

Федеральное государственное бюджетное образовательное
учреждение высшего образования

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.Ломоносова

Факультет вычислительной математики и кибернетики

Кафедра информационной безопасности

На правах рукописи

Логачев Олег Алексеевич

**ПОСТРОЕНИЕ И АНАЛИЗ ЭФФЕКТИВНОСТИ
АЛГОРИТМОВ ОБРАЩЕНИЯ ДИСКРЕТНЫХ
ФУНКЦИЙ В МАТЕМАТИЧЕСКИХ МОДЕЛЯХ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Специальность 05.13.19 — методы и системы защиты информации,
информационная безопасность

ДИССЕРТАЦИЯ

на соискание ученой степени

доктора физико-математических наук

МОСКВА — 2019

Оглавление

	Стр.
Основные обозначения	5
Введение	8
Глава 1. Алгебраические, комбинаторные и метрические характеристики дискретных функций, используемые в методах (алгоритмах) обращения	48
§1 Групповые дискретные функции	48
§2 Комплекснозначные функции на конечных абелевых группах и их свойства	51
§3 Групповые коды Рида-Маллера и их свойства	62
§4 Понятие дуальности для конечных модулей. Обобщённые тождества Мак-Вильямс	74
§5 Бент-функции на конечной абелевой группе	82
§6 sr -полиномы и приведенная оценка Вейля	95
§7 Некоторые характеристики "нелинейности" групповых отображений	105
§8 Невырожденные булевы функции	119
§9 Пространства линейных трансляторов и пустые секции Фурье-кластеризации булевых функций	127
§10 Δ -эквивалентность и глобальные лавинные характеристики булевых функций	131
Глава 2. О связях алгебраических, комбинаторных и криптографических свойств булевых функций со свойствами их сужений	135

§11	Сужения булевых функций	135
§12	Наследование комбинаторных и спектральных свойств при сужении булевых функций. (H, u) -стабильность.	138
§13	Аффинные сужения булевых функций и отображений. Понятие локальной аффинности	151
§14	Локальные аффинности булевых функций, связанные с фиксацией переменных	156
§15	Аффинная нормальная форма булевой функции и ее свойства . .	164
§16	Нелинейная аппроксимация булевых функций	172
 Глава 3. Математические модели обращения дискретных		
	функций	179
§17	Задача обращения дискретных функций в обеспечении информационной безопасности	179
§18	Теоретико-автоматная модель для задачи обращения	188
§19	Частично обратный автомат	191
§20	Асимптотическое поведение характеристик частичного обращения для БПИ-автоматов	197
§21	Локальное обращение БПИ-автоматов	203
§22	Локальное обращение неавтономных регистров сдвига с фильтрующими функциями	212
§23	Локальные аффинности в задачах обращения дискретных функций	226
§24	Синтез совершенно уравновешенных функций на основе операции "сдвиг-композиция"	240
§25	Теоретико-информационная характеристика совершенно уравновешенных функций	248
Заключение		256

Список литературы	261
Приложение А. Некоторые примитивы, используемые при синтезе средств обеспечения информационной безопасности	280
Приложение Б. Аффинная нормальная форма фильтрующей функции генератора псевдослучайных последовательностей шифра LiLi-128	284
Приложение В. Локальные аффинности булевых отображений	286
Приложение Г. Аффинное обращение ограниченно-детерминированных функций, реализуемых конечными автоматами вида $SR(n, f)$	290
Приложение Д. Обращение ограничено-детерминированной функции, реализуемой комбинирующим генератором с устойчивой функцией усложнения.	292

Основные обозначения

- $A, B, C, \dots, M$ — конечные и бесконечные множества;
- $x \in A$ — элемент x принадлежит множеству A (x лежит в A);
- $A = \{x : \text{условие на } x\}$ ($A = \{x \mid \text{условие на } x\}$) — множество A , задаваемое условием, которому должны удовлетворять его элементы;
- "стандартные" числовые множества:

$\mathbb{N}$ — множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$,

$\mathbb{Z}$ — множество всех целых рациональных чисел,

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ — кольцо вычетов по модулю n , $n \in \mathbb{N}$,

$\mathbb{Q}$ — множество всех рациональных чисел,

$\mathbb{R}$ — множество всех действительных (вещественных) чисел,

$\mathbb{R}^+ = \{x \in \mathbb{R}, x \geq 0\}$,

$\mathbb{C}$ — множество всех комплексных чисел;

- если A — множество, то $2^A = \{B : B \subset A\}$ — множество всех подмножеств множества A (включая $\emptyset$ и A);
- если A и B — множества, то множество $A \times B = \{(a, b) : a \in A, b \in B\}$ называется декартовым (прямым) произведением множества A на множество B . Декартово произведение трех, четырех и т.д. множеств определяется индуктивно. Для множества A и натурального n множество

$$A^n = \underbrace{A \times \dots \times A}_{n \text{ экземпляров множества } A}$$

называется n -й декартовой степенью множества A ;

- если A и B — множества, то B^A — множество всех отображений из A в B ;
- A^* — множество всех конечных наборов элементов множества A ;
- $\text{len}(u)$, $u \in A^*$ — длина набора u ;

