксическому отношению между словами предложения — дугу, ведущую из вершины, которой соответствует главное слово отношения, в вершину, которой соответствует зависимое слово, то получившийся граф окажется ориентированным деревом. Это дерево называется *деревом зависимостей*.

Данная работа посвящена созданию программы, осуществляющей синтаксический анализ предложения, взятого из текста нормативного акта. Данный тип текстов был выбран из-за определённой бедности используемого в этих текстах языка, а также потому, что результаты работы такой программы можно применять на практике — например, для того, чтобы автоматически заполнять формы бухгалтерской отчётности, как это описано в [2].

В описываемой в работе программе синтаксический анализ осуществляется следующим образом. На вход программы поступают токены, полученные морфологическим анализатором, созданным на проекте АОТ [3]. В самой программе имеется список *правил*, которые позволяют находить синтаксические связи между словами. Для каждого токена и каждого правила проверяется, применимо ли это правило к данному токену; если применимо, то создаётся продиктованное этим правилом синтаксическое отношение.

Каждое правило состоит из трёх частей. Первая часть проверяет, подходит ли слово для этого правила: обладает ли оно нужным набором морфологических характеристик. В большинстве случаев значение леммы не проверяется, однако есть и правила, которые работают с конкретными леммами. В тех случаях, когда целью правила является построения синтаксического отношения, в котором рассматриваемое слово было бы зависимым, проверяется также, что слово ещё не является зависимым ни в каком построенном синтаксическом отношении. Объясняется эта проверка просто: каждое слово может входить в какое угодно число синтаксических отношений в качестве главного, но лишь в одно отношение — в качестве зависимого.

Вторая часть заключается в поиске слова, которое может входить в синтаксическое отношение с рассматриваемым словом. В некоторых правилах ищется не одно слово, а несколько, притом таких, что каждое из них могло бы образовывать синтаксические отношения либо с другим найденным словом, либо с рассматриваемым словом.

Наконец, третья часть строит синтаксические отношения между рассматриваемым словом и найденными словами.

Приведём пример правила. Рассмотрим правило, которое для существительного (обозначим его N_1) ищет ближайшее находящееся

после него в предложении слово, не являющееся прилагательным в родительном падеже (обозначим это слово N_2). Пусть такое слово найдено и является существительным в родительном падеже. Если между ним и N_1 в предложении нет запятых, точек с запятой и двоеточий, а закрывающих скобок не меньше, чем открывающих, то между N_1 и N_2 создаётся *квазиагентивное* синтаксическое отношение, в котором главным словом является N_1, а зависимым — N_2. Это правило, например, строит синтаксическое отношение между словами «объектам» и «средств», а также между словами «средств» и «организаций» в предложении «По объектам основных средств некоммерческих организаций амортизация не начисляется».

В настоящий момент в программе описано 31 правило, позволяющее проводить синтаксический анализ предложений нормативного акта о бухгалтерском учёте ПБУ 6/01. Продолжается тестирование программы на предложениях из нормативных актов и пополнение списка правил в тех случаях, когда имеющихся правил недостаточно для построения дерева зависимостей, однако такие случаи достаточно редки.

Автор выражает благодарность научному руководителю, профессору, д.ф.-м.н. Э. Э. Гасанову за постановку задачи и помощь в научной работе.

Список литературы

1. Синтаксически размеченный корпус русского языка: информация для пользователей. — Электронный ресурс: `www.ruscorpora.ru/instruction-syntax.html`.

2. Кудрявцев В. Б., Гасанов Э. Э., Перпер Е. М. Автоматическая генерация компьютерной программы, моделирующей нормативно-правовой акт // Интеллектуальные системы. Теория и приложения — 2014. —Т. 18, вып. 2. — С. 133–156.

3. Автоматическая обработка текста. — Электронный ресурс: `www.aot.ru`.

ЛИНЕЙНО РЕАЛИЗУЕМЫЕ АВТОМАТЫ

С. Б. Родин (Москва)

На практике часто необходимо решать задачу перехода от автоматного описания функционирования на язык схем. Например, при логическом синтезе чипов на первом этапе функционирование чипа описывается как конечный автомат. Переход к описанию на языке

схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $\{0,1\}$. При этом важно выбрать кодирование, при котором достигается возможно меньшая сложность схемы. Введем некоторые понятия.

Определение. Нумерованным автоматом назовем пятерку $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, где A-входной алфавит, $Q = \{0...n-1\}$, B-выходной алфавит, φ — функция переходов, ψ — функция выходов.

В работе изучаются автоматы с входным алфавитом $A = E_2$ и выходным алфавитом $B = E_2$

Определение. Кодированием множества $Q = \{0...n-1\}$ назовем взаимоднозначное отображение $F : \{0...n-1\} \to {E_2}^k$. Каждое кодирование F для автомата на множестве Q порождает булевский оператор [1] $\phi : {E_2}^{k+1} \to {E_2}^{k+1}$, где

$$\phi(a, \alpha_1, ..., \alpha_k) = (F(\varphi(a, F^{-1}(\alpha_1, ..., \alpha_k))), \psi(a, F^{-1}(\alpha_1, ..., \alpha_k))),$$

$$a \in A, \alpha_i \in E_2.$$

Данный оператор может быть рассмотрен как набор $k+1$ булевских функций, зависящих от $k+1$ переменной. Обозначим этот набор через $\mathcal{F}_{\mathfrak{A}}(F)$.

Определение. Если для заданного нумерованного автомата $\mathfrak{A}$ существует кодирование F, такое что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики, назовем такой автомат линейно реализуемым посредством кодирования F,или просто линейно реализуемым.

Обозначим через $X_{\mathfrak{A}} = \{s : Q \to Q \,|\, \exists a \in E_2, s(q) = \varphi(a, q)$ для любого $q \in Q\}$, а через $S_{\mathfrak{A}} =< X_{\mathfrak{A}} >$, замыкание множества $X_{\mathfrak{A}}$ относительно операции умножения подстановок [4]. Множество $S_{\mathfrak{A}}$ будем называть внутренней полугруппой переходной системы V, а $X_{\mathfrak{A}}$ — порождающим множеством внутренней полугруппы.

Поскольку входным алфавитом является E_2, то множество $X_{\mathfrak{A}}$ состоит из двух элементов. Обозначим через p_0 подстановку, соответствующую входному символу 0, через p_1 — подстановку, соответствующую входному символу 1 [4].

Определение Пусть задана подстановка $p : \{0, ..., n-1\} \to \{0, ..., n-1\}$. Положим $M_q = \{i \in \{0, ..., n-1\} | p(i) = q\}$. Через $\widetilde{p} : 2^{\{0,...,n-1\}} \to \{0, ..., n-1\}$ обозначим отображение такое, что

$$\widetilde{p}(M) = \begin{cases} q, \text{ если } M = M_q \\ \text{неопределено, в противном случае.} \end{cases}$$

Теорема 1. *Пусть задан нумерованный автомат* $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$, *где* $Q = \{0, \ldots, n-1\}$, *такой что* φ *не зависит существенным образом от входного символа.* $\mathfrak{A}$ *линейно реализуем, тогда и только тогда,когда функции, реализованные в состояниях автомата, имеют одинаковое число существенных переменных* (*то есть во всех состояниях реализуются либо* $\{x, \overline{x}\}$, *либо* $\{0, 1\}$).

Теорема 2. *Пусть задан нумерованный автомат* $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$, *где* $Q = \{0, \ldots, n-1\}$, *такой что* φ *зависит существенным образом от входного символа.* $\mathfrak{A}$ *линейно реализуем посредством кодирования* $F : Q \to E_2^k$, *тогда и только тогда,когда*

- $\widetilde{p_0}$ *и* $\widetilde{p_1}$ *— имеют одинаковую область определения;*
- $p = \widetilde{p_0}^{-1} \cdot \widetilde{p_1}$ *является перестановкой;*
- $p(q) \neq q$, $\forall q \in Q$*;*
- $p(q)$ *есть произведение независимых транспозиций;*
- *функции, реализованные в состояниях автомата, имеют одинаковое число существенных переменных* (*то есть во всех состояниях реализуются либо* $\{x, \overline{x}\}$, *либо* $\{0, 1\}$).

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

2. Лидл Р., Нидеррайтер Г. Конечные поля. — М.: Мир, 1988.

3. Карагаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1982.

4. Арбиб М. А. Декомпозиция автоматов и расширение полугрупп // Алгебраическая теория автоматов, языков и полугрупп — М.: «Статистика», 1975. — С. 46–64.

5. Родин С. Б. Линейно реализуемые переходные системы // Интеллектуальные системы. — Т. 14, вып. 1–4. — С. 491–502.

Секция «Дискретная геометрия»

О ТИПОВЫХ ЧИСЛАХ ГИПЕРПОВЕРХНОСТЕЙ КЕНМОЦУ И САСАКИ В СПЕЦИАЛЬНЫХ ЭРМИТОВЫХ МНОГООБРАЗИЯХ

М. Б. Банару (Смоленск)

Эрмитова геометрия (или геометрия почти эрмитовых многообразий) имеет теснейшие связи со многими другими областями математики. Например, относительно недавно в ней нашел приложения такой важнейший раздел дискретной математики как теория графов [1, 2]. Другое содержательное и интересное приложение дискретной математики в теории почти эрмитовых многообразий — характеризация гиперповерхностей этих многообразий в терминах типовых чисел (характеризация Такаджи—Курихары). В данной работе рассматривается именно такая характеризация гиперповерхностей Сасаки и Кенмоцу специальных эрмитовых (special Hermitian, SH-) многообразий.

Почти контактной метрической структурой на многообразии N называется [3] система тензорных полей $\{\Phi, \xi, \eta, g\}$ на этом многообразии, для которой выполняются условия:

$$\eta(\xi) = 1;\ \Phi(\xi) = 0;\ \eta \circ \Phi = 0;\ \Phi^2 = -id + \xi \otimes \eta;$$

$$\langle \Phi X, \Phi Y \rangle = \langle X, Y \rangle - \eta(X)\eta(Y),\ X, Y \in \aleph(N).$$

Здесь Φ — поле тензора типа $(1, 1)$, ξ — векторное поле, η — ковекторное поле, $g = \langle \cdot, \cdot \rangle$ — риманова метрика, $\aleph(N)$ — модуль гладких векторных полей на многообразии N. Также известно, что многообразие, допускающее почти контактную метрическую структуру, нечетномерно и ориентируемо [3].

К числу наиболее содержательных и интересных видов почти контактных метрических структур относятся структуры Кенмоцу и Сасаки, которые, как известно [4], характеризуются тождествами

$$\nabla_X(\Phi)Y = \langle \Phi X, Y \rangle \xi - \eta(Y)\Phi X,$$

$$\nabla_X(\Phi)Y = \langle X, Y\rangle\,\xi - \eta(Y)X,\ \ X, Y \in \aleph(N),$$

соответственно. Многообразия Кенмоцу и Сасаки и их различные обобщения — одна из самых популярных тематик современной контактной геометрии. Такие многообразия интенсивно исследуются как с точки зрения дифференциальной геометрии, так и теоретической физики [3]. В этой области работают известнейшие современные геометры, в частности Д. Блэр (США), В. Ф. Кириченко (Россия), Г. Питиш (Румыния) и М. М. Трипати (Индия), а также многие другие математики из разных стран.

В. Ф. Кириченко обратил внимание на то, что несмотря на внешнее сходство тождеств, определяющих структуры Сасаки и Кенмоцу, свойства многообразий Кенмоцу в определенном смысле противоположны свойствам сасакиевых многообразий [4].

Не оспаривая ни в коей мере это мотивированное утверждение, заметим только, что и сходство между свойствами многообразий Сасаки и Кенмоцу тоже немалое. Например, результаты из статей [5] и [6] о гиперповерхностях Кенмоцу и Сасаки 6-мерных эрмитовых подмногообразий алгебры октав выглядят абсолютно идентично.

Приведем еще два результата, которые с очевидностью говорят о сходстве некоторых свойств структур Кенмоцу и Сасаки.

Теорема 1. *Гиперповерхность Кенмоцу SH-многообразия является минимальной в том и только том случае, когда ее типовое число четно.*

Теорема 2. *Гиперповерхность Сасаки SH-многообразия является минимальной в том и только том случае, когда ее типовое число четно.*

Из этих теорем вытекает ряд геометрических следствий, связанных с существованием структур Кенмоцу и Сасаки на минимальных гиперповерхностях специальных эрмитовых многообразий.

Работа является продолжением исследований автора, рассматривавшего ранее характеризации Такаджи–Курихары почти контактных метрических гиперповерхностей почти эрмитовых многообразий (см., например [7–11]).

Список литературы

1. Carriazo A., Fernandez L.M. Submanifolds associated with graphs // Proc. Amer. Math. Soc. — 2004. — V. 132(11). — P. 3327–3336.

2. Carriazo A., Fernandez L.M., Rodriguez-Hidalgo A. Submanifolds weakly associated with graphs // Proc. Indian Acad. Sci. (Math. Sci.). — 2009. — V. 119, is. 3. — P. 297–318.

3. Кириченко В. Ф. Дифференциально-геометрические структуры на многообразиях. — М.: МПГУ, 2003.

4. Кириченко В. Ф. О геометрии многообразий Кенмоцу // ДАН. — 2001. — Т. 80, № 5. — С. 585–587.

5. Банару М. Б. Аксиома гиперповерхностей Кенмоцу для 6-мерных эрмитовых подмногообразий алгебры Кэли // Сибирский математический журнал. — 2014. — Т. 55, № 2. — С. 261–266.

6. Банару М. Б. Аксиома сасакиевых гиперповерхностей и 6-мерные эрмитовы подмногообразия алгебры октав // Математические заметки. — 2016. — Т. 99, № 1. — С. 140–144.

7. Банару М. Б. О типовом числе слабо косимплектических гиперповерхностей приближенно келеровых многообразий // Фундаментальная и прикладная математика. — 2002. — Т. 8, вып. 2. — С. 357–364.

8. Банару М. Б. О типовом числе косимплектических гиперповерхностей 6-мерных эрмитовых подмногообразий алгебры Кэли // Сибирский математический журнал. — 2003. — Т. 44, № 5. — С. 981–991.

9. Банару М. Б. О типовых числах почти контактных метрических гиперповерхностей почти эрмитовых многообразий // Материалы VIII Международного семинара «Дискретная математика и её приложения». — М: Изд-во механико-математического ф-та МГУ, 2004. — С. 379–381.

10. Банару М. Б. Почти контактные метрические гиперповерхности с типовым числом 1 или 0 в приближенно келеровых многообразиях // Вестник Московского университета. Сер. 1. Математика. Механика. — 2014. — № 3. — С. 60–62.

11. Банару М. Б. О почти контактных метрических гиперповерхностях с типовым числом 1 в 6-мерных келеровых подмногообразиях алгебры Кэли // Известия высших учебных заведений. Математика. — 2014. — № 10. — С. 13–18.

ГИПЕРБОЛИЧЕСКИЕ ЛИНЗОВЫЕ 3-МНОГООБРАЗИЯ НАД ПЛАТОНОВОЙ ПОВЕРХНОСТЬЮ $\{5, 5\}$ РОДА 4

Ф. Л. Дамиан (Кишинев),
В. С. Макаров, П. В. Макаров (Москва)

В сообщениях [4, 5] был обоснован метод построения гиперболических 3-многообразий исходя из предположения наличия в них вполне геодезического подмногообразия, геометрия которого известна.

Впервые такой пример был нами описан при изучении симметрических 3-подмногообразий 4-многообразия Дэвиса [2, 3]. Этот пример послужил толчком к исследованию некоторых икосаэдрических гиперболических многообразий с вполне геодезическим краем [6], для которых краем оказалась платонова поверхность [1] рода 4 и которая изящно описывается инциденциями граней большого звездного додекаэдра $\{5, 5/2\}$. Напомним, что в [6] многообразия с таким краем строились из ортогонально усеченных ромбического триаконтаэдра и икосаэдра. Если эти фундаментальные многогранники разрезать на равные многогранники призматического типа и собрать их над платоновай картой края, то мы получем 2 "многогранника", схема отождествления граней которых перенесена с указанных выше многогранников. Они аналогичны бесконечным эквидистантным многогранникам (в данном случае правильным [10]), которые будем называть конечными линзовыми многогранниками.

С другой стороны, построение этих же примеров можно начать с образования конечного "линзового" многогранника: берется прямое произведение поверхности на отрезок и полученный обьект ограняется в соответствии с одной из платоновых карт базы. При таком подходе многообразие из ортогонально усеченного ромбического триаконтаэдра получается как линзовый полиэдр с двугранными углами $2\pi/3$ над картой $\{4, 5\}$ и схемой отождествления 2-граней "тор из шестиугольника". Многообразие из ортогонально усеченного икосаэдра представленно линзой над картой $\{5, 5\}$ (в дуальном ее положении) и схемой отождествления, перенесенной с многообразия Зейферта—Вебера [7], посредством звездного $\{5, 5/2\}$. При этом образуются несущественные циклы ребер (по три). В обоих примерах плоскости граней, инцидентных вершине, принадлежат эллиптической связке. Если через многогранник $\{5, 5/2\}$ перенести на карту в базе схему отождествления сферического пространства додекаэдра Пуанкаре [8], то на $\{5, 5\}$ в циклах собирается по пять ребер и следовательно для значения двугранного угла в $2\pi/5$ вершины линзового многогранника должны выйти за абсолют и быть ортогонально усечены. В результате образуется новая компонента края, идентичная базе, а плоскости граней определявших вершину, принадлежат гиперболической связке [11].

На рассматриваемой поверхности рода 4 кроме платоновых карт $\{5, 5\}$ и $\{4, 5\}$, имеется еще $\{5, 4\}$. Для параболического случая, когда вершины линзового многогранника на абсолюте, мы будем использовать в базе карту $\{5, 4\}$ на той же поверхности. У такой линзы с параболическими вешинами все двугранные углы прямые. Его экви-

дистантную границу можно окрасить шахматно и тогда любое парное отождествление “белых” граней дает геодезическую границу из “черных” граней.

Мы остановились на самых симметричных схемах отождествления. Если воспользоваться, при опосредованном через многогранник $\{5, 5/2\}$, схемой отождествления “белых” граней, индуцированной с проективной плоскости, то “черные” грани образуют шесть идентичных компонент края, коими являются сферы с пятью каспами. Если применить схему отождествления, перенесенную с многообразия Пуанкаре, то граница из “черных” граней окажется однокомпонентной и будет представлена схемой инциденций граней звездного многогоранника $\{5, 5/2\}$ со всеми вершинами на абсолюте. При использовании схемы отождествления Зейферта—Вебера, через $\{5, 5/2\}$, граница получаемого многообразия так же однокомпонентна, но комбинаторно представлена многогранником $\{5, 3\}$ со всеми вершинами на абсолюте. Отметим что во всех случаях образующаяся граница является вполне геодезической.

Если в рассмотренных случаях взять по два идентичных экземпляра линзовых многообразий, то легко избавится от края. Однако возможностей комбинирования различных многообразий и способов устранения геодезических краев огромное множество, и следовательно можно построить счетное количество новых гиперболических многообразий конечного обьема.

Список литературы

1. Coxeter H. S M. Regular polytopes. — N.-Y.: 1963.

2. Davis M. W. A hyperbolic 4–manifold // Proceedings of the American Mathematical Society. — 1985. — Vol. 93, no. 2. — P. 325–328.

3. Дамиан Ф. Л. К построению гиперболических четырехмерных многообразий // Геометрия дискретных групп. Математические исследования. — 1990. — Вып. 119. — С. 79–84.

4. Damian F., Makarov V. S. On lens polytopes // International Seminar on Discrete Geometry. 2002. Moldova State University. — P. 32–35.

5. Makarov V. S., Damian F. L., Makarov P. V. Compact lens and hyperbolic manifolds // XIII Internat. Conf. ”Algebra, Number Theory and Discrete Geometry” dedicated to S.S.Ryshkov. 2015. Tula Pedagog. St. Univ. — P. 305–307.

6. Дамиан Ф. Л., Макаров В. С. О трехмерных гиперболических многообразиях с икосаэдрической симметрией // Buletunul Academiei de Ştiinţe a Republicii Moldova. Matematica. — 1995. — № 1. — P. 82–89.

7. Seifert H., Weber C. Die beiden Dodekaederräume // Math. Ztschr. — 1933. — Bd. 35. — S. 237–253.

8. Зейферт Г., Трельфалль В. Топология. — М.Л.: ГТТЛ, 1938.

9. Damian F. L., Makarov V. S. Star polytopes and hyperbolic three-manifolds // Buletunul Academiei de Ştiinţe a Republicii Moldova. Matematica. — 1998. — 2. — P. 102–108.

10. Makarov V. S. Geometric methods of construction of discrete groups of motions of a Lobachevskii space. Itogi Nauki i Tekhniki. Ser. Probl. Geom., VINITI, Moscow. Vol.15. — 1983. — P. 3–59.

11. Damian F., Makarov V. S., Makarov P. V. Star complexes over the regular maps Int. Conf. "Geometry, Topology, and Applications". Yaroslavl, Russia. 2013. — P. 27–32.

ЖЁСТКИЕ ФРАГМЕНТЫ НА ПРОСТЫХ ТРЁХМЕРНЫХ МНОГОГРАННИКАХ С НЕ БОЛЕЕ ЧЕМ ШЕСТИУГОЛЬНЫМИ ГРАНЯМИ

Н. Ю. Ероховец (Москва)

В работе исследуются фрагменты, ограниченные простыми рёберными циклами на поверхности простых трёхмерных многогранников с не более чем шестиугольными гранями. Обозначим множество таких многогранников через $\mathcal{P}_6$, а множество фрагментов на них через $\mathcal{D}_6$. Известно, что каждый такой фрагмент гомеоморфен кругу, поэтому является разбиением круга на многоугольники. Пусть p_k — число k-угольных граней простого многогранника P. Из формулы Эйлера получатся следующая известная формула

$$3p_3 + 2p_4 + p_5 = 12 + \sum_{k \geqslant 7}(k-6)p_k.$$

Назовём *дефектом* многогранника P или фрагмента D величину $\pi = 3p_3 + 2p_4 + p_5$. Если P имеет не более, чем шестиугольные грани, то $\pi(P) = 12$.

Фуллереном называется простой трёхмерный многогранник, у которого все грани являются пятиугольниками или шестиугольниками. Для любого фуллерена $\pi(P) = p_5(P) = 12$.

3-*поясом* простого трёхмерного многогранника называется набор граней (F_i, F_j, F_k), такой что $F_i \cap F_j, F_j \cap F_k, F_k \cap F_i \neq \varnothing$ и $F_i \cap F_j \cap F_k = \varnothing$. k-*поясом*, $k \geqslant 4$, называется циклическая последовательность двумерных граней $(F_{i_1}, \ldots, F_{i_k})$, в которой две грани пересекаются тогда и только тогда, когда они при обходе по циклу следуют друг за другом.

Рассмотрим замощение плоскости $\mathbb{R}^2$ правильными шестиугольниками. Для трёх шестиугольников с общей вершиной возьмём векторы $\mathbf{a}_1$ и $\mathbf{a}_2$, соединяющие центр одного шестиугольника с центрами остальных шестиугольников. Для неотрицательных целых чисел (p, q), $p \geqslant q$, рассмотрим вектор $\mathbf{c} = p\mathbf{a}_1 + q\mathbf{a}_2$. Факторизация плоскости по вектору $\mathbf{c}$ задаёт разбиение цилиндра на шестиугольники. Рассмотрим замкнутую цепочку граней на цилиндре, которая получается, если от заданного шестиугольника пройти p раз вдоль вектора $\mathbf{a}_1$ и q раз вдоль вектора $\mathbf{a}_2$ в произвольном порядке. Граница этой цепочки состоит из двух простых рёберных циклов, которые получаются друг из друга переносом на вектор $\mathbf{a}_1 - \mathbf{a}_2$. Если поверхность многогранника $P \in \mathcal{P}_6$ комбинаторно эквивалентна поверхности, получающейся разрезанием цилиндра вдоль двух таких параллельных циклов и заклеиванием циклов фрагментами из $\mathcal{D}_6$ с $\pi(D) = 6$, то P называется *нанотрубкой типа* (p, q).

Основной результат можно сформулировать следующим образом.

Теорема. *Для любого $k \geqslant 3$ существует конечный набор фрагментов $\mathcal{Q}_k \subset \mathcal{D}_6$ с $\pi(Q) = 6$ для всех $Q \in \mathcal{Q}_k$, такой что семейства многогранников $\mathcal{S}_k \subset \mathcal{P}_6$, $\mathcal{S}_3 \subset \mathcal{S}_4 \subset \cdots \subset \mathcal{S}_k$, где каждый многогранник в $\mathcal{S}_k \setminus \mathcal{S}_{k-1}$ состоит из последовательности $r \geqslant 0$ примыкающих друг к другу k-поясов шестиугольников и двух примыкающих к ним фрагментов из $\mathcal{Q}_k$, обладают следующими свойствами:*

1) *все многогранники в $\mathcal{S}_k$, кроме конечного числа, являются нанотрубками*;

2) *многогранник $P \in \mathcal{P}_6$ принадлежит $\mathcal{S}_k$ тогда и только тогда, когда он содержит фрагмент из $\mathcal{Q}_k$*;

3) *Многогранник $P \in \mathcal{P}_6$ принадлежит хотя бы одному семейству S_k тогда и только тогда, когда он содержит фрагмент с дефектом, равным шести.*

4) *Любой фуллерен P имеет фрагмент, состоящий из шести пятиугольников, и принадлежит хотя бы одному семейству $\mathcal{S}_k$, $k \geqslant 5$.*

Таким образом, фрагменты из $\mathcal{Q}_k$ являются *жёсткими*, то есть накладывают жёсткие условия на комбинаторику многогранника P, содержащего один из таких фрагментов.

Пример 1. Множество $\mathcal{Q}_3$ состоит из шести фрагментов. Первый фрагмент состоит из трёх сходящихся в одной вершине четырёхугольников. Второй и третий фрагмент получаются из первого последовательной срезкой одной и двух внутренних вершин. Эти фрагменты отвечают нанотрубкам типа $(3, 0)$. Четвёртый фрагмент состоит из сходящихся в одной вершине треугольника, четырёхугольника и пятиугольника. Пятый фрагмент получается из него срезкой внутренней вершины. Шестой фрагмент получается из пятого срезкой вершины, в которой сходятся треугольник, четырёхугольник и пятиугольник. Эти фрагменты отвечают нанотрубкам типа $(2, 1)$.

Пример 2. Фрагмент из пятиугольника, окружённого пятью пятиугольниками, является жёстким для фуллеренов: если фуллерен содержит такой фрагмент, то он является нанотрубкой типа $(5, 0)$ и получается из двух таких фрагментов вставкой любого числа 5-поясов шестиугольников между ними.

Доказательство пунктов 1), 2), 3) теоремы получается из описания структуры k-поясов и простых рёберных циклов в работе [1] (теорема 3 и теорема 4).

Для доказательства пункта 4) мы используем следующую лемму и её следствие.

Лемма. *Для каждого трёхмерного простого многогранника с m гипергранями существует последовательность фрагментов, отличающихся на одну двумерную грань, начиная с одной грани, заканчивая $(m-1)$ гранью.*

Этот результат следует из шеллинговости многогранников, а в случае многогранников из $\mathcal{P}_6$ может быть доказан непосредственно.

Следствие. *Для любого фуллерена существует фрагмент D с дефектом $\pi(D) = 6$.*

Отметим, что существуют многогранники в $\mathcal{P}_6$, не имеющие фрагментов с дефектом, равным шести. Примером является треугольная призма.

Работа выполнена при частичной финансовой поддержке гранта победителям конкурса "Молодая математика России".

Список литературы

1. Ероховец Н. Ю. k-пояса и простые рёберные циклы простых многогранников с не более, чем шестиугольными гранями // Дальневосточный математический журнал. — 2015. — Т. 15, № 2. —С. 197–213.

О ШАРНИРНИКАХ С ОДИНАКОВЫМ ВНУТРЕННИМ НАПРЯЖЕНИЕМ

М. Д. Ковалёв (Москва)

Рассматриваем закреплённые шарнирно рычажные конструкции в евклидовой плоскости. Структура такой конструкции определяется *шарнирной структурной схемой* (ШСС) — абстрактным связным графом $G(V, E)$ без петель и кратных рёбер, имеющим вершины двух видов $V = V_1 \cup V_2$ [1]. Вершинам из V_1 отвечают свободные шарниры (вращательные пары), вершинам из V_2 — шарниры конструкции, закреплённые в плоскости. Причём, вершины из V_2 смежны лишь вершинам из V_1. Рёбрам графа отвечают рычаги конструкции. Эти рычаги могут свободно вращаться вокруг соединяющих их шарниров. *Закрепленной шарнирной схемой* (ЗШС) в плоскости называют ШСС, каждой закрепленной вершине $v_i \in V_2$ которой сопоставлена точка $p_i \in R^2$. Задание ЗШС определяет так называемой *рычажное отображение*. Пусть $V_1 = \{v_1, \ldots, v_m\}$, $|E| = r$, тогда рычажное отображение $F : R^{2m} \to \mathcal{R}^r$, задаётся формулами $d_{ij} = (p_i - p_j)^2, v_i v_j \in E$, где в правой части стоят скалярные квадраты векторов. Оно играет ключевую роль в геометрии шарнирных механизмов. Пусть $p_i \in R^2$, $1 \leq i \leq m$. Точка $p = (p_1, p_2, \ldots, p_m) \in R^{2m}$ называется *шарнирником*. Ей отвечает либо шарнирная ферма, либо определённое положение шарнирного механизма. Шарнирник, у которого хотя бы один рычаг имеет нулевую длину (и совпадают смежные шарниры), мы называем *сократимым*, в противном случае — *несократимым*. Если $\dim F(R^{2m}) = r$, то рычажное отображение F и соответствующая ЗШС называются *правильными*. Правильная ЗШС в R^2 называется *изостатической*, если $2m = r$. Конструкции с такими ЗШС чаще всего применяются на практике.

Пусть $p_i p_j$ рычаг с концевыми шарнирами p_i, $p_j \in R^2$. Силу, с которой этот рычаг действует на шарнир p_i, принято записывать как $\omega_{ij}(p_i - p_j)$, где скаляр ω_{ij} называется *внутренним напряжением рычага* $p_i p_j$ [2]. Величины $\omega_{ij} = \omega_{ji}$ напряжений указывают меру напряженности рычагов: если $\omega_{ij} < 0$, то рычаг $p_i p_j$ растянут, если же $\omega_{ij} > 0$, то он сжат. Условие равновесия сил, приложенных к i-му свободному шарниру со стороны смежных шарниров шарнирника, имеет вид

$$\sum_j \omega_{ij}(p_i - p_j) = 0,$$

где суммирование проводится по всем шарнирам смежным в ШСС

i-му. *Внутренние напряжения* шарнирника $\omega=\{\omega_{ij}\}$ определяются как нетривиальные решения однородной системы линейных уравнений:

$$\sum_j \omega_{ij}(p_i - p_j) = 0, \qquad 1 \le i \le m,$$

при заданных положениях p_i шарниров. Механический смысл этой системы суть равновесие сил в каждом свободном шарнире конструкции. Если система имеет лишь тривиальное решение, то говорим, что шарнирник *не допускает внутренних напряжений*. Если система имеет такое решение $\omega=\{\omega_{ij}\}$, что $\omega_{ij} \neq 0$ для любого $(i,j) \in E$, то внутреннее напряжение ω называем *полным*.

Если в этой системе начать считать напряжения $\omega = \{\omega_{ij}\}$ известными, а положения свободных шарниров неизвестными, то для нахождения последних получим систему линейных уравнений:

$$(\sum_{j,(v_i,v_j)\in E} \omega_{ij})p_i - \sum_{j,(v_i,v_j)\in E_1} \omega_{ij}p_j = \sum_{j,(v_i,v_j)\in E_2} \omega_{ij}p_j^0, \qquad 1 \le i \le m.$$

здесь E_2 — множество рёбер, смежных закреплённым шарнирам, $E_1 = E \setminus E_2$. Матрицу $\Omega(\omega)$ этой системы называют матрицей *напряжений*. Пусть для заданного шарнирника $p^0 = \{p_1^0, ..., p_m^0\}$ с закреплением $p_{m+1}^0, ..., p_{m+n}^0$ имеем $p(\omega) = (p_1(\omega), ..., p_m(\omega))$ — множество всех решений последней системы уравнений. Оно представляет собой линейное многообразие размерности $2\,\mathrm{coRank}\,\Omega(\omega)$ в R^{2m}.

Рассмотрим две бесконечных последовательности ШСС: D_m и M_m [3]. Вообще говоря, им отвечают изостатические ЗШС. Схема D_m состоит из цепи $p_1p_2\dots p_m$, составленной из свободных шарниров, и присоединённых к ней закреплённых шарниров $q_0, q_1, \dots, q_m$, причём к шарниру p_1 присоединены закреплённые шарниры q_0 и q_1, а к шарниру $p_i,\ i > 1$ — шарнир q_i. Схема M_m состоит из замкнутого многоугольника $p_1p_2\dots p_m$, с вершинами в свободных шарнирах, и присоединённых к нему рычагами закреплённых шарниров $q_1, \dots, q_m$, причём к шарниру p_i присоединён закреплённый шарнир q_i. Назовём ЗШС *распрямлённой*, если все её закреплённые шарниры лежат на прямой, и *нераспрямлённой* в противном случае. Два шарнирника $p' \neq p$ с одной ЗШС назовём *изометричными*, если $F(p') = F(p)$.

Если ЗШС распрямлена и все её закреплённые шарниры лежат на прямой L, то для любого шарнирника p, не лежащего на L, имеется изометричный шарнирник $p' \neq p$ зеркально симметричный p отно-

сительно L. Такие изометричные шарнирники с одинаковыми полными внутренними напряжениями существуют уже для распрямлённой ЗШС D_2.

Теорема 1. *Для нераспрямлённых изостатических ЗШС типа D_m и M_m невозможны изометричные несократимые шарнирники $p' \neq p$, допускающие одно и то же полное напряжение ω.*

Полнота напряжения необходима. Действительно, возьмём шарнирник p со схемой D_2, шарнир p_1 которого лежит посередине между закреплёнными шарнирами q_0 и q_1, а шарнир p_2 не лежит на прямой q_2p_1. У этого шарнирника имеется неполное внутреннее напряжение ненулевое и одинаковое на рычагах q_0p_1 и q_1p_1, и нулевое на рычагах p_1p_2 и q_2p_2. Имеется изометричный ему шарнирник p', получаемый из p отражением шарнира p_2 от прямой q_2p_1, допускающий то же самое внутреннее напряжение.

Существуют плоские нераспрямлённые изостатические ЗШС, для которых имеются изометричные шарнирники, допускающие одно и то же полное напряжение. Для них справедливы следующие теоремы.

Теорема 2. *Если в многообразии $p(\omega)$ имеется два изометричных шарнирника, то число пар изометричных шарнирников в $p(\omega)$ бесконечно.*

Теорема 3. *В случае* $\operatorname{coRank}\Omega(\omega) = 1$, *если в двумерной плоскости $p(\omega)$ имеется два различных изометричных шарнирника, то множество шарнирников, не имеющих изометричного в $p(\omega)$, есть прямая.*

Список литературы

1. Ковалев М. Д. Геометрическая теория шарнирных устройств // Изв. РАН Сер. матем. — 1994. — 58 (1). — С. 45–70.

2. Ковалев М. Д. О восстановимости шарнирников по внутренним напряжениям // Изв. РАН Сер. матем. — 1997. — 61 (4). — С. 37–66.

3. Ковалев М. Д. Определитель матрицы напряжений и восстановимость шарнирных конструкций по внутренним напряжениям // Изв. РАН Сер. матем. — 2016. — 80 (3). — С. 43–66.

ГЕОМЕТРИЯ БИКРИСТАЛЛОВ И ТРЁХМЕРНЫЕ СФЕРИЧЕСКИЕ МНОГООБРАЗИЯ

Я. В. Кучериненко, В. С. Макаров (Москва)

Симметрия двойника характеризуется точечными трёхмерными группами сросшихся кристаллов и их взаиморасположениями [1]. Изучение взаимных ориентаций в бикристаллах (и в любых парах фигур, имеющих конечные группы симметрии) [2], привело нас к дискретным группам трёхмерной сферы [3], а в данной работе – к сферическим многообразиям.

Исследования, результаты которых изложены ниже, были стимулированы работой [4] и указанными в ней нерешёнными вопросами. Все дискретные группы, действующие на S^3 без неподвижных точек, классифицируютя в [4] по пяти счётным сериям: $C_n \times C_m$, $D_n^* \times C_m$, $T^* \times C_m$, $O^* \times C_m$, $I^* \times C_m$, (где n и m выбираются так, чтобы перемножаемые группы, помимо симметрии в центре S^3, не содержали поворотов с одинаковыми угловыми характеристиками). Для первых двух из них Постников дал описание областей Дирихле в виде линз и правильных призм, а для остальных трёх серий – только для случаев $T^* \times C_1$, $O^* \times C_1$ и $I^* \times C_1$ – в виде октаэдра, усечённого куба и додекаэдра, (последний случай соответствует известному многообразию Пуанкаре).

Для практических целей материаловедения бывает важно знать равноменность распределения ориентаций кристаллических зёрен в образце, для описания каждой из которых обычно выбирают поворот с минимальным углом [5]. Области таких минимальных поворотов имеющие форму выпуклых многогранников в пространстве Родригеса [5, 6], как оказалось, являются центральными (гномоническими) проекциями граней изоэдральных разбиений трёхмерной сферы [3, 7] на касательную трёхмерную гиперплоскость (разбиение является изоэдральным т.к. на ней действует группа, связывающая в одну орбиту все различные описания одной и той же разориентировки кристаллов [3]).

Изучение не одной клетки, а всего разбиения Дирихле с действующей на нём группой позволило обнаружить, что группа стабилизатора любой точки орбиты изоморфна точечной группе симметрии кристаллического двойника [3]. Кроме того на S^3 при рассмотрении двойников и сростков любых двух *одинаковых* кристаллов всегда появляется центр симметрии в точке $(0, 0, 0, 1)$ (следует из [2]), отвечающей тождественному повороту. Поэтому, для получения групп без неподвижных точек, нам понадобится пара *разных* кристаллов (фи-

гур), имеющих только поворотную симметрию и не имеющих одинаковых поворотных симметрий. Выбор разных исходных установок кристаллов относительно координатной системы не приводит к другой группе (или другой орбите), но лишь к их другой ориентации на S^3 [3]. Если при этом всякий раз будем брать $(0,0,0,1)$ в качестве начальной точки, то получим уже новые орбиты и таким способом сможем задать любую из них, что было использовано нами в качестве практического приёма для сравнения групп на S^3 и их факторпространств. Это позволило нам рассмотреть результаты работы [4] с разных сторон: найти примеры групп с разными многогранники Дирихле и, в то же время, для некоторых разных групп получить одинаковые орбиты и одинаковые разбиения Дирихле:

$C_6^* \times C_1$	$C_3^* \times C_2^*$, $2 \parallel 3$:	12 линз, толщиной $\pi/6$
$D_3^* \times C_1$	$C_3^* \times C_2^*$, $2 \perp 3$:	12 6-призм толщиной $\pi/3$
$D_6^* \times C_1$	$D_2^* \times C_3^*$, $2 \parallel 3$:	24 12-призм толщиной $\pi/6$
$T^* \times C_1$	$D_2^* \times C_3^*$, 3 как в кубе:	24 октаэдра { 3,4,3 }
$D_{12}^* \times C_1$	$D_4^* \times C_3^*$, $4 \parallel 3$:	48 24-призм толщиной $\pi/12$
$O^* \times C_1$	$D_4^* \times C_3^*$, 3 как в кубе:	48 24-призм толщиной $\pi/12$
$I^* \times C_1$	$T^* \times C_5^*$, $5 \parallel [01\tau]$:	120 додекаэдров { 5,3,3 },

где в третьем столбце указаны взамные ориентации поворотных осей в исходных установках фигур. В последней строчке таблицы, наряду с известным многообразием Пуанкаре, указан и пример, не описанный в [4] с геометрической точки зрения (самый простой из них).