- A^∞ — множество бесконечных вправо последовательностей элементов множества A ;
- если A — конечное множество, то $\#A$ — мощность множества A ;
- G, H — конечные группы;
- если G, H — группы, то $H < G$ — H подгруппа G , $H \triangleleft G$ — H — нормальный делитель G ;
- если G — конечная группа, то $\hat{G}$ — группа ее характеров;
- если G — конечная группа, то $\text{Aut}(G)$ — группа ее автоморфизмов;
- $\mathbb{F}_q$ — поле Галуа из $q = p^n$ (p — простое) элементов;
- $\mathbb{V}_n = \mathbb{V}_{n,q} = \mathbb{F}_q^n$ — векторное пространство над полем $\mathbb{F}_q$;
- $\mathcal{F}_{n,m,q}$ — множество всех отображений из $\mathbb{F}_q^n$ в $\mathbb{F}_q^m$
 $(\mathcal{F}_{n,1,q} = \mathcal{F}_{n,q}, \mathcal{F}_{n,m,2} = \mathcal{F}_{n,m}, \mathcal{F}_{n,1,2} = \mathcal{F}_n)$;
- если $\mathcal{D} \subset \mathbb{F}_2^n$, то $I^{\mathcal{D}} \in \mathcal{F}_n$ — индикаторная характеристическая функция множества $\mathcal{D}$, принимающая значение 1 тогда и только тогда, когда $x \in \mathcal{D}$;
- $\text{GA}(n,q)$ — полная аффинная группа над полем $\mathbb{F}_q$;
- $\text{GL}(n,q)$ — полная линейная группа над полем $\mathbb{F}_q$;
- S_n — симметрическая группа степени n ;
- $f^{-1}(b), f \in A^B, b \in B$ — полный прообраз элемента b относительно отображения f ;
- $x \preccurlyeq y, x, y \in \mathbb{F}_2^n$ — x не более, чем y , т.е. $x_i \leq y_i, i = 1, 2, \dots, n$;
- $[\alpha]$ — целая часть действительного числа α ;
- $\lceil \alpha \rceil$ — верхнее целое действительного числа α ;
- $\langle x, y \rangle, x, y \in \mathbb{F}_2^n$ — скалярное произведение векторов (наборов) над полем $\mathbb{F}_2$;
- $R[\lambda]$ — кольцо полиномов над кольцом R ;
- $\xi \in_{\mathcal{P}} A$ — случайная величина, принимающая значения в конечном множестве A в соответствии со законом $\mathcal{P}$;

- $\Pr [\xi = a]$ — вероятность того, что случайная величина ξ принимает значение a ;
- $\square$ — знак завершения доказательства.

Введение

Одной из фундаментальных проблем, имеющихся в области обеспечения информационной безопасности (ИБ), является проблема получения обоснованных оценок уровня защиты информации. Методы анализа систем (средств) обеспечения ИБ имеют математическую природу и используются в рамках математических моделей, описывающих функционирование таких систем, действия противника и возможные угрозы ИБ. Для решения задач анализа необходимы различные математические модели и активное использование методов таких разделов математики как математическая логика, алгебра, теория вероятностей и математическая статистика, дискретная математика, теория сложности вычислений и алгоритмов, теория игр, теория кодирования и криптология.

Диссертация представляет результаты исследований в области информационной безопасности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 05.13.19 (физико-математические науки).

Области исследования:

1. Теория и методология обеспечения информационной безопасности и защиты информации.
9. Модели и методы оценки защищенности информации и информационной безопасности объекта.
13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Актуальность темы. Математические методы и модели широко используются при синтезе и анализе объектов (механизмов и средств) информационной безопасности для решения следующих задач:

- обеспечения конфиденциальности информации;
- обеспечения целостности информации;

- обеспечения идентификации и аутентификации;
- обеспечения неотслеживаемости;
- обеспечения доступности информации;
- управления информационными ресурсами;
- разграничения доступа;
- разделения секрета;
- конфиденциальных вычислений и др. (см., например, [Yao 82], [Gol 01], [Gol 04]).

В используемых математических моделях достаточно часто можно выделить один системообразующий элемент, который сущностно позволяет решать указанные выше задачи. Неформально, это дискретная функция (система дискретных функций), обладающая следующими свойствами:

- 1° для любого допустимого аргумента значение функции вычисляется эффективно;
- 2° при известном значении функции вычисление значения аргумента, принадлежащего полному прообразу данного значения функции, является трудной проблемой.

В теоретическом плане понятия "эффективность" и "трудность" вычисления разработаны в теории сложности вычислений и криптологии.

Проблему, упомянутую выше в п. 2°, называют проблемой обращения дискретной функции. Она моделирует действия противника по реализации угрозы информационной безопасности и является центральной в ходе анализа информационной безопасности.

Функция, удовлетворяющая условиям 1° и 2°, получила название односторонней функции (one way function - см. [ArBa 09], [Gol 01], [Gol 04]). С целью обоснования важности задач обращения дискретных функций для обоснования моделей информационной безопасности рассмотрим это понятие подробнее.

Пусть $n \in \mathbb{N}$ и $\{0,1\}^*$ — множество всех конечных двоичных строк. Если строка $u \in \{0,1\}^n \subset \{0,1\}^*$, то длина строки $\text{len}(u) = n$. Для всякой функ-

ции $\varphi : \{0,1\}^* \rightarrow \{0,1\}^*$ через $\varphi^{(n)}$ обозначается ее ограничение (сужение) на множество $\{0,1\}^n$, т.е. функция, определенная на строках длины n (n -местная булева функция). Таким образом, функцию φ можно рассматривать просто как сокращенное обозначение для семейства $\{\varphi^{(n)}, n \in \mathbb{N}\}$.

В современном понимании (тезис Эдмондса, [ArBa 09]) эффективные алгоритмы — это полиномиальные алгоритмы, время реализации которых полиномиально зависит от длины входных данных, представляемых с помощью "разумных схем кодирования" (см. [ГэДж 82]). Например, в однородной модели вычислений эффективные алгоритмы ассоциируются с полиномиальными машинами Тьюринга (детерминированными и вероятностными), а в неоднородной модели вычислений — это семейство схем из функциональных элементов полиномиального размера (в базисах $\{\vee, \wedge, \neg\}$, $\{\wedge, \oplus, 1\}$ и др.).

Следует отметить, что упомянутые выше машины Тьюринга и схемы из функциональных элементов не исчерпывают все множество формализаций понятия алгоритма.

Рассмотрим теперь математическое определение односторонней функции. Функция $\varphi : \{0,1\}^* \rightarrow \{0,1\}^*$ называется односторонней (см. [Gol 01]), если выполнены следующие два условия:

- существует полиномиальный алгоритм A , вычисляющий $\varphi(x)$ для любого $x \in \{0,1\}^*$ (т.е. $A(x) = \varphi(x)$);
- для любого вероятностного полиномиального алгоритма A' и любого положительного полинома $p(\lambda) \in \mathbb{Z}[\lambda]$ неравенство

$$\Pr [A'(f(u^n), 1^n) \in \varphi^{-1}(f(u^n))] < \frac{1}{p(n)}$$

выполнено для всех достаточно больших $n \in \mathbb{N}$ (u^n — случайная строка, равномерно распределенная на множестве $\{0,1\}^n$, $n \in \mathbb{N}$ — параметр безопасности).

Важным в интерпретации сущности односторонней функции является то, что для достаточно больших n любой эффективный (полиномиальный) вероятностный алгоритм решает поставленную задачу нахождения элемента из фиксированного прообраза с пренебрежимо малой надежностью. Кроме того, полиномиальное от n число раз повторенная реализация этого вероятностного алгоритма "в среднем" также не даст решения задачи.

В качестве примера "кандидатов" на роль односторонних функций (см. [Gol 01]) можно упомянуть умножение целых рациональных чисел (задача обращения — разложение на множители) и дискретную экспоненту (задача обращения — дискретное логарифмирование).

Необходимо отметить, что в настоящее время нет примера функции, для которой было бы доказано, что она является односторонней функцией. Вместе с тем, существует и используется большое число практических приложений (в том числе и финансовых), обеспечение информационной безопасности которых основано на реализации функций - "кандидатов" в односторонние функции с конкретными значениями параметра безопасности (т.е. реализации сужений $\varphi^{(n)}$ для некоторых конкретных значений n). Следовательно, при фиксированном n (и, соответственно, реализованной функции $\varphi^{(n)}$ на $\{0,1\}^n$) отсутствует возможность (поскольку нет семейства функций с растущим параметром) обеспечивать необходимые свойства функции $\varphi^{(n)}$ с использованием понятия односторонней функции.

Необходимо отметить подход к оценке безопасности криптографических протоколов, называемый "доказуемой стойкостью" (provable security, см. например [Bell 99]). Этот подход решает определенные частные задачи обоснования свойств криптографических протоколов. Однако, получаемые на его основе результаты имеют относительный характер и сводятся к стойкости некоторых базовых криптографических примитивов (atomic primitive), используемых при синтезе криптографических протоколов.

В результате остается единственная в настоящее время возможность, заключающаяся в построении конкретных алгоритмов обращения функций. При этом вопрос об "эффективности" разработанных алгоритмов переходит из области теоретических разделов математики в область нормативных документов и практических приложений математики. Ярчайшими примерами этих процессов являются конкурсы на разработку хэш-функций (см. [FeRe 07]), потоковых шифров (см. [ECR 04]) и блочных шифров (см. [NIST 97]).

Задачи обращения дискретных функций, являющихся математическими моделями различных средств обеспечения информационной безопасности, имеют значительное число особенностей, определяемых исходными условиями анализа. В математическом плане отсутствует какой-либо перечень (классификация) задач обращения. Однако некоторые регулярно встречающиеся частные виды задач обращения могут быть сформулированы в достаточно краткой форме:

- а) полное обращение дискретной функции — описание полного прообраза для фиксированного значения функции;
- б) частичное обращение дискретной функции — описание множеств, в которые входит полный прообраз для фиксированного значения функции;
- в) поиск хотя бы одного прообраза для фиксированного значения функции;
- г) поиск при известном одном прообразе еще хотя бы одного прообраза для фиксированного значения функции.

Далее в работе будут даваться соответствующие пояснения всякий раз, когда будут рассматриваться конкретные виды обращения.

Приведем поясняющий пример, содержащий наряду с элементами упомянутых выше видов обращений и некоторые дополнительные особенности.

Пусть $f(x_1 x_2 \dots x_n)$ — булева функция от n переменных и m — некоторое натуральное число. Определим функцию $f_m : \{0,1\}^{m+n-1} \rightarrow \{0,1\}^m$ следующим образом

$$\begin{aligned} y^{(m)} &= (y_1 y_2 \dots y_m) = f_m(x_1 x_2 \dots x_{m+n-1}) = \\ &= (f(x_1 x_2 \dots x_n) f(x_2 x_3 \dots x_{n+1}) \dots f(x_m x_{m+1} \dots x_{m+n-1})) \end{aligned}$$

Предположим, что f является симметрической функцией (т.е. ее значения не зависят от перестановки переменных), а $x^{(m+n-1)} = (x_1 x_2 \dots x_{m+n-1})$ — фрагмент линейной рекуррентной последовательности порядка n с характеристическим полиномом $c(\lambda) = \bigoplus_{i=0}^n c_i \lambda^i$ ($c_0 = c_n = 1$, ” $\bigoplus$ ” — сложение по mod2).

Предположим, что известна строка $y^{(m)}$ и необходимо найти какие-либо алгебраические соотношения, которым должны удовлетворять элементы множества $f_m^{-1}(y^{(m)})$.

Напомним, что для фрагмента линейной рекуррентной последовательности $x^{(m+n-1)}$ справедливо следующее утверждение: для любого j , $1 < j \leq m+n-1$ существует линейная от переменных $\{x_1, x_2, \dots, x_n\}$ функция l_j такая, что $x_j = l_j(x_1 x_2 \dots x_n)$.

Будем считать, что строка $y^{(m)}$ отлична от строки, содержащей только одинаковые символы. Тогда существует j_0 , $1 \leq j_0 \leq m-1$ такое, что $y_{j_0} \oplus y_{j_0+1} = 1$ (т.е. $y_{j_0} \neq y_{j_0+1}$). Следовательно, наборы $(x_{j_0} x_{j_0+1} \dots x_{j_0+n-1})$ и $(x_{j_0+1} x_{j_0+2} \dots x_{j_0+n})$ имеют различное число компонент, равных 1, так как значения симметрической функции f на этих наборах различны. С другой стороны, множества компонент этих наборов различаются лишь парой компонент x_{j_0} и x_{j_0+n} . Получаем $x_{j_0} \neq x_{j_0+n}$ (т.е. $x_{j_0} \oplus x_{j_0+n} = 1$). Учитывая рекуррентность, имеем

$$\begin{aligned} x_{j_0} \oplus x_{j_0+n} &= l_{j_0}(x_1 x_2 \dots x_n) \oplus l_{j_0+n}(x_1 x_2 \dots x_n) = \\ &= l(x_1 x_2 \dots x_n) = 1, \end{aligned}$$

где $l(x_1 x_2 \dots x_n)$ — некоторая линейная функция. Таким образом, любая знакоперемена в строке $y^{(m)}$ определяет некоторое линейное соотношение, которому должен удовлетворять фрагмент линейной рекуррентной последовательности $x^{(m+n-1)}$, удовлетворяющий условию $y^{(m)} = f_m(x^{(m+n-1)})$. При определенных условиях наличие этих линейных соотношений позволяет однозначно восстановить $x^{(m+n-1)}$.