Разбиения Дирихле для других примеров нам удалось описать для серий $T^* \times C_m^*$, $O^* \times C_m^*$ и $I^* \times C_m^*$, направив одинаково оси максимальных порядков перемножаемых групп. Полученные фигуры – «ломаные 3-, 4- и 5-угольные призмы» (основания которых, напоминающие правильные 3-, 4- и 5-угольники) скручены между собой соответственно на $\pi/3m$, $\pi/4m$, $\pi/5m$ (это – и расстояния между центрами оснований), а боковые грани – в основном ромбы. В следующей таблице приведены некоторые их геометрические характеристики.

Группа	$T^* \times C_m^*$	$O^* \times C_m^*$	$O^* \times C_m^*$	$I^* \times C_m^*$	$I^* \times C_m^*$
Серия	1	$2a$	$2b$	$3a$	$3b$
m	$2i+3$	$6i-1$	$6i+1$	$6i+1$	$6i-1$
$3n$	$9m$	$8m+8$	$8m+16$	$5m+10$	$5m+20$
3В	$18m$	$16m+40$	$16m+56$	$10m+50$	$10m+70$
Р	$9m+3$	$8m+20$	$8m+28$	$5m+25$	$5m+35$
3Г	$9m+15$	$8m+26$	$8m+34$	$5m+31$	$5m+35$
3р	$9m-9$	$8m-28$	$8m-20$	$5m-35$	$5m-25$

Для серий $3a$ и $3b$ пропукаем значения m, кратные 5; n – число вершин основания; В, Р и Г – числа вершин, рёбер и граней ячейки; р – число боковых граней, имеющих форму ромба; i – натуральное.

Список литературы

1. Мокиевский В. А. Морфология кристаллов. — Л.: Изд-во Недра, 1983. — 295 С.

2. Кучериненко Я. В. О взаимном расположении двух фигур в пространствах постоянной кривизны // Материалы VIII Международного семинара "Дискретная математика и ее приложения"(2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2005. — С. 398–401.

3. Кучериненко Я. В. Разбиения трёхмерной сферы и срастания кристаллических зёрен // Труды II Всероссийской научной школы "Математические исследования в кристаллографии, минералогии и петрографии"(Апатиты, 16–17 октября 2006 г.). — Апатиты: Изд-во K&M, 2006. — С. 63–72.

4. Постников М. М. Трехмерные сферические формы // сб. "Дискретная геометрия и топология"к 100-летию со дня рождения Б. Н. Делоне, Тр. МИАН СССР. — М.: Наука, 1991. — С. 114–146.

5. Sutton A. P., Balluffi R. W. Interfaces in crystalline materials. — Oxford: Clarendon press, 1996.

6. Frank. F. C. Orientation mapping // Metalurgical transactions A. — 1988. — V. 19A, — P. 403–408.

7. Handscomb. D. C. On the random disorientation of two cubes // Canadian journal of mathematics. — 1958. — V. 10 — P. 85–88.

К ТЕОРЕМЕ О ТИПАХ ВЫПУКЛЫХ МНОГОГРАННИКОВ С ПАРКЕТНЫМИ ГРАНЯМИ

Е. С. Окладникова, А. В. Тимофеенко (Красноярск)

Правильногранником называется многогранник, грани которого правильные или составлены из правильных многоугольников так,

что вершины этих многоугольников служат и вершинами многогранника. С точностью до подобия найдены все выпуклые правильногранники, [1, 2]. Кроме правильных ещё пять паркетных многоугольников служат гранями некоторых правильногранников, см. электронный атлас [3]. Напомним, [4], выпуклый многоугольник называется *паркетным*, если он может быть составлен из конечного числа равноугольных многоугольников. Кроме четырех бесконечных серий, существует конечное число типов выпуклых многогранников с паркетными гранями.

Теоремы настоящей работы нацелены на решение проблемы *"Каковы все типы выпуклых многогранников с паркетными гранями?"* В публикации [4] отмечается, что кроме четырёх бесконечных серий существует лишь конечное число типов выпуклых многогранников с паркетными гранями и найти их можно по схеме, которая привела в работе [5] к нахождению всех выпуклых тел с правильными гранями. Теоремы 1 и 2 дают представление насколько увеличивается объём вычислений при поиске тел с паркетными гранями в сравнении с правильногранными телами.

В работе [5] выпуклые правильногранные многогранники, нерассекаемые никакой плоскостью по рёбрам на правильногранные части, названы простыми. Если же таким свойством обладает выпуклый правильногранник, то его называют *несоставным*. Согласно публикациям [5–7] существуют только следующие несоставные тела:

$$\Pi_3, \Pi_4, \dots ; A_4, A_5, \dots ; M_1, M_2, \dots , M_{28}, Q_1, Q_2 \dots , Q_6. \qquad (1)$$

Первыми в этом списке расположены бесконечные серии призм и антипризм. За ними следуют правильногранные пирамиды M_1, M_2, M_3 с трёх-, четырёх- и пятиугольными основаниями соответственно и другие тела, которые называют сегодня многогранниками Залгаллера, Иванова и Пряхина.

Соединением одинаковыми гранями из несоставных тел можно получить каждый выпуклый правильногранник. В отличие от выпуклых правильногранников, каждому типу которых соответствует единственный с точностью до подобия многогранник, типу выпуклого тела с паркетными гранями соответствует, как правило, бесконечное множество попарно неподобных многогранников. Такие тела встречаются и в следующей, доказанной на вэбинаре "Группы и правильногранники" [9] теореме.

Теорема 1. *Выпуклый многогранник с рёбрами длины один или два составлен из не более четырнадцати правильногранных пира-*

мид с единичными рёбрами тогда и только тогда, когда он является одним из следующих тел:

1) M_1, M_2, M_3;

2) $M_1 + M_1$, $M_1 + M_2$, $M_2 + M_2$, $M_3 + M_3$;

3) $^\circ S_{2,2} + M_1$, $S_{2,2} + M_2$, $^\circ S_{2,2} + M_2'$;

4) $^\circ S_{3,1}+M_2$, $^\circ S_{3,1}+M_2'$, $S_{3,2}+M_1$, $S_{2,2}+S_{2,2}$, $S_{2,2}+S_{2,2}'$, $^\circ S_{2,2}+S_{2,2}''$;

5) $^\circ S_{4,1} + M_1$, $^\circ S_{4,4} + M_2$;

6) $^\circ S_{5,1} + M_1$, $^\circ S_{5,2} + M_1$, $^\circ S_{5,2} + M_2$, $^\circ S_{3,1} + S_{3,1}$, $^\circ S_{3,1} + S_{3,3}$;

7) $^\circ S_{6,2} + M_1$, $^\circ S_{6,5} + M_2$, $S_{4,6} + S_{3,1}$;

8) $^\circ S_{7,1} + M_1$, $^\circ S_{7,2} + M_1$, $S_{7,3} + M_2$, $^\circ S_{6,2} + S_{2,2}$, $^\circ S_{6,5} + S_{2,2}$, $^\circ S_{5,1} + S_{3,1}$;

9) $^\circ S_{8,3} + M_2$, $^\circ S_{6,5} + S_{3,1}$, $^\circ S_{6,5} + S_{3,3}$;

10) $^\circ S_{9,1} + M_1$, $^\circ S_{9,1} + M_2$, $^\circ S_{9,3} + M_2$, $^\circ S_{8,3} + S_{2,2}$, $^\circ S_{5,1} + S_{5,1}$;

11) $^\circ S_{10,1} + M_2$, $^\circ S_{10,4} + M_2$, $^\circ S_{10,5} + M_1$;

12) $^\circ S_{11,2} + M_1$, $^\circ S_{11,3} + M_1$, $S_{9,1} + S_{3,1}$, $^\circ S_{9,1} + S_{3,1}'$, $^\circ S_{9,3} + S_{3,1}$;

13)$^\circ S_{12,3} + M_2$, $^\circ S_{12,4} + M_1$, $^\circ S_{10,4} + S_{3,1}$;

14) $^\circ S_{13,1} + M_1$, $^\circ S_{13,1} + M_2$, $^\circ S_{13,3} + M_2$, $^\circ S_{12,3} + S_{2,2}$, $S_{7,3} + S_{7,3}$, $S_{7,3} + S_{7,3}'$;

15) $^\circ S_{14,1} + M_2$, $S_{14,5} + M_2$, $S_{14,6} + M_2$, $S_{12,4} + S_{3,3}$, $^\circ S_{12,5} + S_{3,3}$;

причём многогранник $S_{i,j}$ расположен в списке (i) на j-м месте, штрих указывает на различие многогранников, составленных из двух одинаковых тел, кружком помечены тела с фиктивными вершинами.

Как доказано в [8], семь многогранников списка разбиваются плоскостью на тела с паркетными гранями. Из них пять тел составлены из правильногранных пирамид с единичными рёбрами. Все выпуклые с рёбрами длины 1 или 2 соединения не более 15 таких пирамид расположены выше в теореме 1. Поэтому справедлива

Теорема 2. *Если выпуклый правильногранник никакой плоскостью не рассекается на правильногранники, но существует плоскость, делящая его на многогранники с правильными или составленными из правильных многоугольников гранями, то он составлен из правильногранных пирамид тогда и только тогда, когда является одним из пяти тел: трёхскатный купол M_4, усечённый тетраэдр M_{10}, усечённый октаэдр M_{16}, наклонная призма Q_1, двенадцатигранник Иванова Q_2.*

Работа выполнена при финансовой поддержке РФФИ (проект 15-01-04897).

Список литературы

1. Тимофеенко А. В. К перечню выпуклых правильногранников // Современные проблемы математики и механики. — 2011. — Т. VI., вып. 3 — С. 155–170.

2. Гурин А. М., Залгаллер В. А. К истории изучения выпуклых многогранников с правильными гранями и гранями составленными из правильных // Труды Математического Общества Санкт-Петербурга. —2008. — Т. 14. — С. 215–294.

3. Convex regular-faced polyhedra with conditional edges // Электронный ресурс: `http://tupelo-schneck.org/polyhedra`.

4. Пряхин Ю. А. Выпуклые многогранники, грани которых равноугольны или сложены из равноугольных // Зап. науч. семинаров ЛОМИ. —1974. — Т. 45. — С. 111–112.

5. Залгаллер В. А. Выпуклые многогранники с правильными гранями // Зап. науч. семинаров ЛОМИ. — 1967. — Т. 2. — С. 5–218.

6. Иванов Б.А. Многогранники с гранями, сложенными из правильных многоугольников // Украинский геометрический сборник. —1971. — Т. 10. —С. 20–34.

7. Пряхин Ю. А. О выпуклых многогранниках с правильными гранями // Украинский геометрический сборник. —1973. — Т. 14. — С. 83–88.

8. Тимофеенко А. В. О выпуклых многогранниках с равноугольными и паркетными гранями // Чебышевский сборник. —2011. — Т. 12, вып. 2. — С. 118–126.

9. Группы и правильногранники // Электронный ресурс: `http://icm.krasn.ru/seminar.php?id=reghedra`.

ГРАНИЧНЫЕ ЗНАЧЕНИЯ ДЛЯ ОТНОШЕНИЙ ТИПА ШТЕЙНЕРА

А. С. Пахомова (Москва)

Одной из известных задач геометрической оптмизации является задача нахождения кратчайшей сети, соединяющей данное конечное множество M точек метрического пространства X. При этом ответ зависит от рассматриваемого семейства допустимых сетей, среди которых выбирается кратчайшая. Рассмотрим несколько различных классов взвешенных деревьев, соединяющих множество M. Если рассматривать только графы, множество вершин которых совпадает

с множеством точек M, а в качестве веса ребра рассматривать расстояние по метрике пространства X между вершинами, мы получим конструкцию *минимального остовного дерева* для M. Суммарный вес ребер дерева можно уменьшить, если рассматривать графы, которые содержат еще какие-то дополнительные вершины из пространства X, не входящие в M. В этом случае мы говорим о *минимальном дереве Штейнера* для M. Если же не ограничиваться рассмотрением точек пространства X, а рассмотреть всевозможные изометрические вложения множества M в произвольные метрические пространства и искать деревья Штейнера в них, мы получим конструкцию *минимального заполнения* множества M. Для каждого описанного класса можно поставить задачу нахождения дерева минимального веса. Вес минимального остовного дерева для множества M будем обозначать $\mathrm{mst}(M)$, вес минимального дерева Штейнера — $\mathrm{smt}(M)$, а вес минимального заполнения — $\mathrm{mf}(M)$. Подробнее об этих понятиях можно узнать в работах [1] и [2].

Отношением Штейнера метрического пространства (X, ρ) называется величина

$$\mathrm{sr}(X,\rho) = \inf_{\{M \mid M \subset X\}} \left\{ \frac{\mathrm{smt}(M)}{\mathrm{mst}(M)} \mid 1 < \#M < \infty \right\},$$

где $\#M$ обозначает количество элементов в множестве M.

Отношение Штейнера появилось впервые в работах Джилберта и Поллака в 60-х годах двадцатого века. Интерес к нему связан в частности с гипотезой Джилберта—Поллака [3] об отношении Штейнера евклидовой плоскости. Однако стоит заметить, что многочисленные попытки доказать ее [4] так и не привели к успеху, оставив данный вопрос открытым для исследования [5]. Тем не менее, в ходе изучения отношения Штейнера были получены многие важные результаты, связанные как с общими свойствами этого отношения, так и с отношением Штейнера для конкретных пространств.

Если вместо указанного отношения рассмотреть отношение веса $\mathrm{mf}(M)$ к $\mathrm{mst}(M)$, мы получим определение *отношения Штейнера—Громова* $\mathrm{sgr}(X, \rho)$. А если вместо указанного отношения рассмотреть отношение $\mathrm{mf}(M)$ к $\mathrm{smt}(M)$, мы получим определение *суботношения Штейнера* $\mathrm{ssr}(X, \rho)$. Суботношение Штейнера и отношение Штейнера—Громова, как и конструкция минимального заполнения для конечного метрического пространства, впервые были предложены А.О. Ивановым и А.А. Тужилиным в работе [2]. Три описанных выше отношения мы будем называть *отношениями типа Штейнера*. В тех случаях, когда неважно, о каком из трех отношения идет

речь, мы будем использовать запись $r(X)$.

Помимо описанных выше отношений типа Штейнера можно рассмотреть *n-точечные отношения типа Штейнера* для фикисированного натурального $n \geq 2$. Для этого в определении соответствующего отношения точную нижнюю грань по всем конечным подмножествам нужно заменить на точную нижнюю грань по тем подмножествам, что содержат не более n точек.

Таким образом, отношения типа Штейнера являются важной характеристикой метрического пространства, показывающей, насколько хорошо минимальные деревья из разных классов приближают друг друга.

Следующая теорема была доказана в работе [6] для случая отношения Штейнера и в работе автора [7] для двух других отношений.

Теорема. *Для любого отношения типа Штейнера $r(X)$ справедливы оценки $\frac{1}{2} \leq r(X) \leq 1$. Для любого n-точечного отношения типа Штейнера $r_n(X)$ справедливы оценки $\frac{n}{2(n-1)} \leq r_n(X) \leq 1$.*

Отдельный интерес представляет рассмотрение метрических пространств, значение отношения типа Штейнера которых равно 1, т.е. является максимально возможным. Автором были описаны все метрические пространства, для которых отношение Штейнера—Громова равно единице.

Теорема. *Пусть (X, ρ) — метрическое пространство. Следующие условия эквивалентны:*
1) *$sgr(X) = 1$;*
2) *Для любого $n \geq 2$ $sgr_n(X) = 1$;*
3) *Для некоторого $n > 3$ $sgr_n(X) = 1$;*
4) *Все треугольники в пространстве X вырождены, т.е. для любых трех точек неравенство треугольника является равенством;*
5) *X изометрично некоторому подмножеству евклидовой прямой или четырехточечному пространству $\{x_1, x_2, x_3, x_4\}$, в котором все треугольники вырождены и $\rho(x_i, x_j) = \rho(x_k, x_l)$ для любой перестановки (i, j, k, l) индексов $(1, 2, 3, 4)$.*

Автор выражает благодарность своему научному руководителю д. ф.-м. н. А. О. Иванову, д. ф.-м. н. А. А. Тужилину и всем участникам семинара «Оптимальные сети» за помощь и проявленный интерес к работе. Работа выполнена при финансовой поддержке гранта РФФИ (проект 16–01–00378а) и гранта Президента РФ поддержки ведущих научных школ РФ (проект НШ–7962.2016.1).

Список литературы

1. Иванов А. О., Тужилин А. А. Одномерная проблема Громова

о минимальном заполнении // Матем. сб. — 2012. — 203 (5). — С. 65–118.

2. Ivanov A. O., Tuzhilin A. A. Minimal fillings of finite metric spaces: The state of the art //Discrete Geometry and Algebraic Combinatorics (Vol. 625 of Contemporary Mathematics, AMS, Providence, RI, 2014). — P. 9–35.

3. Gilbert E. N., Pollak H. O., Steiner minimal trees // SIAM J. Appl. Math. — 1968. — 16 (1). — P. 1–29.

4. Du D.-Z., Hwang F. K. A proof of the Gilbert—Pollak conjecture on the Steiner ratio // Algoritmica. — 1992. — Vol.7. — P. 121–135.

5. Ivanov A. O., Tuzhilin A. A. The Steiner Ratio Gilbert—Pollak Conjecture Is Still Open // Algorithmica. — Vol. 62, iss. 1–2. — P. 630–632.

6. Cieslik D. The Steiner Ratio. — Kluwer Academic Publishers, 2001

7. Пахомова А. С. Оценки для суботношения Штейнера и отношения Штейнера—Громова // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2014. — № 1 – С. 17–25.

МНОГОГРАННИКИ С СИММЕТРИЧНЫМИ РОМБИЧЕСКИМИ ВЕРШИНАМИ

В. И. Субботин (Новочеркасск)

Рассмотрены свойства замкнутых выпуклых многогранников в трёхмерном евклидовом пространстве, связанные с симметрией звёзд некоторых вершин многогранника.

Определение 1. Вершина многогранника называется *ромбической*, если её звезда состоит из равных одинаково расположенных ромбов.

Таким образом, все ромбы сходятся в вершине либо острыми, либо тупыми углами. Если таких ромбов n штук, то вершину будем называть *n-ромбической*, а совокупность этих n ромбов-ромбической шапочкой. Под звездой ромбической шапочки будем понимать объединение ромбической шапочки и всех граней, имеющих хотя бы одну общую вершину с ромбами шапочки.

Определение 2. Ромбическая вершина называется *симметричной*, если она расположена на оси вращения звезды её ромбической шапочки.

Определение 3. Ромбическая вершина называется *изолированной*, если её звезда не имеет общих элементов со звездой любой другой ромбической вершины многогранника.

Если рассматривать многогранники, каждая вершина которых является симметричной ромбической, но не изолированной, то, как известно, класс таких многогранников исчерпывается двумя многогранниками: ромбическим додекаэдром и ромботриаконтаэдром [1].

Далее будем рассматривать многогранники, каждая ромбическая вершина которых является симметричной и изолированной. При этом каждая грань F, не входящая в звезду ромбической вершины, имеет ось вращения, перпендикулярную F. Предполагается, что эта ось вращения является осью вращения звезды грани F. Такой класс многогранников будем обозначать RS.

Доказана следующая теорема:

Теорема 1. *Всякий многогранник класса RS может быть получен при помощи преобразования отсечения некоторых трёхгранных вершин одного из сильно симметричных относительно вращения граней многогранников и последующего симметричного продления полученных треугольных сечений до ромбов.*

Для доказательства теоремы достаточно из всех многогранников, сильно симметричных относительно вращения граней [1], выбрать те, к которым применимо указанное в формулировке теоремы преобразование.