Заметим, что в приведенном выше примере функция выбрана из функционального класса - симметрические функции. Выбор функции из некоторого функционального класса вносит в задачу обращения конкретной функции определенную специфику. Укажем лишь на одну из возможных особенностей.

В различных разделах математики встречаются примеры функциональных классов, в которых каждая функция однозначно определяется по своим значениям, принимаемым на небольшом подмножестве области определения. Приведем три возможных варианта этого свойства: из области вещественных функций, из области полиномов над конечными полями и из области булевых функций.

Известно, что любой вещественный полином алгебраической степени $d-1$ однозначно определяется по своим значениям в d точках, не лежащих на кривой $(d-2)$ -степени. Поэтому можно говорить, что вся информация о полиноме конечной степени содержится в конечном числе его значений. Аналогичным свойством обладает полином алгебраической степени не превосходящей d над конечным полем, определяемый своими значениями в d различных элементах поля (интерполяционная формула Лагранжа). И, наконец, любая булева функция n переменных, степень многочлена Жегалкина которой не превосходит d , однозначно определяется по своим значениям в шаре радиуса d с центром в нулевом наборе. Следовательно, вся информация о булевой функции содержится в шаре, радиус которого равен степени ее полинома Жегалкина.

Математические задачи, которыми приходится заниматься с целью обращения дискретных функций в процессе синтеза и анализа средств обеспечения

информационной безопасности, настолько естественны, что многие из этих задач исследовались математиками в различных аспектах, исходя из совершенно иных соображений. Это обстоятельство влечет за собой различия в оценках и интерпретациях получаемых результатов. Информация о разработке алгоритма решения какой-либо математической задачи свидетельствует о ее алгоритмической разрешимости, но может мало говорить о возможной эффективности разработанного алгоритма.

Необходимо отметить еще один важный момент, связанный с синтезом и анализом дискретных функций, используемых для обеспечения информационной безопасности. Как правило, набор операций, реализующих синтезируемую дискретную функцию, достаточно беден (например, одна бинарная групповая операция и некоторое небольшое число унарных операций над соответствующими алфавитами). Выбор этих операций осуществляется в соответствии с рядом принципов. Одним из таких принципов является принцип итеративности структуры дискретной функции, обеспечивающий эффективность ее реализации и вычисления ее значений. Другим важным принципом является отсутствие "согласованности" используемых операций, т.е. отсутствие нетривиальных конгруэнций у порождаемой этими операциями алгебраической системы.

Именно этим объясняется скудность алгебраических моделей, используемых в анализе дискретных функций, описывающих функционирование средств информационной безопасности. Однако, развитый математический аппарат также необходим для совершенствования различных методов анализа информационной безопасности (комбинаторных, вероятностно-статистических, теоретико-кодowych и др.). Именно в связи с этим в области математических методов анализа информационной безопасности сформировалась тематика исследований, направленных на обобщение известных понятий, принципов и результатов, используемых в данной области. Содержательно, получаемые в этом направлении результаты способствуют совершенствованию математического аппарата, используемого в анализе информационной безопасности.

В определенном смысле процессы синтеза и анализа используемых для обеспечения информационной безопасности дискретных функций следуют известному в алгебре принципу координатизации. Некоторые фундаментальные черты изучаемых нами дискретных функций должны отражаться в координатизирующих параметрах и операциях, которые можно производить над этими параметрами.

Например, в [Шаф 86] координатизация представлена одним из основных этапов развития любого раздела алгебры: "... сталкиваясь с новым типом объектов, мы вынуждены конструировать (или открывать) и новые типы координатизирующих их величин."

Цель диссертационной работы — совершенствование математических моделей и повышение на основе полученных результатов эффективности методов решения задач обращения дискретных функций, используемых при синтезе средств обеспечения информационной безопасности.

Для достижения поставленной цели были решены следующие задачи:

1. Задача построения на множестве комплексных функций на конечной абелевой группе математической модели, представляющей код типа Рида-Маллера с соответствующими алгебраическими, комбинаторными и метрическими свойствами.
2. Задача построения на множестве комплексных функций на конечной абелевой группе математической модели, представляющей понятие обобщенной бент-функции.
3. Задача разработки и обоснования характеристик "нелинейности" групповых отображений.
4. Задача построения и обоснования новых нормальных форм булевых функций.
5. Задача наследования комбинаторных и спектральных свойств при сужении булевых функций.

6. Задача изучения алгебраических и комбинаторных свойств семейства локальных аффинностей произвольной булевой функции.
7. Задача построения алгоритмов обращения ограниченно-детерминированных (конечно-автоматных) функций и оценки параметров их эффективности.

В работе использованы математические методы теории групп, теории булевых функций, теории графов, комбинаторики, теории кодирования и теории автоматов.

Научная новизна работы характеризуется следующими результатами:

1. Для множества комплекснозначных функций на конечной абелевой группе предложен и развит математический аппарат, обобщающий понятие "алгебраической степени нелинейности" и другие параметры классических колец полиномов. На основе этого подхода для групповых функций получен ряд их свойств, аналогичных свойствам кодов Рида-Маллера.
2. Для произвольной конечной абелевой группы рассмотрено понятие бент-функции, обобщающее понятие бент-функции на элементарной абелевой p -группе. Получены аналоги свойств бент-функции для рассматриваемого обобщения, а также описан ряд его новых свойств.
3. Для группового отображения предложено представление, обобщающее аффинное расщепление булевых отображений. На основе параметров этого представления введена характеристика "нелинейности" исходного группового отображения. Получен ряд соотношений и неравенств, связывающих эту характеристику "нелинейности" с основными параметрами отображения.
4. Предложена новая нормальная форма булевой функции на основе понятия локальной аффинности булевой функции. Строение и особенности этой нормальной формы определяют перспективность ее исполь-

- зования при разработке алгоритмов и методов обращения дискретных функций, основанных на аффинной аппроксимации уравнений.
5. Предложен подход к изучению вопросов наследования комбинаторных и спектральных свойств при сужении булевых функций на основе понятия $(H, 0^n)$ -стабильности. Доказан критерий $(H, 0^n)$ -стабильности булевой функции, связывающий ее комбинаторные, спектральные и криптографические параметры.
 6. С целью развития аппарата анализа булевых функций и отображений рассмотрена концепция локальных аффинностей булевых функций при сужении их на плоскости в пространстве Хэмминга. Введены параметры, характеризующие структуру семейства локальных аффинностей булевой функции. Доказаны соотношения, показывающие влияние этих параметров на различные свойства булевых функций.
 7. Рассмотрена теоретико-автоматная модель частичного обращения ограниченно-детерминированных функций. Получены соотношения, показывающие влияние особенностей функции на параметры частичного обращения.
 8. Для автоматов Мили без потери информации рассмотрена модель локального обращения. Доказан критерий, показывающий, что наличие локального обращения для такого автомата связано со свойством синхронизируемости у ассоциированного с ним автомата без выхода.

На защиту выносятся: обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в заключении диссертации.

1. Координатизация и описание алгебраических и комбинаторных свойств линейных кодов на конечных абелевых группах и конечных модулях.

2. Обобщение понятия "бент-функции" для произвольной конечной абелевой группы и описание ее спектральных, алгебраических и комбинаторных свойств.
3. Развитие аппарата изучения и оценки "нелинейности" групповых функций на основе линейных разветвлений аффинных групповых функций.
4. Приведенная оценка Вейля для тригонометрических сумм аддитивных характеров конечных полей.
5. Описание некоторых семейств пустых секций кластеризации булевых функций на гиперсфере в евклидовом пространстве.
6. Новые свойства обобщенной глобальной лавинной характеристики для пар булевых функций.
7. Свойство (H, u) -стабильности булевых функций и наследование комбинаторных и спектральных свойств при сужении булевых функций. Новая характеристика семейства корреляционно-иммунных функций.
8. Исследование свойств класса невырожденных булевых функций. Произвольная булева функция RM -эквивалентна некоторой невырожденной булевой форме той же алгебраической степени.
9. Развитие аппарата исследований булевой функции на основе семейства ее локальных аффинностей. Новая аффинная нормальная форма булевой функции и ее свойства.
10. Теоретико-автоматная модель для задач обращения дискретных функций. Частично обратный автомат и асимптотическое поведение его характеристик при обращении БПИ-автоматов.
11. Локальное обращение БПИ-автоматов. Связь локальной обратимости БПИ-автомата с синхронизируемостью ассоциированного с ним автомата без выхода. Новые классы регистров сдвига с фильтрующими булевыми функциями, обладающие свойством локальной обратимости. Но-

вая теоретико-информационная характеристика семейства совершенно-уравновешенных функций.

12. Математическая модель "нелинейной" аппроксимации булевых функций на основе биортогональных базисов.

Публикации и апробация работы.

Результаты работы изложены в 17 публикациях в журналах:

- Доклады РАН,
- Проблемы передачи информации,
- Дискретная математика,
- Информатика и ее применения,
- Дискретный анализ и исследование операций (г. Новосибирск),
- Прикладная дискретная математика (г. Томск),
- Электроника ИНФО (республика Беларусь);

докладывалась на конференциях и семинарах различного уровня, в том числе:

- в МГУ имени М.В. Ломоносова на конференции с международным участием "Математика и безопасность информационных технологий" (МАБИТ-2003, 2006, 2008),
- в МГУ имени М.В. Ломоносова на 9 Международном семинаре "Дискретная математика и ее приложения" (Мех.-мат. факультет, 2007),
- на международной конференции "Boolean Functions in Cryptology and Information Security" (Звенигород, 2007),
- на международном семинаре "Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes" (Veliko Tarnovo, 2008),
- на научных семинарах факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова (руководители семинаров Моисеев Е.И., Соколов И.А., Алексеев В.Б.), механико-математического факультета МГУ имени М.В. Ломоносова (руководитель семинара Лупанов О.Б.), Института проблем передачи информации РАН (руководитель семинара Бассалыго Л.А.), ИПИБ МГУ имени М.В. Ломоносова.

Структура и объем работы

Диссертация состоит из введения, трех глав, заключения, списка литературы из 181 наименования и пяти приложений. Работа изложена на 297 страницах.

Содержание работы

Во введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В первой главе развивается математический аппарат анализа алгебраических, комбинаторных и криптографических свойств и параметров групповых функций. На основе дифференциально-разностного подхода для семейств групповых функций строятся и исследуются математические модели, в алгебраическом смысле обобщающие известные коды Риды-Маллера, а также максимально-нелинейные (бент) функции. Результаты исследований в этом направлении представлены в работах [Амб 94], [ЛСЯ 97], [ЛЯ 98], [ЛСЯ 98], сформировавших новое направление в изучении свойств дискретных функций. В последнее десятилетие эти исследования были продолжены. Их результаты можно найти, например, в [Сол 02], [Чер 10], [Чер 13], [Чер 14], [Сол 16] и др.

Для конечной абелевой группы G и группы вращений окружности T рассматривается множество групповых функций T^G . Относительно аффинной группы преобразований

$$\text{Aff}(G) = \{\sigma \in S_G : x^\sigma = e^\sigma x^\varphi, \varphi \in \text{Aut}(G)\}$$

(S_G — симметрическая группа всех перестановок элементов группы G , e — единица группы G) все множество T^G разбивается на орбиты (называемые аффинными классами). Рассмотрен параметр, характеризующий корреляционные связи произвольной функции $f \in T^G$ и некоторого аффинного класса $K \subseteq T^G$. Обозначим через $B(f, K)$ множество различных значений (f, g) , $g \in K$ с ука-

занием, сколько раз это значение встречается, когда g пробегает K . Показано (теорема 2.1), что мультимножество $B(f, k)$ является аффинным инвариантом для любого аффинного класса K .