На основании этой теоремы получаются следующие типы многогранников класса RS, исчерпывающие этот класс:

1) многогранник, полученный из усечённого ромбического триаконтаэдра [2];

2) многограннмк, полученный из 2-го полуусечённого ромбического триаконтаэдра [2];

3) многогранник, полученный из усечённого икосаэдра;

4) вытянутый ромбический додекаэдр;

5) вытянутые ромбоэдры.

Следующий класс, рассматриваемый в работе — класс многогранников с двумя изолированными симметричными ромбическими вершинами, которые разделены равными правильными многоугольниками одного типа. Причём все ромбы обеих звёзд вершин равны между собой. Этот класс будем обозначать RR.

Доказана следующая теорема:

Теорема 2. *Всякий многогранник класса RR принадлежит одному из следующих типов:*

1) *вытянутый ромбический додекаэдр;*

2) 20-*гранник с квадратными гранями, разделяющими 5-*

ромбические вершины;
3) *многогранники с правильными треугольными гранями, разделяющими n-ромбические вершины,* $3 < n < 12$.

Замечание. Отметим, что многогранники класса RS с двумя ромбическими вершинами можно использовать для построения каждого из пяти трёхмерных *параллелоэдров* с помощью соответствующего геометрического преобразованиия.

Список литературы

1. Субботин В. И. Перечисление многогранников, сильно симметричных относительно вращения // Труды участников международной школы-семинара по геометрии и анализу памяти Н. В. Ефимова (5–11 сент. 2002 г.). — С. 77–78.

2. Субботин В. И. О многогранниках, сильно симметричных относительно вращения // Чебышевский сборник. — 2006. — Т. 7, вып. 2(18). — С. 168–171.

Секция «Теория кодирования и математические вопросы теории защиты информации»

К ВОПРОСУ О ДЕДУКТИВНОЙ БЕЗОПАСНОСТИ ВЫЧИСЛЕНИЙ НАД ЗАШИФРОВАННЫМИ ДАННЫМИ

Н. П. Варновский, В. А. Захаров, А. В. Шокуров (Москва)

Открытие стойких систем вполне гомоморфного шифрования [1] создало теоретические предпосылки решения задачи обеспечения информационной безопасности систем удаленных вычислений, включая системы облачных вычислений. Однако, как показано в [2], даже в том случае, когда проводится лишь вычисление функций от хранящихся на облаке конфиденциальных значений аргументов, защита данных невозможна уже для системы с двумя пользователями. Для преодоления этой трудности в статье [3] была предложена специальная модель облачных вычислений, в состав которой помимо облачного сервера входят криптосерверы, на которых реализуется пороговая гомоморфная криптосистема с открытым ключом (TSHE). В статье [4] показано, что если TSHE является стойкой и доля криптосерверов, контролируемых противником, не превосходит заданного порога, то предложенная система облачных вычислений является стойкой для вычислений ограниченной глубины.

Доказанная в [4] стойкость облачных вычислений не отменяет, тем не менее, возможности противника компрометировать конфиденциальные данные пользователей: располагая вычисленными значениями функций $f_i(c_1, \ldots, c_n), i \in I$, зависящих от данных пользователя, противник может попытаться решить обратную задачу и вычислить значения аргументов этих функций. Для предотвращения этой возможности в системе облачных вычислений [3, 4] предусмотрен контроль доступа: облако передает запрос клиента в центр аутентификации, который проверяет полномочия клиента на вычисление запрашиваемой функции и, при наличии таковых, санкционирует выполнение запроса. Однако вопрос о том, как осуществлять проверку полномочий, оставался открытым. Данная статья инициирует исследование этого вопроса.

Рассмотрим упрощенную модель облачной базы данных. Каждый пользователь $u_i, 1 \le i \le n$, хранит в базе данных конфиденциальное истинностное значение σ_i базового предиката P_i, ассоциированного с этим пользователем. Клиент базы данных может обращаться к ней с запросами. Запросом является произвольная булева формула $\varphi(P_1, \ldots, P_n)$, зависящая от предикатов пользователей. Ответом на запрос является значение $\varphi(\sigma_1, \ldots, \sigma_n)$. Клиент базы данных имеет полномочие обращаться с запросами из некоторого множества $\mathcal{Q} = \{\varphi_1, \ldots, \varphi_N\}$. Сформулируем требование безопасности для множества запросов.

Для всякой формулы φ и $\delta, \delta \in \{0, 1\}$, обозначим записью φ^δ формулу $\neg\varphi$, если $\delta = 0$, и φ, если $\delta = 1$. Для набора формул $\mathcal{Q} = (\varphi_1, \ldots, \varphi_N)$ и двоичного набора $\Delta = (\delta_1, \ldots, \delta_N)$ запись $\mathcal{Q}^\Delta$ будет обозначать набор формул $(\varphi_1^{\delta_1}, \ldots, \varphi_N^{\delta_N})$. Для набора формул $\mathcal{Q} = (\varphi_1, \ldots, \varphi_N)$, зависящих от предикатов $P_1, \ldots, P_n$, и двоичного набора $\Sigma = (\sigma_1, \ldots, \sigma_n)$ обозначим записью $\mathcal{Q}(\Sigma)$ набор значений функций $(\varphi_1(\Sigma), \ldots, \varphi_N(\Sigma))$. Символами $\bar{0}$ и $\bar{1}$ обозначим двоичные наборы, состоящие из 0 и 1 соответственно. Символом $\models$ обозначается отношение логического следования в классической логике высказываний.

Определение. Набор запросов $\mathcal{Q} = \{\varphi_1, \ldots, \varphi_N\}$ к базе данных, состоящей из значений базовых предикатов $P_1, \ldots, P_n$, называется *дедуктивно безопасным*, если для любого двоичного набора $\Sigma = (\sigma_1, \ldots, \sigma_n)$ соотношение $\mathcal{Q}^{\mathcal{Q}(\Sigma)} \models P_i^{\sigma_i}$ не выполняется ни для одного предиката $P_i, 1 \le i \le n$.

Дедуктивная безопасность набора запросов подразумевает, что клиент базы данных, получив ответы на все доступные ему запросы, не может дедуктивно выведать значения предикатов пользователей базы данных. Таким образом, контроль полномочий клиента состоит в проверке дедуктивной безопасности множества запросов, с которыми клиент обращается к базе данных.

Теорема 1. *Набор запросов $\mathcal{Q}$ является дедуктивно безопасным тогда и только тогда, когда для любого предиката $P_i, 1 \le i \le n$, и для любого набора Σ_1 истинностных значений базовых предикатов существует такой набор Σ_2, для которого выполняются соотношения $P_i(\Sigma_1) \ne P_i(\Sigma_2)$ и $\mathcal{Q}(\Sigma_1) = \mathcal{Q}(\Sigma_2)$.*

Из теоремы 1 следует

Теорема 2. *Задача проверки дедуктивной безопасности наборов запросов к базе данных является со-NP^{NP}-полной.*

Поскольку задача проверки дедуктивной безопасности запросов является вычислительно трудной, целесообразно выделить некото-

рые практически значимые классы запросов, для которых эта задача может быть решена эффективно. Булева функция $f(y_1, \ldots, y_k)$ называется симметрической, если для любой перестаноки $\theta : [1, k] \to [1, k]$ верно равенство $f(y_1, \ldots, y_k) = f(y_{\theta(1)}, \ldots, y_{\theta(k)})$. В сущности, симметрические запросы призваны собирать статистические сведения о данных пользователей базой данных. Дедуктивная безопасность таких запросов означает, что статистические сведения, собранные клиентом базы данных, не позволяют ему получить сведения о данных какого-либо пользователя этой базы.

Теорема 3. *Пусть $\mathcal{Q}$ — некоторое множество симметрических запросов к базе данных. Тогда $\mathcal{Q}$ является дедуктивно безопасным тогда и только тогда, когда существует такая пара наборов Σ_0 и Σ_1 истинностных значений базовых предикатов, для которых выполняются соотношения $\Sigma_0 \neq \bar{0}$, $\Sigma_1 \neq \bar{1}$, $\mathcal{Q}(\Sigma_0) = \mathcal{Q}(\bar{0})$ и $\mathcal{Q}(\Sigma_1) = \mathcal{Q}(\bar{1})$.*

Предложенный критерий дедуктивной безопасности симметрических запросов можно проверить за полиномиальное время.

Следствие. *Если $\mathcal{Q}$ — некоторое множество симметрических запросов к базе данных, то для его дедуктивной безопасности достаточно, чтобы выполнялось равенство $\mathcal{Q}(\bar{0}) = \mathcal{Q}(\bar{1})$.*

Работа поддержана грантом РФФИ (проект 16-01-00714).

Список литературы

1. Gentry C. Fully homomorphic encryption using ideal lattices // Proceedings of the 41-st ACM Symposium on Theory of Computing. New York: ACM, 2009. — P. 169–178.

2. Van Dijk M., Juels A. On the impossibility of cryptography alone for privacy-preserving cloud computing // Proceedings of the 5-th USENIX Conference on Hot Topics in Security. — Berkeley: USENIX Association, 2010. — P. 1–8.

3. Варновский Н. П., Мартишин С. А. Храпченко М. В., Шокуров А. В. Пороговые системы гомоморфного шифрования и защита информации в облачных вычислениях // Программирование. — 2015. — № 4. — С. 47–51.

4. Варновский Н. П., Захаров В. А., Шокуров А. В. К вопросу о существовании доказуемо стойких систем облачных вычислений // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2015. — № 2. — С. 32–38.

ДЗЕТА-ФУНКЦИИ МНОГООБРАЗИЙ И СЕМЕЙСТВ МНОГООБРАЗИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

Н. М. Глазунов (Киев)

Дан краткий обзор дзета и L-функций многообразий и семейств многообразий над конечными полями вида $\mathbb{F}_q$, где $q = p^n$, число p простое, а n — натуральное. Обзор включает недавние результаты, которые получили C. Greither, N. Ramachandran, и другие. В терминах элементов колец Витта рассмотрен случай L-функций семейства накрытий Артина-Шрайера.

Дзета и L-функции семейств алгебраических кривых. Пусть X есть алгебраическое многообразие или схема конечного типа [1] над $\mathbb{F}_q$. Для X над $\mathbb{F}_q$ имеются два альтернативных определения дзета-функции: (i) пусть $x \in X$ есть замкнутая точка X и $d(x)$ степень её поля вычетов над $\mathbb{F}_q$. Тогда $Z(X,t)$ определяется как $\prod_{x\in X}(1-t^{d(x)})^{-1}$; (ii) пусть $\#X(\mathbb{F}_{q^r})$ есть число $\mathbb{F}_{q^r}$-рациональных точек на X. Тогда $Z(X,t) = \exp(\sum_{r\geq 1}\#X(\mathbb{F}_{q^r})\frac{t^r}{r})$. В работе [2] исследуется случай семейства суперэллиптических кривых. Рассматривается суперэллиптическая кривая над полем $K = \mathbb{F}_q(t)$ и её модель $\mathcal{E}$ над проективной прямой. В [2] предполагается, что все особенности $\mathcal{E}$ рациональны, и формулируются условия, когда это так. Автор [2] использует мотивную интерпретацию якобиана исследуемой кривой, разрабатывает и применяет новую технику для построения соответствующих L-функций, получает сравнения для степени L-функций и верхнюю оценку для аналитического ранга соответствующего якобиана.

В работе [3] автор исследует дзета-функции схем конечного типа [1] над $\mathbb{F}_q$. Среди представленных в [3] результатов — выражения для дзета-функций произведения схем X и Y, дзета-функция n-кратного произведения схемы X, а также выражения для дзета-функций гладких собственных геометрически связных многообразий над $\mathbb{F}_{q^m}$, представленные через произведения Витта дзета-функций соответствующих схем.

Большое кольцо Витта. Пусть A есть коммутативное кольцо с единицей. Большим кольцом Витта (выше и далее — кольцом Витта) $W(A)$ называют коммутативное кольцо с единицей, аддитивная группа $(W(A),+)$ которого изоморфна подгруппе $(1+tA[[t]],\times)$ группы единиц $A[[t]]^*$ кольца $A[[t]]$ относительно умножения формальных

степенных рядов, а умножение $*$ определяется единственным способом условием $(1-at)^{-1} * (1-bt)^{-1} = (1-abt)^{-1}, a, b \in A$ и функториально относительно $W(-)$: любой гомоморфизм колец $f\colon A \to B$ индуцирует гомоморфизм колец $W(f)\colon W(A) \to W(B)$. Единицей относительно сложения является элемент $1 = 1 + 0t + 0t^2 + \cdots$, а единицей относительно умножения - элемент $[1] = (1-t)^{-1}$.

L-функции накрытий Артина—Шрайера как элементы кольца Витта. Постоянным накрытием Артина—Шрайера называют накрытие вида $y^p - y = cx + \frac{d}{x}, c, d \in \mathbb{F}_q^*$. Можно рассмотреть и относительный случай, рассматривая накрытия Артина—Шрайера над проективной прямой над $\mathbb{F}_q$, то есть над полем функций $\mathbb{F}_q(t)$. В последнем случае непостоянные накрытия Артина—Шрайера имеют вид $y^p - y = c(t)x + \frac{d(t)}{x}, c(t), d(t) \in \mathbb{F}_q[t]$. Здесь мы рассматриваем случай постоянных накрытий Артина—Шрайера над простым конечным полем. Хорошо известно (см. например, [4]), что L-функция такого накрытия имеет вид $L(X,t) = 1 - T_p(c,d)t + pt^2$, где $T_p(c,d) = \sum_{x=1}^{p-1} \exp(2\pi i \frac{cx+\frac{d}{x}}{p})$ есть сумма Клостермана.

Теорема 1. *Пусть X и Y есть накрытия Артина—Шрайера. Тогда $L(X \times Y, t)$ функция произведения таких накрытий есть произведение Витта L-функций накрытий: $L(X \times Y, t) = L(X,t) * L(Y,t)$.*

Множество всех накрытий Артина—Шрайера параметризуется пространством модулей $\mathcal{M} = \mathbb{F}_p^* \times \mathbb{F}_p^*$.

Теорема 2. *L-функция произведения всех накрытий Артина-Шрайера над $\mathcal{M}$ имеет вид $L(X_1 \times \cdots \times X_{(p-1)^2}, t) = L(X_1, t) * \cdots * L(X_{(p-1)^2}, t)$.*

Список литературы

1. Шафаревич И. Р. Основы алгебраической геометрии. Тт. 1–2. — М.: Наука, 1988.

2. Greither C. Families of curves with Galois action and their L-functions // J. Number Theory. — 2015. — Vol. 154. — P. 292–323.

3. Ramachandran N. Zeta functions, Grothendieck groups, and the Witt ring // Bull. Sci. Math. — 2015. — V. 139, I. 6. — P. 599–627.

4. Глазунов Н. М. Разработка методов обоснования гипотез формальных теорий. — Saarbrucken.: LAP, 2014.

СЖИМАЕМОЕ ОПОЗНАВАНИЕ: МАТЕМАТИЧЕСКИЕ ОСНОВЫ И КОМПЬЮТЕРНАЯ РЕАЛИЗАЦИЯ

Н. М. Глазунов, О. В. Кузик (Киев)

Задача восстановления матрицы по выборке её элементов, которая может быть соотнесена с кодированием источника, формулируется как задача выпуклой оптимизации [1–3]. Изначально присущей особенностью рассматриваемой задачи восстановления матрицы по выборке её элементов является недифференцируемость этой задачи, что обуславливает проблематичность применения классических методов дифференцируемой оптимизации. В связи с этим обстоятельством для её решения предлагается применение r-алгоритмов [1, 4]. Представлена общая схема, компьютерная реализация которой выполняется на Java.

Постановки задачи и применения. В рамках кодирования источника сжатое опознавание интерпретируется как восстановление информации источника по неполным данным, кодирующим элементы этой информации. Хотя ниже речь идет о вещественных матрицах, фактически при вычислениях матрицы целочисленны, или имеют рациональные коэффициенты. Задача восстановления матрицы по выборке её элементов возникает во многих математических и прикладных исследованиях. Упомянем следующие прикладные задачи: базы данных; триангуляция по неполным данным; сжатое опознавание (Compressed Sensing); машинное обучение (Machine Learning).

Пусть X есть искомая матрица, $M_{i,j}$ известные значения. Одна из математических формулировок вышеперечисленных задач имеет следующее представление:

$$\begin{array}{l}\text{minimize } \operatorname{rank}(X)\\ \text{subject to } X_{i,j} = M_{i,j},\ (i,j) \in \Omega,\end{array}$$

где (i, j) есть множество индексов, $M_{i,j} \in \Omega$ наблюдаемые значения. К сожалению, как доказано в [3], в такой постановке задача суперэкспоненциальна по сложности.

Напомним [1], что задача полуопределенного программирования состоит в минимизации линейной функции от m вещественных переменных относительно матричного неравенства

$$\begin{array}{l}\text{minimize } c^T x\\ \text{subject to } F(x) \geq 0,\end{array}$$

где $F(x) = F_0 + \sum_{i=1}^{m} x_i F_i$ и $F_0, F_1, \ldots, F_m$ есть симметрические матрицы. Задача полуопределенного программирования является зада-

чей выпуклой оптимизации, так как целевая функция и ограничения выпуклы: если $F(x) \geq 0$ и $F(y) \geq 0$, то для всех $\lambda, 0 \leq \lambda \leq 1$ $F(\lambda x + (1-\lambda)y) = \lambda F(x) + (1-\lambda)F(y) \geq 0$.

Пусть X есть матрица размера $n \times m$, X^* есть матрица, сопряженная к X. Тогда собственные значения матриц XX^* и X^*X совпадают и являются положительными. Арифметические значения квадратных корней общих собственных значений матриц XX^* и X^*X называют сингулярными значениями матрицы X. Далее полагаем, что σ_k есть k-е сингулярное значение матрицы X, и что эти сингулярные значения занумерованы в порядке убывания $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_n > 0$ где σ_n есть наименьшее сингулярное значение. Сингулярные значения $\sigma_{n+1}, \ldots$ полагают нулевыми.

Математическая модель. Скалярное произведение (X, Y) матриц X и Y размера $n \times m$ определяют как след $\mathrm{tr}(X^*Y)$ произведения указанных матриц. Напомним, что субградиентом матричной выпуклой функции f называют матрицу $g_f(X_0)$, удовлетворяющую неравенству $f(X) - f(X_0) \geq (g_f(X_0), X - X_0)$ для всех вещественных матриц размера $n \times m$. Ядерной нормой матрицы X называют величину $\|X\|_* = \sum_{k=1}^{n} \sigma_k(X)$ где $\sigma_k(X)$ k-е сингулярное значение X. Исследуется задача оптимизации (с ядерной нормой):

$$\begin{array}{l} \text{minimize } \|(X)\|_* \\ \text{subject to } X_{i,j} = M_{i,j}, (i,j) \in \Omega. \end{array}$$

Метод решения. Метод решения вышеприведенной оптимизационной задачи основывается на матричном расширении r-алгоритма Н. З. Шора [1]. Для сингулярного разложения матрицы ранга s выражение для субградиента ядерной нормы этой матрицы известно. В процессе выполнения r-алгоритма преобразуется пространство поиска и выполняются ортогональные проектирования.

Реализация. В настоящее время реализация выполняется на Java. Главная процедура `ShorNonDifferentiableMethod` использует набор утилит, реализующих метод, а также служащих для целей тестирования.

Список литературы

1. Shor N. Z. Nondifferentiable optimization and polynomial problems. — Boston.: Kluwer Acad. Publ., 1998.

2. Candès E., Recht B. Exact Matrix Completion via Convex Optimization // Found. Comput. Math. — 2009. — 9. — P. 717–772.

3. Chistov A. L., Grigoriev D. Yu. Complexity of quantifier elimination in the theory of algebraically closed fields // Lecture Notes in Computer Science. — 1984. — Vol. 176. — P. 17–31.

4. Глазунов Н. М. Арифметическое моделирование случайных процессов и r-алгоритмы // Кибернетика и системный анализ. — 2012. — 1. — С. 23–32.