Относительно покомпонентного умножения функций T^G является бесконечной абелевой группой, а T_q^G — конечной абелевой группой (T_q^G — группа корней степени q из единицы). Для дифференциального оператора $\frac{d}{du} : T^G \rightarrow T^G$, $u \in G$, задаваемого соотношением

$$\frac{df}{du}(x) = \bar{f}(x)f(ux),$$

рассматриваются множества для $f \in T^G$ вида

$$L_f = \left\{ u \in G : \frac{df}{du}(x) \equiv \text{const} \right\},$$

являющиеся подгруппами (лемма 2.2) группы G . Подгруппа L_f характеризует скрытую "линейность" (по аналогии с булевым случаем [ЛССЯ 15]) функции f . Группу L_f назовем группой гомоморфных трансляторов.

Пусть группа G представлена в виде прямого произведения $G = U \times V$ подгрупп. Функция $f \in T^G$ разложима по подгруппе U с выделением характера (или что от функции отщепляется характер группы U), если для всех $u \in U, v \in V$ выполнено равенство

$$f(u, v) = \chi(u)g(u)$$

с некоторыми $\chi \in \hat{U}$ ($\chi \in \hat{U}$ — группа характеров группы U) и $g \in T^V$. Показано (теорема 2.3), что при наличии представления $G = U \times V$ от функции $f \in T^G$ отщепляется характер группы U в том и только том случае, когда U — подгруппа L_f .

Одним из следствий теоремы 2.3 является необходимый признак нетривиальности группы L_f — наличие некоторого количества нулей среди коэффи-

циентов Фурье функции f (лемма 2.4). Это связано с тем, что преобразование Фурье любого характера имеет только одно ненулевое значение.

Для аффинно эквивалентных функций f и f^π , где $x^\pi = e^\pi x^\varphi, \varphi \in \text{Aut}(G)$, для любых $x \in G$, показано (теорема 2.5), что $L_{f^\pi} = (L_f)^\varphi$.

При использовании аппарата производных и работе со скалярным произведением функций из T^G полезно следующее соотношение (лемма 2.6)

$$\sum_{u \in G} \left(\frac{df_1}{du}, \frac{df_2}{du} \right) = |(f_1, f_2)|^2$$

для любых $f_1, f_2 \in T^G$.

Для конечной абелевой группы G порядка n и экспоненты q совместно с циклической группой T_q вводится математическая модель для группы (относительно покомпонентного умножения функций) T_q^G , обобщающая коды Рида-Маллера. Используя дифференциально-разностный подход, положим

$$\begin{aligned} \text{RM}_{-1}(G) &= \{f \in T_q^G : f(x) \equiv 1\}, \\ \text{RM}_0(G) &= \{f \in T_q^G : f(x) \equiv \text{const}\}, \\ \text{RM}_1(G) &= \{f \in T_q^G : \exists u, v \in G, f(x) = \chi_u(vx)\}, \end{aligned}$$

Далее для $r = 2, 3, \dots$ по определению положим

$$\text{RM}_r(G) = \left\{ f \in T_q^G : \frac{df}{du} \in \text{RM}_{r-1}(G), \forall u \in G \right\}.$$

Семейство $\{\text{RM}_r(G), r = -1, 0, 1, \dots\}$ — будем называть семейством кодом типа Рида-Маллера на группе G . В силу конечности T_q^G , начиная с некоторого N , будут выполнены равенства

$$\text{RM}_{r+1}(G) = \text{RM}_r(G), r = N, N+1, \dots$$

При этом для некоторых групп (в зависимости от их строения) может оказаться, что $\text{RM}_N(G) = T_q^G$, а для некоторых групп в множестве T_q^G содержатся функции, не принадлежащие ни одному коду типа Рида-Маллера.

Код $\text{RM}_1(G)$ является прямым аналогом множества аффинных булевых функций, составляющих "классический" код Рида-Маллера первого порядка. Код $\text{RM}_1(G)$ составляют функции из T_q^G , соответствующие характерам группы G и их сдвигам. Функции из $\text{RM}_1(G)$ естественно назвать аффинными функциями на G : $f \in \text{RM}_1(G)$ тогда и только тогда, когда $f(x) = f(e)\chi_u(x)$ для некоторого $u \in G$ при всех $x \in G$. Очевидно, что $\#\text{RM}_1(G) = qn$.

Аналогию с классическим вариантом кода продолжает утверждение о строении группы автоморфизмов кода $\text{RM}_1(G)$. Показано (теорема 3.1), что $\text{Aut}(\text{RM}_1(G)) = \text{Aff}(G)$. Доказана также максимальность группы линейных трансляторов для функций из $\text{RM}_1(G)$ (теорема 3.2):

$$\text{RM}_1(G) = \{f \in T_q^G : L_f = G\},$$

что является дополнительной характеристикой кода $\text{RM}_1(G)$.

Для изучения свойств семейства кодов Рида-Маллера на группе G полезно рассмотреть следующую алгебраическую конструкцию.

Множество функций $\Phi \subseteq T_q^G$ назовем A_0 -группой, если выполнены следующие свойства:

1. Φ является подгруппой группы T_q^G ;
2. Φ замкнуто относительно действия аффинной группы преобразований, т.е. если $f \in \Phi$, то $f^\pi \in \Phi$ для всех $\pi \in \text{Aff}(G)$;
3. Φ замкнуто относительно "сужений" или, другими словами, "фиксации части переменных".

Подфункции, получаемые из f при "фиксации части переменных" в случае, если группа G представима в виде прямого произведения $G = U \times V$, суть $f_u^{u_0}(u, v) = f(u_0, v)$, $f_v^{v_0}(u, v) = f(u, v_0)$, $u_0 \in U, v_0 \in V$.