ОБ ИСПОЛЬЗОВАНИИ АТАКИ ЛИНЕЙНЫМ РАЗЛОЖЕНИЕМ ПРИ ПОСТРОЕНИИ ПРОТОКОЛА ГЕНЕРАЦИИ ОБЩЕГО КЛЮЧА

И. В. Зубков (Москва)

Введение. Недавно В. А. Романьков предложил в [1] принципиально новую атаку на протоколы, названную *атакой линейным разложением.* С помощью данной атаки при условии, что используемая в криптосистеме группа является линейной, за время, полиномиальное от исходных данных, во многих случаях удается получить секретный ключ, не находя секретные данные пользователей. Новизна предлагаемого ниже подхода к построению протокола заключается в том, что первый пользователь на одном из этапов применяет атаку линейным разложением для нахождения промежуточных данных.

Атака линейным разложением. Пусть дана линейная группа G. Пусть U, V — два конечных подмножества G, коммутирующие друг с другом. Пусть $A = \langle U\rangle$ и $B = \langle W\rangle$ являются подмоноидами G, порожденными множествами U и W соответственно. Для любых $a \in A, b \in B, g \in G$ положим $g^a = aga^{-1}$, $g^b = bgb^{-1}$.

Тогда по открытым данным U, W, g, g^a, g^b за полиномиальное число операций от исходных данных можно вычислить g^{ab}.

Протокол генерации общего ключа. Пусть $G = GL_k(\mathbf{F}_{3^m})$ и $Aut(G)$ — группа автоморфизмов группы G. Далее, пусть U и W — два подмножества $Aut(G)$, причем элементы U попарно коммутируют с элементами из W, а также элементы U коммутируют друг с другом. Обозначим через A и B подгруппы $Aut(G)$, порожденные U и W соответственно. Зафиксируем элемент $g \in G$. Открытые данные: U, W, g.

Алиса выбирает автоморфизм $b_1 \in B$, вычисляет $b_1(g)$, затем строит матрицу $f \in G$ такую, чтобы для любого $u \in U$ было выполнено $u(f) = f$, причем матрица $b_1(g) + f$ должна быть вырожденной, и отправляет Бобу $b_1(g) + f$.

Боб выбирает два автоморфизма $a_1, a_2 \in A$ и отправляет Алисе пару элементов $a_1(b_1(g)+f) = a_1(b_1(g))+f, a_2(b_1(g)+f) = a_2(b_1(g))+f$. Алиса вычитает из обоих элементов, полученных от Боба, матрицу f и применяет автоморфизм b_1^{-1} к полученной паре: $b_1^{-1}(a_1(b_1(g))) = a_1(g), b_1^{-1}(a_2(b_1(g))) = a_2(g)$.

После этого она применяет атаку линейным разложением и получает матрицу $a_1(a_2(g))$. Наконец, Алиса выбирает автоморфизм $b_2 \in B$ и отправляет Бобу $b_2(g)$.

Получение ключа. Алиса вычисляет $K_A = b_2(a_1(a_2(g)))$, Боб вычисляет $K_B = a_1(a_2(b_2(g)))$. Тогда общий ключ равен $K = K_A = K_B$, поскольку элементы A и B попарно коммутируют.

Выбор U, W, g. Для любого $g \in G$ определим $\chi \in Aut(G)$ так: положим $\chi(g) = \det(g) \cdot g$.

Рассмотрим три попарно коммутирующие матрицы $x, y, z \in GL_k(\mathbf{F}_{3^m})$. Тогда определим $U = \{\overline{x}; \overline{y}\}$, $W = \{\chi; \overline{z}\}$, где автоморфизмы типа $\overline{x}$ понимаются как действие сопряжением соответствующей матрицей x, то есть $\overline{x}(g) = xgx^{-1}$, где $g \in G$.

Для определения матриц x, y, z строится матрица $P \in GL_{20m}(\mathbf{F}_3)$, реализующая умножение на некоторый примитивный элемент r в мультипликативной группе поля $\mathbf{F}_{3^{20m}}$. Столбцы матрицы P^i, где $i \in \mathbb{N}$, представляют из себя столбцы матрицы P, умноженные на r^{i-1}, поэтому все матрицы P, P^2, …, $P^{3^{20m}-1}$ различны, поскольку порядок r равен $3^{20m} - 1$.

Матрицы x, y и z будут блочно-диагональными, причем верхние три блока будут размером $20m$, два из которых являются единичными матрицами, а третий — матрица P, стоящая на первом, втором и третьем местах в x, y и z соответственно. Последние блоки обозначим за x_1, y_1 и z_1, которые будут принадлежать классу C_{k-60m}, состоящему из коммутирующих матриц. Пусть C — фиксированная матрица, принадлежащая $GL_{k-60m}(\mathbf{F}_{3^m})$. Определим

$$C_{k-60m} = \{CDC^{-1} \mid D = diag\{d_1, \ldots, d_{k-60m}\}, d_1, \ldots, d_{k-60m} \in \mathbf{F}_{3^m}^*\}.$$

В качестве элемента $g \in G$ берем матрицу, состоящую из 16 блоков, причем размеры верхних левых девяти блоков равны $20m$, блоки, стоящие на диагоналях, являются невырожденными, а блоки, стоящие ниже диагональных, — нулевые.

В качестве используемой на втором этапе протокола матрицы f Алиса выбирает блочно-диагональную матрицу, два верхних блока которой равны P^{t_1} и P^{t_2} соответственно, где t_1, t_2 — случайные натуральные числа, не превосходящие $3^{20m} - 1$, третий — F' выбирается

из условия, что при приведении матрицы $b_1(g) + f$ методом Гаусса к ступенчатому виду мы должны получить вырожденную матрицу, четвертый — $F'' \in C_{k-60m}$.

Вычислительная сложность протокола. Сложность протокола оценена при фиксированных значениях параметров $k = 10001$, $m = 53$: на протокол требуется максимум 2^{105} операций в поле $\mathbf{F}_3$.

Оценка мощности множества генерируемых ключей. Количество различных ключей не менее 2^{1680}.

Стойкость протокола. Злоумышленник знает элементы g, $b_1(g) + f$, $a_1(b_1(g) + f), a_2(b_1(g) + f), b_2(g)$, следовательно, может получить $a_1(a_2(b_1(g) + f))$. Для поиска ключа можно попытаться найти автоморфизм $b' \in Aut(G)$ такой, что $b'(b_1(g) + f) = b_2(g)$, причем b' коммутирует со всеми элементами из U. Тогда при успешном поиске вычисляется $b' \circ a_1(a_2(b_1(g)+f)) = a_1(a_2(b'(b_1(g)+f))) = a_1(a_2(b_2(g))) = K$. Но тогда матрица $b_1(g) + f$ является прообразом $b_2(g)$ при действии автоморфизмом b', следовательно, является невырожденной. Полученное противоречие доказывает, что данный тип атаки к протоколу не применим.

Полный перебор всех автоморфизмов из подгрупп A и B также невозможен, поскольку они содержат не меньше, чем 2^{1680} различных элементов.

Благодарности. Автор выражает благодарность научному руководителю к.ф.-м.н. А. Е. Пакратьеву за постановку задачи и помощь в работе, а также к.ф.-м.н. А. В. Галатенко и к.ф.-м.н. В. А. Носову, которые ознакомились с результатами работы и сделали ряд полезных замечаний.

Список литературы

1. Романьков В. А. Алгебраическая криптография. — Омск: изд-во Ом. гос ун-та, 2013.

ПОДМНОЖЕСТВА МАЛОЙ МОЩНОСТИ В СИСТЕМАХ ШТЕЙНЕРА $S(2,4,4^h)$.

М. Э. Коваленко (Москва)

Системой Штейнера $S(t,k,v)$ называется пара $(V,\mathcal{B})$, где V — множество из v элементов, а $\mathcal{B}$ — семейство k-элементных подмножеств V, называемых *блоками*, таких, что любое t-элементное подмножество V лежит ровно в одном блоке. С основными результатами по системам Штейнера можно ознакомиться, например, в [1].

Наиболее изученными являются системы Штейнера с параметрами $t=2$ и $k=3$ называемые *системами троек Штейнера* $S(2,3,v)$. В России исследованием подобных систем Штейнера занимаются, в частности, В. А. и Д. В. Зиновьевы [2]. Системы Штейнера с $t=3, k=4$ также известны как *системы четверок Штейнера* $S(3,4,v)$ и тоже, в свою очередь, активно исследуются, в том числе и в России. Из последних работ можно отметить работу Д. И. Ковалевской и Ф. И. Соловьевой [3].

В последнее время уделяется больше внимания и системам Штейнера с $t=2, k=4$: так в 2010 году вышел первый обзор [4] о системах Штейнера $S(2,4,v)$. Но в то же время остается большое количество неисследованных вопросов и взаимосвязей с другими комбинаторными структурами.

Частным случаем $S(2,q,q^n)$ систем Штейнера являются системы прямых в аффинном пространстве $\mathbf{F}_q^n$ — $\mathbf{EG}_1(4,h)$.

А именно, аффинная геометрия $\mathbf{EG}(n,p^s)$ — аффинное пространство $\mathbf{F}_{p^s}^n$, где точки — это вектора из $\mathbf{F}_{p^s}^n$, прямые — это одномерные подпространства $\mathbf{F}_{p^s}^n$ и их смежные классы (по операции сложения векторов), d-мерные плоскости — d-мерные подпространства $\mathbf{F}_{p^s}^n$ и их смежные классы.

При этом, как известно, например, из [5], существует единственная система Штейнера $S(2,4,16)$, и она изоморфна аффинной плоскости. Заметим, что с ростом n появляются $S(2,q,q^n)$ системы Штейнера, не изоморфные системе, соответствующей набору прямых в аффинном пространстве.

Системы Штейнера, изоморфные аффинным геометриям, назовем *системами Штейнера особого вида.*

Здесь и далее подразумевается, что поле $\mathbf{F}_4$ реализовано в виде фактор-алгебры $\mathbf{F}_2[x]\Big/\{x^2+x+1\}$.

Теперь обратимся к строению $S(2,4,n)$. Введем для $S(2,4,n)$ следующие обозначения для различных множеств по 4 элемента, а имен-

но: $\mathbf{B}_0$ — блоки $S(2,4,n)$; $\mathbf{B}_1$ — 4-х элементные множества, пересекающиеся с каким-нибудь блоком ровно по трем элементам; $\mathbf{B}_2$ — остальные 4-х элементные множества, т. е. пересекающиеся со всеми блоками не более чем по двум элементам.

Заметим, что эти классы множеств не пересекаются. Рассмотрим множества $\mathbf{B}_2$. Они могут быть получены из трех пар блоков (так как разбиваются на три различные пары по два элемента), блоки внутри пар могут пересекаться или нет. Такие три пары блоков назовем *образующими*. Среди множеств, входящих в $\mathbf{B}_2$, за $\mathbf{S}_i$ обозначим множество четверок, для которых среди 3 пар образующих их блоков ровно в i парах есть пересечение. Выберем четверку из $\mathbf{S}_2$. Назовем две пары пересекающихся образующих блоков *проверочными*.

Рассмотрим совокупность всех подмножеств $\mathbf{F}_4^h$ как векторное пространство над $\mathbf{F}_2$ с операцией симметрической разности. Обозначим это векторное пространство за $\mathcal{A}(h)$, а за $x_i(a)$ — i-ю координату элемента $a \in A \in \mathcal{A}(h)$ или, что то же самое, $a \in \mathbf{F}_4^h$. Выбранное пространство эквивалентно булеву кубу размерности 4^h.

Итак, в $\mathbf{F}_4^h$ каждому двоичному вектору $c \in \mathbf{F}_2^{4^h}, \mathrm{wt}(c) = p$, соответствует p-множество точек из V, а им в свою очередь соответствуют p точек из $\mathbf{F}_4^h$, каждая из этих точек задается h координатами из $\mathbf{F}_4$. Тогда введем операцию сложения блоков или множеств точек из $\mathbf{F}_4^h$: при сложении рассматриваем двоичные векторы кода, соответствующие слагаемым, получаем двоичный вектор суммы и рассматриваем соответствующий ему блок или множество точек. Эта операция по своей сути эквивалентна операции симметрической разности для множеств. Блокам $S(2,4,4^h)$ соответствуют прямые $\mathbf{F}_4^h$.

Теорема 1. *Для любой системы Штейнера $S(2,4,4^h)$ особого вида сумма любых проверочных блоков принадлежит этой системе.*

Квазигруппой Штейна называют пару $(P;\circ)$, если P группоид, а $\circ$ удовлетворяет следующим свойствам:

$$x \circ x = x;\ (x \circ y) \circ y = y \circ x;\ (y \circ x) \circ y = x.$$

Тогда рассмотрим $B := \{\{x, y, x \circ y, y \circ x\} | x, y \in P, x \neq y\}$. Очевидно, что (P, B) является системой Штейнера $S(2,4,v)$, и по системе Штейнера $S(2,4,v)$ можно построить квазигруппу Штейна. Для этого определим на $\{0,1,2,3\}$ бинарную операцию «$\cdot$»:

$$\left(\begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 2 & 3 & 1 \\ 1 & 3 & 1 & 0 & 2 \\ 2 & 2 & 3 & 2 & 0 \\ 3 & 1 & 0 & 1 & 3 \end{array}\right).$$

Тогда для каждого блока $b \in B$ выберем биекцию $\phi_b : b \to \{0;1;2;3\}$ и определим на P операцию «$\circ$» так: $x \circ y := \phi_b^{-1}(\phi_b(x) \cdot \phi_b(y))$, для всех $x, y \in P$, для которых определены $\phi_b(x)$ и $\phi_b(y)$. Полученная пара $(P;\circ)$ будет квазигруппой Штейна.

Известно, что, если для квазигруппы Штейна выполняется дистрибутивность $(x \circ y) \circ (z \circ w) = (x \circ z) \circ (y \circ w)$, то соответствующая система Штейнера будет особого вида. Также можно отметить выполнение указанной дистрибутивности для блоков и проверочных четверок. То же верно и для проверочных блоков. Можно утверждать следующее:

Теорема 2. *В системах Штейнера особого вида отсутствуют четверки вида* $\mathbf{S}_1$ *и* $\mathbf{S}_3$.

Более того для четверок $\mathbf{S}_3$ верно и обратное:

Теорема 3. *Если для любых проверочных блоков их сумма принадлежит системе Штейнера, то в ней не могут лежать четверки, для которых среди трех пар образующих блоков во всех парах есть пересечение.*

Список литературы.

1. Colbourn C. J., Dinitz J. H. Handbook of combinatorial designs, second edition. — Chapman and Hall, CRC, 2006.

2. Zinoviev V.A., Zinoviev D.V. Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+1 over $\mathbf{F}_2$ // Problems of Information Transmission — 2012. — Vol. 48, no. 2 — P. 102–126.

3. Ковалевская Д. И., Соловьева Ф. И. О системах четвёрок Штейнера малого ранга, вложимых в расширенные совершенные двоичные коды // Дискретн. анализ и исслед. опер. — 2012. — Т. 19, № 5. — С. 47 – 62.

4. Reid C., Rosa A. Steiner systems $S(2,4,v)$ — a survey // The Electronic Journal of Combinatorics. — 2010. — DS18.

5. Таранников Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011.

ОБОБЩЁННЫЕ ТАБЛИЦЫ СООТВЕТСТВИЯ СОСТОЯНИЙ СПЕЦИАЛЬНЫХ КЛАССОВ РЕГУЛЯРНЫХ ЯЗЫКОВ И ОЦЕНКИ ЧИСЛА ЭТИХ ТАБЛИЦ

С. Ю. Корабельщикова (Архангельск),
Б. Ф. Мельников (Самара)

Согласно [1, 2] и др., каждому регулярному языку можно с помощью специального сюръективного отображения поставить в соответствие определённое для этого языка бинарное отношение # (или, по-другому, таблицу соответствия состояний). Это бинарное отношение определено для пар, состоящих из Q_π (состояние автомата $\widetilde{L}$ — канонического автомата для рассматриваемого регулярного языка L) и Q_ρ (состояние автомата $\widetilde{L^R}$ — канонического автомата для регулярного языка L^R). Более того, также согласно [1, 2] (см. также [3]), при некоторых ограничениях на отношение # любой вариант этого отношения соответствует некоторому регулярному языку L — языку полного конечного автомата.

При этом по таблице соответствия состояний определяются псевдоблоки — пара непустых подмножеств $P \subseteq Q_\pi$ и $R \subseteq Q_\rho$, таких что

$$(\forall p \in P)\ (\forall r \in R)\ (p \# r).$$

Среди псевдоблоков особое значение имеют блоки, для каждого из которых (пусть рассматриваемый псевдоблок — снова (P, R)) дополнительно выполняются следующие два условия:

$$\big(\forall p \in Q_\pi \backslash P\big)\ \big(\text{пара}\,(P \cup \{p\}, R)\,\text{не является псевдоблоком}\big);$$

$$\big(\forall r \in Q_\rho \backslash R\big)\ \big(\text{пара}\,(P, R \cup \{r\})\,\text{не является псевдоблоком}\big).$$

Несложно показывается, что в случае $|Q_\pi| = |Q_\rho| = n$ максимально возможным количеством блоков является $2^n - 2$.

При рассмотрении специальных классов регулярных языков [4; гл.7] (см. также [5, 6] и др.) возникают задачи, являющиеся обобщением вышеописанных на k-мерный случай. В этом случае состояния канонических конечных автоматов $\widetilde{L}$ и $\widetilde{L^R}$ строятся на основе различных вариантов двух непустых непересекающихся подмножеств k-элементных множеств. В общем вместо бинарных рассматриваются k-арные отношения, для которых аналогичным образом

определяются псевдоблоки и блоки. Например, для $k = 3$ псевдоблоком является тройка непустых подмножеств $P \subseteq Q_\pi$, $R \subseteq Q_\rho$ и $S \subseteq Q_\sigma$, таких что

$$(\forall p \in P)\ (\forall r \in R)\ (\forall s \in S)\ (\#(p, r, s)).$$

Полученные объекты мы называем обобщёнными таблицами соответствия состояний специальных классов регулярных языков.

После определения блока несложно показывается, что если тройка (P, R, S) образует блок (в 3-мерном случае), то пара (P, R) образует блок в 2-мерном случае. (Аналогично — для 2 оставшихся пар подмножеств, для многомерного случая, и т.д.)

Обозначив записью $\Omega_k(n)$ максимально возможное число k-арных блоков в случае, когда каждое из k подмножеств состоит из n элементов, мы при $k = 2$ несложно получаем достижимую нижнюю оценку значения $\Omega_2(n)$:

$$\Omega_2(n) = 2^n - 2.$$

(Здесь в наших обозначениях в 2-мерном случае выше рассматриваются 2 подмножества, P и R.) Поэтому на основе вышеизложенного очевидны такие нижние оценки значений $\Omega_k(n)$:

$$\Omega_k(n) \geq 2^n - 2.$$

Сформулируем сказанное выше, а также некоторые факты, в виде следующих утверждений.

Утверждение 1. $\Omega_2(n) = 2^n - 2$.

Утверждение 2. $(\forall k \geq 2)\,(\Omega_k(n) < \Omega_{k+1}(n))$.

Отметим, что из сказанного выше следовало только нестрогое неравенство. Строгое неравенство является следствием того факта, что при построении проекции k-арного отношения на меньшую размерность прообразы некоторых псевдоблоков, не являющихся блоками, могут являться блоками.

Утверждение 3.

$$\Omega_3(n) \geq 6 - n + \sum_{i=2}^{n-1} (2^i - 2) \cdot C_n^i\,.$$

Последняя оценка получена путём рассмотрения конкретного примера.

Список литературы

1. Долгов В. Н., Мельников Б. Ф. Построение универсального конечного автомата. I. От теории к практическим алгоритмам // Вестник Воронежского государственного университета. Серия «Физика. Математика». — 2013. — № 2. — С. 173–181.

2. Долгов В. Н., Мельников Б. Ф. Построение универсального конечного автомата. II. Примеры работы алгоритмов // Вестник Воронежского государственного университета. Серия «Физика. Математика». — 2014. — № 1. — С. 78–85.

3. Долгов В. Н., Мельников Б. Ф. Об алгоритмах автоматического построения Ватерлоо-подобных конечных автоматов на основе полных автоматов // Эвристические алгоритмы и распределенные вычисления. — 2014. — № 4. — С. 24–45.

4. Саломаа А. Жемчужины теории формальных языков. — М.: Мир, 1986.

5. Мельников Б. Ф. Описание специальных подмоноидов глобального надмоноида свободного моноида // Известия высших учебных заведений. Математика. — 2004. — № 3. — С. 46–56.

6. Корабельщикова С. Ю., Чесноков А. И., Тутыгин А. Г. О первообразных корнях из языков специального вида // Труды IX Международной конференции «Дискретные модели в теории управляющих систем». — 2015. — С. 116–118.

О РАССТОЯНИИ ХЭММИНГА МЕЖДУ САМОДУАЛЬНЫМИ БУЛЕВЫМИ БЕНТ-ФУНКЦИЯМИ

А. В. Куценко (Новосибирск)

В данной работе рассматриваются бент-функции — булевы функции от чётного числа переменных, обладающие максимально возможной нелинейностью — одним из важнейших криптографических свойств и в силу этого представляющие большой интерес.

Скалярным произведением векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_2^n$ называется число $\langle x, y\rangle = \bigoplus\limits_{i=1}^{n} x_i y_i$, где операция $\oplus$ есть *сложение* по модулю 2. *Преобразование Уолша—Адамара*

булевой функции f от n переменных — целочисленная функция $W_f : \mathbb{Z}_2^n \to \mathbb{Z}$: $W_f(y) = \sum\limits_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x,y \rangle}$. В 60-х годах XX века О. Ротхаусом было введено понятие *бент-функции*. Одними из первых отечественных учёных, исследовавших эти функции в то же время, были В. А. Елисеев и О. П. Степченков [1]. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{Z}_2^n$ [2]. Для каждой бент-функции f равенством $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$, $x \in \mathbb{Z}_2^n$ определяется *дуальная* к ней булева функция $\tilde{f}$. Бент-функция f называется *самодуальной (анти-самодуальной)*, если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается как $dist(f, g)$.

Сложной задачей является полная характеризация и описание класса самодуальных бент-функций. Этим и другим вопросам посвящены несколько работ за рубежом (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou и др.). В частности, в работе [3] перечислены все самодуальные бент-функции от 2, 4, 6 переменных и все квадратичные самодуальные бент-функции от 8 переменных. В статье [4] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных можно найти в работе [5].

Известна следующая конструкция бент-функций — *конструкция Мэйорана—МакФарланда*, 1973 г.: пусть h — любая перестановка на $\mathbb{Z}_2^n$, пусть g — произвольная булева функция от $n/2$ переменных. Тогда функция $f(x, y) = \langle x, h(y) \rangle \oplus g(y)$ является бент-функцией от n переменных [6]. Эта конструкция является достаточно богатой. В работе [3] были найдены необходимые и достаточные условия самодуальности бент-функции, построенной с помощью конструкции Мэйорана—МакФарланда, в случае $h \in GL(n/2, \mathbb{Z}_2)$.

В работе получен полный спектр расстояний Хэмминга между бент-функциями из класса Мэйорана—МакФарланда, совпадающими со своими дуальными, со следующим ограничением: перестановка, фигурирующая в данной конструкции, должна быть элементом полной линейной группы соответствующего порядка. На основании этого результата сделан вывод о минимальном расстоянии Хэмминга между рассмотренными функциями.

Теорема. *Пусть f_1, f_2 — различные бент-функции от чётного*

числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана—МакФарланда при условии, что перестановка является элементом $GL(n/2, \mathbb{Z}_2)$. Если f_1, f_2 — самодуальные бент-функции, то

$$dist(f_1, f_2) = \begin{cases} 2^{n-1} \\ 2^{n-1}\left(1 \pm \frac{1}{2}\right) \\ 2^{n-1}\left(1 \pm \frac{1}{2^2}\right) \\ \vdots \\ 2^{n-1}\left(1 \pm \frac{1}{2^{n/2-1}}\right) \\ 2^n \end{cases}.$$

Следствие. *Пусть f_1, f_2 — различные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана—МакФарланда при условии, что перестановка является элементом $GL(n/2, \mathbb{Z}_2)$. Если f_1, f_2 — самодуальные бент-функции, то*

$$dist(f_1, f_2) \geqslant 2^{n-2}.$$

Список литературы

1. Tokareva N. Bent functions: results and applications to cryptography. — Acad. Press. Elsevier, 2015.

2. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. — 1976. — V. 20, I. 3. — P. 300–305.

3. Carlet C., Danielson L. E., Parker M. G., Solé P. Self dual bent functions // Int. J. Inform. Coding Theory. — 1. — 2010. — P. 384–399.

4. Hou X. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. — 2012. — 63. — P. 183–198.

5. Feulner T., Sok L., Solé P., Wassermann A. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr — 2013. — 68. — P. 395–406.

6. McFarland R. L. A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. — 1973. — V. 15, I. 1. — P. 1–10.

О РАСПРЕДЕЛЕНИИ НЕТЕРМИНАЛОВ В ДЕРЕВЬЯХ ВЫВОДА СОГЛАСОВАННОЙ СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКИ

И. М. Мартынов (Нижний Новгород)

В работе исследуются деревья вывода высоты t, порождаемые согласованной стохастической КС-грамматикой, при $t \to \infty$.

Стохастической КС-грамматикой [1] называется четвёрка $G = \langle V_N, V_T, R, s\rangle$, где V_N и V_T — конечные алфавиты *нетерминальных* и *терминальных* символов, $s \in V_N$ — аксиома, $R = \cup_{i=1}^{n} R_i$, где $n = |V_N|$ и R_i — конечное множество *правил вывода* r_{ij} вида:

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij},$$

где $j = 1, 2, \ldots, |R_i|$, $A_i \in V_N$, $\beta_{ij} \in (V_N \cup V_T)^*$, и p_{ij} — вероятность применения правила r_{ij}, причём $0 < p_{ij} \leq 1$ и $\sum_{j=1}^{n_i} p_{ij} = 1$.

Применение правила r_{ij} грамматики к слову $\alpha \in (V_N \cup V_T)^*$ состоит в замене какого-либо вхождения нетерминала A_i в α на слово β_{ij}. Язык L_G, порождаемый грамматикой G, содержит все слова из алфавита V_T, которые можно получить из аксиомы s последовательным применением правил вывода.

Каждому слову α из L_G соответствует последовательность $\omega(\alpha) = (r_1, r_2, \ldots, r_k)$ правил вывода, с помощью последовательного применения которых слово α можно получить из аксиомы s. При этом $\omega(\alpha)$ называется *выводом* слова α. Выводу слова соответствует *дерево вывода* [2] d, вероятность $p(d)$ которого определяется как произведение вероятностей правил, образующих вывод: $p(d) = \prod_{i=1}^{k} p(r_i)$. Одному и тому же слову $\alpha \in L_G$ может соответствовать более одного дерева вывода. Вероятность слова $\alpha \in L_G$ определяется как сумма вероятностей всех порождающих его деревьев.

Грамматика называется *согласованной*, если сумма вероятностей всех конечных деревьев вывода равна 1. Согласованная стохастическая грамматика G задаёт распределение вероятностей на множестве слов порождаемого ею языка L_G. В работе рассматриваются согласованные грамматики.

По стохастической КС-грамматике строится матрица A первых моментов. Её элемент a_j^i определяется как $\sum_{k=1}^{n_i} p_{ik} s_{ik}^j$, где величина s_{ik}^j равна числу нетерминальных символов A_j в правой части правила вывода r_{ik}. *Перронов корень* [3] матрицы A обозначим через r. Известно, что для согласованной грамматики $r \leq 1$.

Будем обозначать $A_i \to A_j$, если в грамматике имеется правило вывода вида $A_i \xrightarrow{p_{ij}} \alpha_1 A_j \alpha_2$, где $\alpha_1, \alpha_2 \in (V_N \cup V_T)^*$. Рефлексивное транзитивное замыкание отношения $\to$ обозначим $\to_*$. Будем обозначать $A_i \leftrightarrow_* A_j$, если одновременно $A_i \to_* A_j$ и $A_j \to_* A_i$. Множество V_N нетерминалов разбивается на классы эквивалентности $K_1, K_2, \ldots, K_m$ по отношению $\leftrightarrow_*$. Будем обозначать $K_i \prec K_j$, если существуют $A_{k_i} \in K_i$ и $A_{k_j} \in K_j$, такие что $A_{k_i} \to A_{k_j}$. Рефлексивное транзитивное замыкание $\prec$ обозначим $\prec_*$.

Случай $r < 1$ (докритический случай) рассматривался Л. П. Жильцовой в [4] и других работах. А. Е. Борисов обобщил полученные результаты на случай $r \leq 1$ для разложимой грамматики, содержащей два класса нетерминалов.

Пусть классы нетерминалов пронумерованы таким образом, что $i \leq j$ для любых $K_i \prec_* K_j$. Матрица A первых моментов грамматики в этом случае имеет вид:

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1,m} \\ 0 & A_{22} & \cdots & A_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{m,m} \end{pmatrix}.$$

Для каждого класса K_i матрица A_{ij} неразложима. Обозначим через r_i перронов корень матрицы A_{ii}. Очевидно, $r = \max_i\{r_i\}$. Обозначим $J = \{i : r_i = r\}$.

Для пары классов K_i и K_j рассмотрим всевозможные цепочки $K_{i_1} \prec K_{i_2} \prec \ldots \prec K_{i_k}$, где $i_1 = i$ и $i_k = j$. Обозначим через s_{ij} максимальное число классов с номерами из J в такой цепочке. Будем также обозначать $s_i = \max_j\{s_{ij}\}$.

Рассмотрим случайное дерево вывода d высоты t, порождённое грамматикой. Обозначим число применений правила r_{ij} в таком дереве через $q_{ij}(t)$, и число нетерминалов A_i в дереве через $q_i(t)$.

Теорема 1. *Для деревьев вывода высоты t, порождённых согласованной стохастической КС-грамматикой, выполняются соотношения:*

$$M(q_{ij}(t)) \sim c_i \cdot p_{ij} \cdot t^{\left(\frac{1}{2}\right)^{s_1 - s_{1l} - 1}},$$

$$M_i(t) \sim d_i \cdot t^{\left(\frac{1}{2}\right)^{s_1 - s_{1l} - 1}}$$

где p_{ij} — вероятность правила r_{ij}, c_i и d_i — некоторые константы, и $A_i \in K_l$.

Теорема 2. *Для любой пары нетерминалов $A_i \in K_h$, $A_j \in K_l$, такой что $s_{1h} = s_{1l}$, при $t \to \infty$ выполняется условие:*

$$D\left(\frac{q_i(t)}{q_j(t)} - \frac{d_i}{d_j}\right) \to 0,$$

где $q_i(t)$, $q_j(t)$ — число нетерминалов A_i и A_j в случайном дереве вывода высоты t, d_i и d_j — некоторые константы.

Теоремы 1 и 2 обобщают результаты, опубликованные в [5] и [6].

Таким образом, соотношение числа нетерминалов в деревьях вывода высоты t становится всё ближе к фиксированному значению при $t \to \infty$.

Список литературы

1. Фу. К. Структурные методы в распознавании образов. — М.: Мир, 1977.

2. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. — М.: МИР, 1978.

3. Гантмахер Ф. Р. Теория матриц. — М.: ФИЗМАТЛИТ, 2010.

4. Жильцова Л. П. Закономерности применения правил грамматики в выводах слов стохастического контекстно-свободного языка // Математические вопросы кибернетики. — М.: Наука, 2000. Вып. 9. — С. 101–126

5. Мартынов И. М. О распределении нетерминалов в деревьях вывода стохастической КС-грамматики вида "цепочки"// Материалы XVII Международной конференции "Проблемы теоретической кибернетики"(Казань, 16–20 июня 2014 г.). — С. 195–197.

6. Мартынов И. М. О числе нетерминалов в деревьях вывода разложимой стохастической КС-грамматики // Труды IX Международной конференции "Дискретные модели в теории управляющих систем". (Москва и Подмосковье, 20–22 мая 2015 г.) — С. 159-161.

О ПРИМЕНЕНИИ БУЛЕВЫХ ФУНКЦИЙ ДЛЯ ПОСТРОЕНИЯ КВАЗИГРУПП И СИНТЕЗА БЛОЧНЫХ ШИФРОВ

В. А. Носов, А. Е. Панкратьев (Москва)

Для криптографических приложений большой интерес представляют способы построения широких классов квазигрупп. Различные

квазигрупповые операции, определенные на одном множестве элементов, используются для синтеза поточных шифров [1]; таблица Кэли квазигруппы, представляющая собой латинский квадрат, служит основой для шифра табличного гаммирования.

Один из способов построения больших параметрических семейств латинских квадратов основан на использовании семейств функций, обладающих свойством правильности [2]. А именно, семейство функций $F = \{f_1, \ldots, f_n\}$ от n переменных $x_1, \ldots, x_n$ называется правильным, если для любых различных наборов $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ найдется индекс α такой, что $x'_\alpha \neq x''_\alpha$, но при этом $f_\alpha(x') = f_\alpha(x'')$.

Теорема [2]. *Пусть L — матрица размера $2^n \times 2^n$, элементы которой суть n-мерные двоичные векторы, причем номера строк и столбцов матрицы L представлены также в виде двоичных векторов размерности n. Далее, пусть элемент $L(x, y) = (z_1, \ldots, z_n)$ на пересечении строки $x = (x_1, \ldots, x_n)$ и столбца $y = (y_1, \ldots, y_n)$ определяется формулами*

$$z_i = x_i + y_i + f_i(p_1(x_1, y_1), p_2(x_2, y_2), \ldots, p_n(x_n, y_n)), \qquad i = 1, \ldots, n,$$

где p_i и f_i, $i = \overline{1, n}$, являются булевыми функциями соответственно от 2 и от n переменных.

Тогда матрица L является латинским квадратом при любом выборе функций p_i, $i = \overline{1, n}$, в том и только том случае, когда семейство $F = \{f_1, f_2, \ldots, f_n\}$ является правильным.

Имеется ряд примеров правильных семейств функций в произвольных размерностях. Кроме того, установлены некоторые их свойства (в том числе в терминах графа существенной зависимости) и исследованы мощности образов соответствующих отображений. Однако вопрос о нахождении количества правильных семейств функций произвольной размерности и их полной классификации пока остается открытым.

Еще одно криптографическое применение правильных семейств функций связано с возможным обобщением схемы Фейстеля.

Схема Фейстеля [2] — криптографический примитив, широко используемый при синтезе блочных шифров. Входной блок текста подразбивется на правую и левую половины (L_0, R_0) и преобразуется по формулам

$$\begin{cases} L_1 = R_0, \\ R_1 = L_0 \oplus F(R_0, K_0), \end{cases}$$

где функция F осуществляет усложняющее преобразование, зависящее от ключа K_0. Как правило, в системах защиты информации используется несколько итераций схемы Фейстеля с подходящим выбором ключей.

Рассмотрим шифр, который преобразует блок $x = (x_1, \ldots, x_n)$ двоичного текста длины $n = 2^k$ в блок $y = (y_1, \ldots, y_n)$ шифртекста по правилу

$$y_j = x_j + f_j(p_1(x_1), p_2(x_2), \ldots, p_n(x_n)), \qquad j = \overline{1,n}, \qquad (0)$$

где p_i и f_i, $i = \overline{1,n}$, суть булевы функции от 1 и от n аргументов соответственно. Сформулируем условия, которым должно удовлетворять семейство функций $F_0 = \{f_1, \ldots, f_n\}$ для того, чтобы отображение (0) являлось биекцией при любом выборе функций $p_1, \ldots, p_n$.

Теорема. *Отображение* (0) *является биекцией при любом выборе функций* p_i, $i = \overline{1,n}$, *тогда и только тогда, когда семейство функций* F_0 *является правильным.*

Теперь представим входной блок в виде последовательности биграмм $(x_1, \ldots, x_n) \to (x'_1, \ldots, x'_{n/2})$, $x'_i = (x_{2i-1}, x_{2i})$, и определим преобразование $x' \to y'$ блока биграмм по следующим формулам:

$$y'_j = x'_j + f'_j(p'_1(x'_1), p'_2(x'_2), \ldots, p'_{n/2}(x'_{n/2})), \qquad j = \overline{1,n/2}. \qquad (1)$$

Здесь p'_i и f'_i, $i = \overline{1,n}$, — функции 4-значной логики.

Теорема. *Отображение* (1) *является биекцией при любом выборе функций* p_i, $i = \overline{1,n}$, *тогда и только тогда, когда семейство функций* $F_1 = \{f'_1, \ldots, f'_{n/2}\}$ *является правильным.*

Теперь объединим биграммы в пары, далее перейдем к фрагментам по 8 бит, и продолжим укрупнять разбиение входного блока, попарно объединяя фрагменты. На каждом шаге приведенное выше утверждение о биективности отображения остается справедливым.

Наконец, на $(k-1)$-м шаге укрупнения мы получаем два полублока $x_1^{(k-1)} = (x_1, x_2, \ldots, x_{2^{k-1}})$, $x_2^{(k-1)} = (x_{2^{k-1}+1}, x_{2^{k-1}+2}, \ldots, x_{2^k})$, которые преобразуются по формулам

$$y_j^{(k-1)} = x_j^{(k-1)} + f_j^{(k-1)}(p_1^{(k-1)}(x_1^{(k-1)}), p_2^{(k-1)}(x_2^{(k-1)})), \qquad (k-1)$$

где $j = 1, 2$.

Теорема. *Отображение* $(k-1)$ *является биекцией при любом выборе* $p_1^{(k-1)}, p_2^{(k-1)}$ *если и только если семейство* $\{f_1^{(k-1)}, f_2^{(k-1)}\}$

является правильным; в случае двух функций это означает, что одна из функций является константой, а другая не зависит существенным образом от одноименного аргумента.

Нетрудно видеть, что, с точностью до перестановки полублоков, полученное преобразование соответствует классической схеме Фейстеля.

Таким образом, в работе предлагается метод обобщения схемы Фейстеля посредством подразбиения входного блока на более чем два фрагмента, выбора правильного семейства функций $\{f_j\}$, и использования преобразований (0), (1), ..., $(k-1)$, где функции p_j играют роль сменных ключей. Вопрос об оптимальном выборе шага укрупнения остается открытым, поскольку его нахождение сопряжено с определением мощности ключевого пространства, что напрямую связано с подсчетом количества правильных семейств соответствующей размерности.

Список литературы

1. Markovski S., Gligoroski D., Bakeva V. Quasigroup string processing: Part 1 // Proc. of Maced. Acad. of Sci. and Arts for Math. and Tech. Sci. — 1999. — XX (1–2). — P. 13–28.

2. Feistel H. Cryptography and computer privacy // Scientific American. — 1973. — 228 (5). — P. 15–23.

3. Nosov V. A., Pankratiev A. E. Latin squares over Abelian groups // Journal of Mathematical Sciences. — 2008. — 149 (3). — P. 1230–1234.

О ВОЗМОЖНОСТИ ПОСТРОЕНИЯ m-УСТОЙЧИВЫХ ФУНКЦИЙ С ОПТИМАЛЬНОЙ НЕЛИНЕЙНОСТЬЮ В РАМКАХ ОДНОГО МЕТОДА

Ю. В. Таранников (Москва)

Вес $\mathrm{wt}(f)$ булевой функции f над $\mathbf{F}_2^n$ — это число наборов x из $\mathbf{F}_2^n$, для которых $f(x) = 1$. *Подфункцией* булевой функции f называется функция f', полученная подстановкой в f некоторых констант 0 или 1 вместо некоторых переменных.

Для двух булевых функций f_1 и f_2 на $\mathbf{F}_2^n$ расстояние между f_1 и f_2 определяется как $d(f_1, f_2) = |\{x \in \mathbf{F}_2^n | f_1(x) \neq f_2(x)\}|$. Для заданной функции f из $\mathbf{F}_2^n$ минимум расстояний $d(f, l)$, где l пробегает множество всех аффинных функций, называется *нелинейностью* функции f и обозначается через $\mathrm{nl}(f)$.