Примерами A_0 -групп являются $RM_{-1}(G)$, $RM_0(G)$, $RM_1(G)$.

Определим оператор J , действующий на множествах $\Phi \subseteq T_q^G$:

$$J\Phi = \left\{ f \in T_q^G : \frac{df}{du} \in \Phi, \forall u \in G \right\}.$$

Этот оператор описывает рекуррентный переход в определении кодов типа Рида-Маллера над группой G поскольку

$$RM_r(G) = JRM_{r-1}(G), \quad r = 0, 1, 2, \dots$$

Важным свойством этого оператора является то, что он переводит A_0 -группу в A_0 -группу (теорема 3.3). Непосредственным следствием из этого свойства является принадлежность всех кодов типа Рида-Маллера на группе G к семейству A_0 -групп из группы T_q^G . Теперь представить определение кода $RM_{r-1}(G)$ можно кратко в виде:

$$RM_{r-1}(G) = J^{r-1}RM_0(G) = J^rRM_{-1}(G)$$

или

$$RM_{r-1}(G) = \left\{ f \in T_q^G : \frac{d}{du^1} \frac{d}{du^2} \cdots \frac{d}{du^r} f \equiv 1, \forall u^1, \dots, u^r \in G \right\}.$$

Для исследования свойств кодов $RM_r(G)$ удобно использовать полугруппу операторов на T_q^G , порожденную операторами дифференцирования. При этом бывает полезна следующая более общая алгебраическая конструкция.

Для группового кольца $\mathbb{Z}_q G$ определим действие на T_q^G : если $a = \sum_{u \in G} \lambda_u u \in \mathbb{Z}_q G$, то

$$(af)(x) = \prod_{u \in G} (f(ux))^{\lambda_u - 1}.$$

Оператор a является гомоморфизмом группы T_q^G , а умножению операторов соответствует умножение в кольце $\mathbb{Z}_q G$. Операторы сдвига и дифференцирования удовлетворяют соотношениям

$$uf(x) (u^{-1}f)(x),$$

$$\frac{d}{du}f(x) = ((u^{-1} - 1)f)(x),$$

где 1 — единица кольца $\mathbb{Z}_qG$ и $\bar{f}(x) = (f(x))^{-1}$ для любой функции $f \in T_q^G$. Используя этот подход, доказан критерий возможности представления функции $f \in T_q^G$ в виде производной некоторой функции $g \in T_q^G$ по направлению $u \in G$, $u^t = e$ (лемма 3.8), состоящий в выполнении для f соотношения

$$\prod_{i=0}^{t-1} f(u^i x) \equiv 1,$$

при всех $x \in G$.

Используя операции в групповом кольце $\mathbb{Z}_qG$, мы можем теперь записать определение кода $RM_{r-1}(G)$ в виде

$$RM_{r-1}(G) = \left\{ f \in T_q^G : \prod_{i=1}^r \left((u^i)^{-1} - 1 \right) f \equiv 1, \forall u^1, \dots, u^r \in G \right\},$$

где

$$G(u^1, \dots, u^r) = \prod_{i=1}^r \left((u^i)^{-1} - 1 \right) = \sum_{u \in G} \lambda_u u -$$

элемент группового кольца $\mathbb{Z}_qG$.

Выполнение равенства

$$RM_N(G) = T_q^G$$

эквивалентно существованию такого натурального N , что в кольце $\mathbb{Z}_qG$ выполнено тождество

$$G(u^1, \dots, u^N) = 0$$

для всех $u^1, \dots, u^N \in G$. В силу коммутативности кольца $\mathbb{Z}_q G$ такое N существует тогда и только тогда, когда каждый элемент вида $u - 1$, $u \in G$ является нильпотентным элементом кольца $\mathbb{Z}_q G$. Показано (лемма 3.8), что любой элемент $u - 1$, $u \in G$ является нильпотентным элементом кольца $\mathbb{Z}_q G$ в том и только том случае, когда q имеет вид p^s , p — простое, s — натуральное. Отсюда вытекает (следствие 3.9), что любая функция из T_q^G принадлежит некоторому коду типа Рида-Маллера на группе G в том и только том случае, когда q имеет вид p^s , p — простое, s — натуральное.

Для оператора дифференцирования $\frac{d}{du}$ найдены (3.10) необходимые и достаточные условия существования нетривиального решения в T_q^G дифференциального уравнения $\frac{df}{du}(x) = f(x)$.

Пространство гомоморфных трансляторов определено для произвольной A_0 -группы. Показано (лемма 3.12, теорема 3.13) существование для A_0 -групп свойств, аналогичных свойствам кода $RM_1(G)$.

Использование теоретико-кодовых моделей в ходе решения задач обеспечения информационной безопасности приводит к необходимости вычисления ряда параметров линейных кодов. При этом весьма плодотворной оказалась концепция пары взаимно дуальных кодов и тождеств Мак-Вильямс, связывающих характеристики таких кодов (см. [MWS 77]). Естественное развитие классические результаты получили в направлении распространения их на разнообразные алгебраические системы. Для групповых кодов — подгрупп конечных абелевых групп — эта концепция при достаточно общих предположениях рассмотрена в работе [ЗиЭр 96]. Для линейных кодов, построенных с помощью идеалов коммутативных колец и подмодулей квазифробениусовых модулей, эта концепция рассмотрена в [Неч 95].

В диссертации рассматриваются свойства дуальности для конечных модулей и приложения этих свойств к теории кодирования. Идея "координатизации" в данном случае проявляется в стремлении добиться того, чтобы модули обладали теми же свойствами, что и векторные пространства, т.е. наилучшими

возможными свойствами дуальности. На языке теории решеток указанные наилучшие возможные свойства дуальности — это дуальный изоморфизм (в другой терминологии — антиизоморфизм) решеток двух сопряженных подпространств.