Булева функция f от n переменных называется m-устойчивой, если $\mathrm{wt}(f') = 2^{n-m-1}$ для любой ее подфункции f' от $n-m$ переменных.

Нелинейность и корреляционная иммунность (m-устойчивость) относятся к числу наиболее важных криптографических характеристик булевых функций, поэтому крайне желательно, чтобы функции, использующиеся в шифрах, обладали одновременно высокими нелинейностью и устойчивостью. Однако в 2000 была доказана [1–3] верхняя оценка нелинейности m-устойчивых функций на $\mathbf{F}_2^n$:

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^{m+1} \tag{1}$$

при $m \leq n-2$, в которой если и может достигаться равенство, то только при $\frac{n-3}{2} \leq m \leq n-2$. Одновременно в [2] были построены функции, для которых достигалось равенство в (1) при $\frac{2n-7}{3} \leq m \leq n-2$. Отсюда актуальной стала задача построения функций, достигающих равенства в оценке (1) (как говорили, построения функций с максимально возможной нелинейностью). С практической точки зрения важна не столько нелинейность, сколько *относительная нелинейность,* т. е. величина $\frac{\mathrm{nl}(f)}{2^n}$, точнее, отклонение относительной нелинейности от 0.5. Отклонение относительной нелинейности любой булевой функции на $\mathbf{F}_2^n$ от 0.5 не меньше $\frac{1}{2^{\frac{n}{2}+1}}$, в то же время, если построить m-устойчивую функцию на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ при m, близком к $0.5n$, то отклонение ее относительной нелинейности от 0.5 будет равно $\frac{1}{2^{n-m-1}}$, т. е. близко к нижней оценке наилучшего возможного отклонения. Поэтому прогресс в задаче построения m-устойчивых функций на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ при m, близких к $0.5n$, по прежнему является важным, потому что позволит соединить нелинейность, близкую к оптимальной, с очень высокой устойчивостью. Область значений параметров, для которых построены функции, на которых достигается равенство в (1), неоднократно расширялась. В 2014 году с помощью техники *обобщенных подходящих матриц* в [4] построены функции, достигающие равенства в (1), для $m \geq 0.5789...n(1+o(1))$. В [5] техни-

ка рекурсивного построения обобщенных подходящих матриц была сформулирована на языке несократимых разложений сумм продуктов.

Утверждение 1. [5] *Пусть* $n, C_k \in \mathbf{N}$, $C_k \leq A_{n,k}$, $k = 0, 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$, *где* $A_{n,k}$ — *максимально возможное значение длины суммы* (n,k)*-продуктов с несократимым разложением. Положим* $C = \frac{1}{1+\log_2 X_{max}}$, *где* X_{max} — *старший корень многочлена* $x^n - \sum\limits_{k=0}^{\lfloor \frac{n}{2} \rfloor} C_k x^k$. *Тогда для любого* $\varepsilon > 0$, *начиная с некоторого* n_0, *для всех пар* (n,m), *таких что* $\frac{m}{n} > C + \varepsilon$, $n \geq n_0$, $m \leq n-2$, *существует* m*-устойчивая функция от* n *переменных, на которой достигается равенство в* (1).

В связи с этим становится понятно, что для того, чтобы с помощью техники рекурсивного построения обобщенных подходящих матриц работ [4] и [5] была возможность построить m-устойчивые функции на $\mathbf{F}_2^n$ с оптимальной нелинейностью с отношением m/n, стремящимся к 0.5, нужно, чтобы старший корень X_{max} уравнения

$$x^n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} A_{n,k} x^k \tag{2}$$

с ростом n стремился к 2.

В настоящей работе показывается, что X_{max} не стремится к 2.

Пусть $k/n \to \lambda$; предположим, что k-е слагаемое — максимальное в правой части (2).

Из $A_{n,k} \leq \frac{\binom{n}{k}}{2^k}$ следует, что $X_{max}^n \leq X_{max}^k \cdot \frac{2^{nH(k/n)}}{2^k} \cdot Pol(n)$, т. е.

$$X_{max} \leq 2^{(H(\lambda)-\lambda)/(1-\lambda)}.$$

Аналогично из $A_{n,k} \leq \binom{n}{2k}$ следует, что $X_{max}^n \leq X_{max}^k \cdot 2^{nH(2k/n)} \cdot Pol(n)$, т. е.

$$X_{max} \leq 2^{H(2\lambda)/(1-\lambda)}.$$

Таким образом, $X_{max} \leq \min\{2^{(H(\lambda)-\lambda)/(1-\lambda)}, 2^{H(2\lambda)/(1-\lambda)}\}$.

Равенство $H(\lambda) - \lambda = H(2\lambda)$ достигается при $\frac{H(\lambda)-\lambda}{1-\lambda} = 0.97896...$, что с учетом поведения графиков функций дает $X_{max} \leq 1.971044...$

Отсюда следует, что ограничиваясь средствами, предложенными в [4, 5], нельзя построить m-устойчивые функции от n переменных с

оптимальной нелинейностью при $m/n \leq \frac{1}{1+\log_2(1.971044...)}(1+o(1)) = 0.505316...(1+o(1))$. Впрочем, сказанное не исключает дальнейшего совершенствования методов. Заметим, что отношение m/n, близкое к 0.505316..., для многих практических целей является хорошим, поэтому построения в рамках техники [5] тоже представляют интерес.

Работа выполнена при финансовой поддержке РФФИ, проект 16–01–00226.

Список литературы

1. Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions // Advanced in Cryptology: Crypto 2000, Proceedings. Lecture Notes in Computer Science. — Springer-Verlag, 2000. — V. 1880. — P. 515–532.

2. Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity // Proceedings of Indocrypt 2000. Lecture Notes in Computer Science. — Springer-Verlag, 2000. — V. 1977. — P. 19–30.

3. Zheng Y., Zhang X.-M. Improved upper bound on the nonlinearity of high order correlation immune functions // Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000. Lecture Notes in Computer Science. — Springer-Verlag, 2001. — V. 2012. — P. 264–274.

4. Tarannikov Y. V. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters // Сибирские электронные математические известия — 2014. — V. 11. — P. 229-245 (`http://semr.math.nsc.ru/v11/p229-245.pdf`).

5. Таранников Ю. В. Несократимые разложения однородных произведений двучленов для построения m-устойчивых функций с максимально возможной нелинейностью // Проблемы теоретической кибернетики. Материалы XII международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 271–272.

СОХРАНЯЮЩИЕ МЕРУ И ЭРГОДИЧЕСКИЕ АСИНХРОННО АВТОМАТНЫЕ ОТОБРАЖЕНИЯ

Л. Б. Тяпаев (Саратов)

Автоматные преобразования над алфавитом $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, где p простое, совпадают с непрерывными в p-адической метрике преобразованиями кольца целых p-адических чисел $\mathbb{Z}_p$. Более того, отображения реализуемые синхронными автоматами удовлетворяют p-адическому условию Липшица с константой равной 1. Характеризация сохраняющих меру и эргодических 1-липшицевых преобразований была получена В. С. Анашиным [1]. Автоматные отображения в ракурсе геометрических образов — множеств точек плоскости с рациональными координатами, а также динамических систем — аффинных и ортогональных преобразований геометрических образов, изучались автором ранее [4–7]. Объектом исследования является асинхронно автоматное преобразование (специального типа) кольца $\mathbb{Z}_p$ в контексте p-адической динамики: автоматы рассматриваются как динамические системы на фазовом пространстве $\mathbb{Z}_p$.

Синхронный автомат (преобразователь) это шестерка объектов $\mathfrak{A} = (\mathfrak{I}, \mathcal{S}, \mathcal{O}, S, O, s_0)$, где $\mathfrak{I}$ — входной алфавит, $\mathcal{S}$ — множесто состояний автомата, $\mathcal{O}$ — выходной алфавит, $S\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{S}$ — функция переходов, $O\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{O}$ — функция выхода, $s_0 \in \mathcal{S}$ — начальное состояние. *Асинхронный автомат* $\mathfrak{B}$ определяется похожим образом, за исключением функции выхода: $O\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{O}^*$. Т. о., синхронные автоматы осуществляют отображения «буква в букву», асинхронные же — «буква в слово». Алфавиты $\mathfrak{I}, \mathcal{O}$ суть конечные множества, однако $\mathcal{S}$ не обязательно конечно. Будем рассматривать достижимые автоматы: любое состояние $s \in \mathcal{S}$ автомата достижимо из начального состояния s_0 после подачи на вход автомата слова $u \in \mathfrak{I}^*$ конечной длины. Положим $\mathfrak{I} = \mathcal{O} = \mathbb{F}_p$.

В случае с автоматом $\mathfrak{A}$ слова конечной длины над алфавитом $\mathbb{F}_p$ суть неотрицательные целые числа: слово $u = \alpha_{n-1} \ldots \alpha_1 \alpha_0$, где $\alpha_i \in \mathbb{F}_p$ $i = 0, 1, 2, \ldots, n-1$, мы рассматриваем как число $\alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{n-1} \cdot p^{n-1}$, записанное в системе счисления с основанием p. В свою очередь, это число есть элемент кольца вычетов $\mathbb{Z}/p^n\mathbb{Z}$ по модулю p^n. Т. о., каждому автомату $\mathfrak{A}$ соответсвует отображение $\mathbb{Z}/p^n\mathbb{Z}$ в $\mathbb{Z}/p^n\mathbb{Z}$, для всех $n = 1, 2, 3 \ldots$. Более того, каждый автомат $\mathfrak{A}$ *определяет отображение* $f_{\mathfrak{A}}$ *из кольца целых* p*-адических чисел* $\mathbb{Z}_p$ *в себя*: слово бесконечной длины $\alpha = \ldots \alpha_{n-1} \ldots \alpha_1 \alpha_0$ над алфавитом $\mathbb{F}_p$ рассматривается как целое p-адическое число x, $x = x(\alpha) = \alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{n-1} \cdot p^{n-1} + \ldots = \sum_{i=0}^{\infty} \delta_i(x) \cdot p^i$, где $\delta_i(x) \in \mathbb{F}_p$. Для

любого $x \in \mathbb{Z}_p$ положим $\delta_i(f_{\mathfrak{A}}(x)) = O(\delta_i(x), s_i)$, $i = 0, 1, 2, \ldots$, где $s_i = S(\delta_{i-1}(x), s_{i-1})$, $i = 1, 2, \ldots$. Будем говорить, что отображение $f_{\mathfrak{A}}$ является *автоматным отображением* автомата $\mathfrak{A}$. Аналогичным образом мы можем рассматривать и *асинхронно автоматные отображения*: асинхронный автомат $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0)$ осуществляет преобразование $f_{\mathfrak{B}}$ кольца целых p-адических чисел $\mathbb{Z}_p$. Класс автоматных отображений совпадает с классом 1-липшицевых отображений [1]; класс асинхронно автоматных отображений — нет.

Рассмотрим асинхронно автоматные отображения специального типа. Отображение $f_{\mathfrak{B}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется *отображением с задержкой* n, $n \in \mathbb{N}$, если данный асинхронный автомат $\mathfrak{B}$ бесконечное слово $\alpha = \ldots \alpha_{n-1} \ldots \alpha_1 \alpha_0$ преобразует в слово $\beta = \ldots \beta_{n+1} \beta_n$ так что, $O(\delta_i(\alpha_{n-1} \ldots \alpha_1 \alpha_0), s_i) = e$, где e пустое слово, $i = 0, 1, 2 \ldots, n-1$, $s_i = S(\delta_i(\alpha_{n-1} \ldots \alpha_1 \alpha_0), s_{i-1})$, $i = 1, 2, \ldots, n-1$; $O(\delta_i(\alpha), s_i) = \delta_i(\beta)$, $i = n, n+1, \ldots$. Заметим что, как правило, термин «задержка» («задержка на n тактов») используется в более узком смысле (по сравнению, например, с [3]): а именно, преобразователь с задержкой определяется как автомат, который прочитывает входное слово буква за буквой в течение первых n тактов и печатает пустое слово; после этого автомат выдает входное слово без изменений. В частности, *односторонний сдвиг* [2], определяется асинхронным автоматом с одиночной задержкой.

Динамическая система есть тройка $(\mathbb{S}, \mu, f)$, где S есть измеримое пространство с мерой μ, а $f \colon \mathbb{S} \to \mathbb{S}$ измеримая функция. Пространство $\mathbb{S}$ называют *фазовым пространством. Траекторией динамической системы* называется последовательность $x_0, x_1 = f(x_0), \ldots\ x_i = f(x_{i-1}) = f^i(x_0), \ldots$. Точка x_0 называется *начальной точкой* траектории. Отображение $F \colon \mathbb{S} \to \mathbb{S}$ называется *сохраняющим меру*, если $\mu(F^{-1}(S)) = \mu(S)$ для всякого измеримого $S \subset \mathbb{S}$. Сохраняющее меру отображение F называется *эргодическим*, если для каждого измеримого $S \subset \mathbb{S}$ такого, что $F^{-1}(S) = S$, либо $\mu(S) = 1$, либо $\mu(S) = 0$. Тройка $(\mathbb{Z}_p, \mu, f)$, где $f = f_{\mathfrak{B}}$ отображение с задержкой n, суть динамическая система на фазовом пространстве $\mathbb{Z}_p$. Элементарными подмножествами в $\mathbb{Z}_p$ являются шары $B_{p^{-k}}(a) = a + p^k \mathbb{Z}_p$, причем $\mathbb{Z}_p$ можно снабдить нормализованной *мерой Хаара* $\mu = \mu_p$: $\mu_p(\mathbb{Z}_p) = 1$ и $\mu_p(B_{p^{-k}}(a)) = p^{-k}$. Пусть F_k редукция f по модулю $p^{n \cdot (k-1)}$ на элементах кольца $\mathbb{Z}/p^{n \cdot k}\mathbb{Z}$ для $k = 2, 3, \ldots$.

Теорема. *Отображение $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ с задержкой n сохраняет меру тогда и только тогда, когда число $\#F_k^{-1}(x)$ F_k-прообразов*

точки $x \in \mathbb{Z}/p^{n\cdot(k-1)}\mathbb{Z}$ *равно* p^n, $k = 2, 3, \ldots$.

Пусть $x_0 \in \mathbb{Z}_p$ и существует $r \in \mathbb{N}$ такое, что $f^r(x_0) = x_0$. Число r — *длина* периода точки x_0. Орбита точки x_0 есть $\{x_0, x_1, \ldots, x_{r-1}\}$, где $x_j = f^j(x_0)$, $0 \leq j \leq r-1$. Такая орбита называется r-*циклом*. Пусть $\gamma(k)$ есть $r(k)$-цикл $\{x_0, x_1, \ldots, x_{r(k)-1}\}$, $k = 1, 2, 3, \ldots$, где $x_j = (f \mod p^{kn})^j(x_0)$, $0 \leq j \leq r(k)-1$.

Теорема. *Пусть отображение* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *с задержкой* n *сохраняет меру. Тогда* f *эргодично, если* $\gamma(k)$ *единственный цикл, для всех* $k \in \mathbb{N}$.

Список литературы

1. Anashin V., Krennikov A. Applied algebraic dynamics. — Berlin-N.Y.: Walter de Gruyter GmbH & Co., 2009.

2. Grigorchuk R. I, Nekrashevich V. V., Sushchanskii V. I. Automata, dynamical systems, and groups // Proc. Steklov Institute Math. — 2000. — 231. — P. 128–203.

3. Linz P.. An introduction to formal languages and automata. — Jones and Bartlett learning, 2011.

4. Тяпаев Л. Б. Геометрическая модель поведения автоматов и их неотличимость // Математика. Механика. — Изд-во Сар. ун-та, 1999. — С. 139–143.

5. Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сар. ун-та, Нов. серия. Сер.: Математика. Механика. Информатика — 2006. — 6 (1-2) — С. 121–133.

6. Тяпаев Л. Б. Геометрические образы автоматов и динамические системы// Материалы X Международного семинара "Дискретная математика и ее приложения". — М.: Изд-во мех.-мат. факультета МГУ, 2010. — С. 510–513.

7. Тяпаев Л. Б., Василенко Д. В. Дискретные динамические системы, определяемые геометрическими образами автоматов // Интеллектуальные системы. — 2013. — 17 (1-4). — С. 196–201.

О ДВУХ НОВЫХ РЕКУРСИВНЫХ КОНСТРУКЦИЯХ ПЛАТОВИДНЫХ УСТОЙЧИВЫХ БУЛЕВЫХ ФУНКЦИЙ

Е. В. Хинко (Москва)

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и регулярно поднимается в работах многих авторов. Например, в [1] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работе [2] построены соответствующие конструкции функций. В [3] Ю. В. Тарannиковым построены рекурсивные конструкции устойчивых булевых функций с высокой нелинейностью, где на каждом шаге рекурсии добавляется пара квазилинейных переменных. К относительно схожей теме в [4] также обращался К. В. Захаров, исследовавший рекурсивные конструкции бент-функций, которые можно считать подмножеством платовидных, с шагом числа переменных 2.

Задачу проделанной работы можно в общей формулировке поставить следующим образом: пусть имеются b, $b \in \mathbb{N}$, платовидных m-устойчивых булевых функций от n переменных $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, среди которых, возможно, есть совпадающие с точностью до взятия отрицания; добавим три переменные x_{n+1}, x_{n+2} и x_{n+3}. Новые функции от $n+3$ переменных обозначим $f_{n+3}^s(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, x_{n+3})$, $s = 1, \ldots, 8$.

Представляет интерес подбор соотношений индикаторов σ_{sj} и порождающих функций f_n^i, чтобы для полученных новых функций от $n+3$ переменных выполнялись следующие свойства:

а) сохранение свойства платовидности;

б) обеспечение роста устойчивости;

в) рекурсивное воспроизведение конструкции.

Связь между функциями от n и $n+3$ переменных можно схематично записать так:

$$f_{n+3}^s = \sigma_{s1} g_{s1} \ |\sigma_{s2} g_{s2} \ |\sigma_{s3} g_{s3} \ |\sigma_{s4} g_{s4} \ |\sigma_{s5} g_{s5} \ |\sigma_{s6} g_{s6} \ |\sigma_{s7} g_{s7} \ |\sigma_{s8} g_{s8},$$

где $g_{sj} = f_n^i$ или $g_{sj} = \overline{f_n^i}$; $s, j \in \{1, \ldots, 8\}$; $i \in \{1, \ldots, b\}$.

Введём обозначение

$$\sigma_{sj} g_{sj} = \begin{cases} f_n^i, \sigma_{sj} = 1, \\ \overline{f_n^i}, \sigma_{sj} = -1, \end{cases}$$

где $s = 1, \ldots, 8$. Здесь σ_{sj} выполняет роль индикатора: выбирается функция или её отрицание.

В [5] автором была построена конструкция с примерами начальных функций для случая $b = 4$, удовлетворяющая приведённым условиям, где порождающие функции $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, удовлетворяют следующим свойствам:
(К1) каждый двоичный набор $u \in V_n$ содержится в носителе спектра в точности нуля, двух или всех четырёх функций;
(К2) мощности всевозможных попарных пересечений носителей спектров порождающих функций f_n^i, $i = 1, \ldots, 4$, совпадают, а мощность пересечения носителей спектров всех четырёх функций равна четверти мощности носителя спектра каждой функции;
(К3) для каждого набора $u \in V_n$, содержащегося в носителе спектра всех четырёх функций f_n^i, $i = 1, \ldots, 4$, коэффициенты Уолша трёх функций одного знака, а четвёртой — другого знака.

Отличительной особенностью построенной в [5] конструкции, а также конструкций, построенных в данной работе, является то, что рассматривается случай порождающих функций с пересекающимися носителями спектра, в то время как в большинстве из построенных ранее конструкций порождающие функции обладали непересекающимися носителями спектра.

В настоящей работе представлены две новые конструкции, удовлетворяющие поставленной задаче.

Первая конструкция схожа с построенной в [5], в ней присутствуют такие же соотношения между функциями f_n^i, $i = 1, \ldots, 4$ и f_{n+3}^i, $i = 1, \ldots, 4$, что и в [5], однако (К2) выглядит иначе: "мощность пересечения носителей спектров всех четырёх функций f_n^i, $i = 1, \ldots, 4$, равна пяти восьмым мощности носителя спектра каждой функции". Таким образом показано, что вторая часть (К2) из [5] является достаточным, но не необходимым условием существования конструкции, удовлетворяющей поставленной задаче, для случая $b = 4$.

Вторая конструкция является примером выполнения поставленной задачи для случая $b = 2$.

В качестве индикаторов σ_{sj}, как и в конструкции для $b = 4$ из [5], берутся строки матрицы Адамара—Сильвестра порядка 8 (строки нумеруются с 1), только немного видоизменённые:
$f_{n+3}^1 : S^1 = (+-+-+--+)$ (то есть строка 2, с инвертированными символами 7-8 или строка 6 с инвертированными символами 5–6),
$f_{n+3}^2 : S^2 = (+--++-+-)$ (то есть строка 4, с инвертированными символами 7-8 или строка 8 с инвертированными символами 5–6).

Полученные функции также могут быть записаны следующим образом:
$f^1_{n+3}(\overrightarrow{x}, x_{n+1}, x_{n+2}, x_{n+3}) = f^1_n(\overrightarrow{x}) \cdot (x_{n+1}+1) + f^2_n(\overrightarrow{x}) \cdot x_{n+1} + x_{n+1} \cdot x_{n+2} + x_{n+3}$,
$f^2_{n+3}(\overrightarrow{x}, x_{n+1}, x_{n+2}, x_{n+3}) = f^1_n(\overrightarrow{x}) \cdot (x_{n+1}+1) + f^2_n(\overrightarrow{x}) \cdot x_{n+1} + x_{n+1} \cdot x_{n+2} + x_{n+2} + x_{n+3}$.

Список литературы

1. Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001. Proc. Lecture Notes in CS. — V. 2247. — P. 254–256.

2. Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics. — V. 6.

3. Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — 2002. — С. 91–148.

4. Захаров К. В. О порождении бент-функций рекурсивными конструкциями. — Дипломная работа, 2008.

5. Хинко Е. В. Об одной рекурсивной конструкции платовидных устойчивых булевых функций с шагом числа переменных 3 // ПДМ. — 2016. — № 1 (31). — С. 92–103.

ХЕШ-ФУНКЦИИ В БУЛЕВОМ КУБЕ

А. В. Чашкин (Москва)

Пусть $D \subseteq \{0,1\}^n$. Линейный оператор $f_a : \{0,1\}^n \to \{0,1\}^m$ назовем линейной a-хеш-функцией ранга m множества D, если у любого элемента из $f_a(D) = \{\boldsymbol{y} \in \{0,1\}^m \,|\, \boldsymbol{y} = f_a(\boldsymbol{x}),\ \boldsymbol{x} \in D\}$ в D существует не более a прообразов. Известно (см., например, [1]), что при $a = 1$ имеет место следующее утверждение.

Теорема 1. *Для любой области $D \subseteq \{0,1\}^n$, состоящей из не более чем $\sqrt{2^n}$ наборов, найдется линейная 1-хеш-функция, для числа компонент которой справедливо неравенство*

$$m \leq \lfloor 2 \log_2 |D| \rfloor - 1.$$

Покажем, что для бóльших значений параметра a справедлива аналогичная теорема.

Теорема 2. *Пусть D — M-элементное подмножество в $\{0,1\}^n$ и $a \leq M^{1/2} 2^{-5}$. Для D найдется линейная a-хеш-функция, для числа компонент которой справедливо неравенство*

$$m \leq \lfloor 2 \log_2 M - 2 \log_2 a \rfloor - 1.$$

Для доказательства теоремы 1 достаточно несколько раз подряд использовать тот простой факт, что линейный оператор $f : \{0,1\}^k \to \{0,1\}^{k-1}$ является линейной 1-хеш-функцией множества $D \subseteq \{0,1\}^k$ тогда и только тогда, когда его ядро не пересекается с множеством попарных сумм элементов из D. В основе доказательства теоремы 2 лежит аналогичный факт: *линейный оператор $f : \{0,1\}^k \to \{0,1\}^{k-2}$ является линейной 2-хеш-функцией множества $D \subseteq \{0,1\}^k$ тогда и только тогда, когда его ядро содержит не более одной из трех попарных сумм любых трех элементов из D.* Действительно, линейный оператор f отображает наборы $\boldsymbol{x}, \boldsymbol{y}$ и $\boldsymbol{z}$ в один и тот же набор только в том случае, когда попарные суммы этих наборов принадлежат ядру оператора, т. е. $f(\boldsymbol{x} \oplus \boldsymbol{y}) = f(\boldsymbol{x} \oplus \boldsymbol{z}) = f(\boldsymbol{y} \oplus \boldsymbol{z}) = 0$. При этом, если 2-мерное подпространство содержит две попарные суммы, например, $\boldsymbol{x} \oplus \boldsymbol{y}$ и $\boldsymbol{x} \oplus \boldsymbol{z}$, то это подпространство содержит и третью сумму, так как $\boldsymbol{y} \oplus \boldsymbol{z} = (\boldsymbol{x} \oplus \boldsymbol{y}) \oplus (\boldsymbol{x} \oplus \boldsymbol{z})$.

В доказываемой далее лемме используется простое обобщение указанного выше свойства линейного оператора быть 2-хеш-функцией множества.

Лемма 1. *Пусть D — M-элементное подмножество в $\{0,1\}^n$, f_a — a-хеш-функция ранга m множества D, и*

$$a^2 2^{2m-2} \geq 9M^3. \tag{1}$$

Тогда для D существует $2a$-хеш-функция ранга $m-2$.

Доказательство. Множество $f_a(D)$ разобъем на два подмножества A и B, первое из которых состоит из элементов, имеющих в D не менее $a/3$ прообразов, а второе из всех остальных. Очевидно, что $|A| \leq 3M/a$. Трехэлементное подмножество в $f_a(D)$ назовем

«плохим», если число прообразов его элементов больше $2a$. Легко видеть, что подмножество будет «плохим» только в том случае, когда не менее двух его элементов лежит в A. Поэтому число «плохих» подмножеств не больше чем

$$\binom{|A|}{2}|B| + \binom{|A|}{3} = \frac{|A|(|A|-1)}{2}|B| + \frac{|A|(|A|-1)(|A|-2)}{6} < \\ < \frac{|A|^2}{2}\Big(|B| + \frac{|A|}{3}\Big) < \frac{|A|^2 M}{2} \le \frac{9M^3}{2a^2}.$$

При $m \ge 5$ из предыдущего неравенства и неравенства (1) следует, что

$$\frac{(2^m-1)(2^m-2)}{6} > 2^{2m-3} \ge 9M^3/2a^2 > \binom{|A|}{2}|B| + \binom{|A|}{3},$$

т. е. число двумерных подпространств в $\{0,1\}^m$ больше числа «плохих» трехэлементных подмножеств в $f_a(D)$. Каждое трехэлементное подмножество $\{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}\}$ в $\{0,1\}^m$ однозначно определяет в $\{0,1\}^m$ единственное двумерное подпространство $\mathsf{H}_{\boldsymbol{xyz}} = \langle \boldsymbol{x}\oplus\boldsymbol{y}, \boldsymbol{x}\oplus\boldsymbol{z}\rangle$, которое содержит все три попарные суммы элементов этого множества. Поэтому в $\{0,1\}^m$ найдется 2-мерное подпространство H, которое не совпадает ни с одним из подпространств $\mathsf{H}_{\boldsymbol{xyz}}$, соответствующих «плохим» подмножествам. Следовательно, это подпространство H содержит не более одной из трех попарных сумм элементов из любого «плохого» подмножества в $f_a(D)$.

Пусть $f_{\mathsf{H}} : \{0,1\}^m \to \{0,1\}^{m-2}$ — линейный оператор с ядром H. Покажем, что композиция $f_{\mathsf{H}} \circ f_a$ будет $2a$-хеш-функцией множества D ранга $m-2$. Действительно, оператор f_{H} отображает в один и тот же набор не более четырех элементов множества $f_a(D)$. Если все эти элементы лежат в B, то число их прообразов в D не превосходит $4a/3$. Если один элемент лежит в A, а три — в B, то число их прообразов в D не превосходит $2a$. В остальных случаях среди этих элементов найдется не менее двух элементов из A, т. е. среди этих элементов можно выбрать три, которые будут образовывать «плохое» подмножество в $f_a(D)$, что, очевидно, невозможно, так как противоречит выбору оператора f_{H}. Таким образом, у рассматриваемых элементов общее число прообразов в D не больше $2a$. Лемма доказана.

Доказательство теоремы 2. Индукцией по k покажем, что если $k \le \lfloor \log_2 M^{1/2} \rfloor - 5$, то на множестве D существует 2^{k+1}-хеш-функция

$f_{2^{k+1}}$ ранга $m_k = \lfloor 2\log_2 M - 2(k+1)\rfloor - 1$. В основание индукции положим случай $k = 0$. В этом случае в силу теоремы 1 для множества D существует линейная 1-хеш-функция f_{2^0} с $m_0 = \lfloor 2\log_2 M\rfloor - 1$ компонентами. Допустим, что при $k \geq 0$ на D существует 2^k-хеш-функция f_{2^k} ранга $m_k = \lfloor 2\log_2 M - 2k\rfloor - 1$. Тогда из неравенства

$$2^{2k}2^{2m_k-2} = 2^{2k+2\lfloor 2\log_2 M-2k\rfloor-4} \geq 2^{4\log_2 M-2k-6} =$$
$$= M^4 2^{-2k-6} = M^4 2^{-2\lfloor \log_2 M^{1/2}\rfloor+4} > 16M^3$$

следует, что можно воспользоваться леммой 1. В силу этой леммы для множества D существует линейная 2^{k+1}-хеш-функция $f_{2^{k+1}}$ ранга $m_{k+1} = \lfloor 2\log_2 M - 2(k+1)\rfloor - 1$.

Пусть $2^k < a \leq 2^{k+1}$. Тогда линейный оператор $f_{2^{k+1}}$ будет на множестве D a-хеш-функцией ранга $m_{k+1} \leq \lfloor 2\log_2 M - 2\log_2 a\rfloor - 1$. Теорема доказана.

Работа выполнена при финансовой поддержке РФФИ, проект 14-01-00598.

Список литературы

1. Чашкин А. В. О линейных операторах, инъективных на произвольных подмножествах // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки, 156. — 2014. — Вып. 3. — С. 132–141.

РАСПРЕДЕЛЕНИЕ РАНГА КВАДРАТИЧНОЙ ФОРМЫ НАД ПОЛЕМ ИЗ ДВУХ ЭЛЕМЕНТОВ

А. В. Черемушкин (Москва)

Каждую квадратичную форму от n переменных ранга $2r$, $1 \leq r \leq \lfloor n/2\rfloor$, можно линейным преобразованием аргументов привести к виду $x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2r-1}x_{2r} \oplus l(x_1, \ldots, x_n)$, где l — некоторая линейная функция. Вероятность того, что квадратичная форма от n переменных имеет ранг $2r$, равна $p_{2r}(n) = Q_r(n)/2^{n(n-1)/2}$, где $Q_r(n)$ — число квадратичных форм от n переменных ранга $2r$. Из

описания групп автоморфизмов квадратичных форм [1 – 3] следует, что

$$Q_r(n) = \frac{(2^n-1)\dots(2^n-2^{2r-1})}{|\mathbf{Sp}(2r,2)|}, \tag{1}$$

где $|\mathbf{Sp}(2r,2)| = 2^{r^2}\prod\limits_{i=1}^{r}(2^{2i}-1)$. При $1 \le r \le n/2-1$ имеем

$$\frac{Q_r(n)}{Q_{r+1}(n)} = \frac{4}{(2^{n-2r}-1)(2^{n-2r-1}-1)}\left(1-\frac{1}{2^{2r+2}}\right). \tag{2}$$

Поэтому числа $Q_r(n)$, $1 \le r \le n/2-1$, образуют монотонно возрастающую последовательность.

Основным результатом является

Теорема. *Пусть $k = [n/2]$, $n = 2k+c$, $c = 0,1$, и последовательность ε_k выбрана так, что $\varepsilon_k\sqrt{\log_2 k} \to \infty$ при $k \to \infty$. Тогда при $n \to \infty$ доля квадратичных форм от n переменных ранга меньшего, чем $2k-2\left\lceil\sqrt{(\log_2 k)/2}+(\varepsilon_k+(-1)^c)/2\right\rceil$, стремится к нулю. Поэтому для ранга почти всех квадратичных форм q от n переменных при $n \to \infty$ справедлива оценка*

$$2k \ge r(q) \ge 2k-2\left\lceil\sqrt{\frac{1}{2}\log_2 k}+\frac{\varepsilon_k+(-1)^c}{2}\right\rceil+2.$$

Изучим теперь более подробно свойства распределения ранга. Сначала оценим вероятность максимальности ранга. Имеем

$$p_n(2k) = \begin{cases} \left(1-\frac{1}{2^{2k-1}}\right)\left(1-\frac{1}{2^{2k-3}}\right)\dots\left(1-\frac{1}{2}\right), & n=2k; \\ \left(1-\frac{1}{2^{2k+1}}\right)\left(1-\frac{1}{2^{2k-1}}\right)\dots\left(1-\frac{1}{2^3}\right), & n=2k+1. \end{cases}$$

В частности, $p_{2k-2}(2k-1) = 2p_{2k}(2k)$ при $k \ge 2$.

Верхнюю оценку вероятности $p_{2k}(2k)$ с наперед заданной точностью можно получить путём перемножения только части сомножителей, например, при $k > 14$

$$p_{2k}(2k) = \prod_{i=1}^{k}\left(1-\frac{1}{2^{2i-1}}\right) < \prod_{i=1}^{14}\left(1-\frac{1}{2^{2i-1}}\right) < 0{,}4194224428.$$

Нижнюю оценку вероятности $p_{2k}(2k)$ можно получить, используя подход из работы [4]:

$$\ln p_{2k}(2k) = \sum_{i=1}^{k} \ln\left(1 - \tfrac{1}{2^{2i-1}}\right) = -\sum_{i=1}^{k} \sum_{m=1} \tfrac{1}{m} \left(\tfrac{1}{2^{2i-1}}\right)^m =$$
$$= -\sum_{m=1} \tfrac{2^m}{m} \sum_{i=1}^{k} \left(\tfrac{1}{2^{2m}}\right)^i = -\sum_{m=1} \tfrac{2^{-m}}{m} \tfrac{1-1/(2^{2m})^k}{1-1/2^{2m}}.$$

При $k > s$ можно воспользоваться приближённой формулой

$$\ln p_{2k}(2k) > -\frac{2^{2m}}{2^{2m}-1} \ln 2 - \sum_{m=1}^{s-1} \tfrac{2^{-m}}{m} \left(\tfrac{1}{2^{2m}-1} - \tfrac{1}{2^{2r}-1}\right).$$

В частности, полагая $s = 8$, получаем, что при $k > 8$ имеет место нижняя оценка $p_{2k}(2k) > 0{,}41942244$. Поэтому при больших чётных $n = 2k > 28$

$$0{,}4194224428 > p_{2k}(2k) > 0{,}41942244.$$

При больших нечетных $n = 2k + 1 > 27$ получаем

$$0{,}8388448856 > p_{2k}(2k+1) = 2p_{2k+2}(2k+2) > 0{,}83884488.$$

Так как с уменьшением ранга вероятности $p_n(2r)$ быстро убывают, то для математического ожидания и дисперсии ранга случайной квадратичной формы от n переменных можно получить оценки с заданной точностью. Например, справедливо

Утверждение. *Пусть $k = \lfloor n/2 \rfloor$. При $n > 28$ для математического ожидания и дисперсии ранга $r(q)$ случайной квадратичной формы q от n переменных справедливы оценки:*

1) *при $n = 2k$ имеем*

$$\begin{aligned} 2k - 1{,}2014788 < {} & \mathrm{E}\, r(q) < 2k - 1{,}201478798\,(1 - 1/2^n), \\ 1{,}13053549\,(1 - 1/2^n) < {} & \mathrm{D}\, r(q) < 1{,}13053551; \end{aligned}$$

2) *при $n = 2k + 1$ имеем*

$$\begin{aligned} 2k - 0{,}324311085 < {} & \mathrm{E}\, r(q) < 2k - 0{,}324311084\,(1 - 1/2^n), \\ 0{,}554431153\,(1 - 1/2^n) < {} & \mathrm{D}\, r(q) < 0{,}554431159. \end{aligned}$$

Как следствие получаются оценки уровня аффинности двоичных функций степени нелинейности не выше двух. Уровень аффинности la(f) двоичной функции f определяется как минимальное число переменных, произвольная фиксация значений которых делает функцию аффинной. В терминах теории графов это соответствует вершинному покрытию графа, ассоциированного с квадратичной формой. Обобщенный уровень аффинности $\mathcal{L}a(f)$ двоичной функции f определяется как минимальное число линейных комбинаций переменных, некоторая фиксация значений которых делает функцию аффинной, $\mathcal{L}a(f) \leq$ la(f).

Поскольку обобщенный уровень аффинности квадратичной формы ранга $2r$ равен r, то из приведенных выше асимптотических оценок ранга непосредственно вытекают оценки обобщенного уровня аффинности для почти всех квадратичных функций, а также нижняя оценка вершинного покрытия для почти всех неориентированных графов. В частности, можно заметить, что оценки уровня аффинности почти всех квадратичных форм из [5] не являются точными.

Список литературы

1. Dixon L. E. Linear groups with an expositions to the Galois field theory. — Leipzig: Publ. by B. G. Teubner, 1901.

2. Дьедонне Ж. Геометрия классических групп. — М.: Мир, 1974.

3. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

4. Рязанов Б. В., Чечета С. И. О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. — 1995. — Т. 7, вып. 3. — С. 129–145.

5. Буряков М. Л. Асимптотические оценки уровня аффинности для почти всех булевых функций // Дискретная математика. — 2008. — Т. 20, вып. 3. — С. 73–79.

СПИСОК ПЛЕНАРНЫХ ДОКЛАДОВ, ПРОЧИТАННЫХ НА СЕМИНАРЕ

В. В. Кочергин (Москва) *Об одной задаче О. Б. Лупанова*

М. П. Минеев, В. Н. Чубариков (Москва) *Криптография и p-адический анализ*

А. М. Зубков, А. А. Серов (Москва) *Итерации случайных отображений конечных множеств*

Л. А. Шоломов (Москва) *Две постановки задачи кодирования недоопределенных данных*

С. А. Ложкин, В. А. Коноводов (Москва) *Синтез схем и формул из элементов с прямыми и итеративными входами*

Ф. М. Аблаев, М. Ф. Аблаев (Казань) *Квантовое криптографическое хеширование*

В. Б. Кудрявцев (Москва) *О кафедре МаТИС*

С. Н. Селезнёва (Москва) *Сложность полиномиальных представлений функций k-значной логики*

А. В. Тимофеенко (Красноярск) *К теории выпуклых многогранников с правильными и сложенными из правильных многоугольников гранями*

А. А. Часовских (Москва) *Условия выразимости и полноты в классах линейных автоматов*

И. П. Чухров (Москва) *Задача минимизации булевых функций: условия минимальности и вероятностный метод*

Ф. И. Соловьёва (Новосибирск) *О пропелинейных, транзитивных и гомогенных кодах*

Д. С. Кротов (Новосибирск) *Трейды в комбинаторных конфигурациях*

Д. Г. Мещанинов (Москва) *Семейства замкнутых классов в P_k, определяемых полиномиальными и аддитивными представлениями функций*

Р. М. Колпаков (Москва) *Об оценке числа и эффективном поиске повторов и палиндромов с разрывами в формальных словах*

С О Д Е Р Ж А Н И Е

Пленарные доклады

Секция «Синтез, сложность и надежность управляющих систем»

Секция «Функциональные системы»

Секция «Комбинаторный анализ»

Секция «Теория графов»

Секция «Математическая теория интеллектуальных систем»

Секция «Дискретная геометрия»

Секция «Теория кодирования и математические вопросы теории защиты информации»