Для произвольного бинарного билинейного отношения между элементами двух конечных U и V (над конечным коммутативным кольцом) рассмотрено понятие дуальности для их подмодулей

$$A \subseteq U \longrightarrow A^* \in V,$$

$$B \subseteq V \longrightarrow B^+ \in U,$$

обладающие рядом свойств, позволяющих перенести это понятие на функции, называемые ρ -структурами кодов из $U(V)$. По существу, ρ -структуры представляют собой максимально общую модель метрических и комбинаторных характеристик кодов из $U(V)$.

В теореме 4.5 получены тождества, связывающие дуальные ρ -структуры для дуальных кодов. В следствии 4.6 полученные общие соотношения интерпретируются для классического вида ρ -структур — весовых характеристик двоичных линейных кодов (тождество Мак-Вильямс).

Для функций из T^G рассмотрено понятие "уравновешенности", обобщающее "классическое" понятие уравновешенности, основанное на частотах появления значений дискретной функции. Функции из множества

$$UF(G) = \left\{ f \in T^G : \hat{f}(e) = \sum_{x \in G} f(x) = 0 \right\}$$

назовем уравновешенными. Ясно, что если для некоторой f из T^G выполнено условие $\hat{f}(a) = 0, a \in G$, то $\bar{\chi}_a(x)f(x) \in UF(G)$. Для функций из $UF(G) \cap T_q^G$ понятие уравновешенности совпадает с классическим.

Функцию $f \in T^G$, для которой при всех $a \in G$ выполнено

$$\left| \widehat{f}(a) \right|^2 = n,$$

будем называть бент-функцией. Множество всех бент-функций на группе G обозначим $BF(G)$.

Множества $UF(G)$ и $BF(G)$ замкнуты относительно действия группы $\text{Aff}(G)$, то есть состоят из некоторого числа аффинных классов.

При этом уместны аналогии с булевым случаем. Функции из $RM_0(G)$ — это константы, функции из $RM_1(G)$ — это аффинные функции, так как они получаются из характеров (линейных функций) умножением на константу. Функции из $RM_2(G)$ — это квадратичные функции на G , так как любая их производная — аффинная функция.

Для бент-функций из $BF(G)$ имеет место (теорема 5.3) аналог критерия Ротхауза для булева случая. Функция $f \in T^G$ лежит в $BF(G)$ тогда и только тогда, когда $df/du \in UF(G)$ для любого $u \in G \setminus e$.

Необходимо отметить, что аналогичный критерий для элементарной абелевой p -группы получен в [Амб 94].

Еще один вид характеристики бент-функций на группе G можно получить, рассмотрев для функций из T^G следующую числовую характеристику:

$$\delta^2 f = \sum_{u \neq e} \left| \widehat{\frac{df}{du}}(e) \right|^2.$$

Эта характеристика является аффинным инвариантом для группы G . Показано (следствие 5.4), что

$$BF(G) = \{ f \in T^G : \delta^2 f = 0 \}.$$

Таким образом, аффинный инвариант $\delta^2 f$ можно рассматривать как меру удаления функций из T^G от множества $BF(G)$.

Бент-функция на группе G обладает также одним интересным свойством. Функция $f \in T^G$ является бент-функцией (теорема 5.6) тогда и только тогда, когда система из $n = \#G$ функций

$$f'(x) = \frac{df}{du}(x), u \in G$$

образует ортогональный базис в $\mathbb{C}^G$.

Рассмотрено понятие бент-базиса $\mathbb{C}^G$ и установлено взаимно однозначное соответствие (теорема 5.8) между множеством таких бент-базисов $BB(G)$ и множеством нормированных бент-функций $BNF(G)$.

По аналогии с булевым случаем определим для функции $f \in T^G$ "критерий распространения" как

$$PC(f) = \{u \in G : df/du \in UF(G)\}.$$

Для $f \in T^G$ и $Q < G$ найдены (теорема 5.10) необходимые и достаточные условия того, что $Q \setminus e \subseteq PC(f)$.

Понятие дуальной функции к бент-функции f определяется соотношением $\sqrt{n}\tilde{f}(u) = \hat{f}(u)$, $u \in G$. Показано (теорема 5.13), что дуальная функция является бент-функцией на G .

Для конкретных областей обеспечения информационной безопасности в качестве математических моделей, как правило, рассматривают специфические семейства групповых функций. В частности для теории кодирования и криптографии важную роль играет семейство групповых комплекснозначных функций, являющихся композицией некоторого аддитивного характера χ конечного поля $\mathbb{F}_q$ ($q = p^l$, p — простое) и полинома P с коэффициентами из этого же поля.

Важнейшие комбинаторные и криптографические свойства функций $f(x) = \chi(P(x))$ выражаются с помощью величины

$$W(\chi, P) = \sum_{x \in \mathbb{F}_q} \chi(P(x)),$$

называемой суммой Вейля (частный вид так называемых тригонометрических сумм). Задача точного вычисления этих сумм для многочленов общего положения чрезвычайно сложна. Поэтому ограничиваются оценкой модуля $W(\chi, P)$ или вычисления $W(\chi, P)$ для некоторых классов полиномов. Нетривиальной является оценка Вейля

$$|W(\chi, P)| \leq (n-1)q^{1/2},$$

доказанная в предположениях, что $P \in \mathbb{F}_q[x]$ — полином степени $n \geq 1$, $(n, q) = 1$ и χ — нетривиальный аддитивный характер. Легко видеть, что оценка Вейля зависит только от мощности поля q и степени полинома $\deg(P) = n$. Естественнo ожидать, что при уточнении оценки Вейля в нее могут вводиться новые параметры.

Поскольку нас интересуют суммы Вейля, то можно определить на $\mathbb{F}_q[x]$ эквивалентности, задаваемые суммами Вейля, и сократить число рассматриваемых полиномов. Простейшей такой эквивалентностью является совпадение полиномов как отображений $\mathbb{F}_q$ в себя. Кроме того, алгебраические степени полиномов могут не превышать $q-1$. Легко показать, что для исследования эквивалентностей полиномов относительно сумм Вейля можно ограничиться множеством полиномов $\mathcal{K}$ из $\mathbb{F}_q[x]$ степени не выше $q-2$ с нулевым свободным членом. Для полиномов из $\mathcal{K}$ вводится эквивалентность по следу, задаваемая соотношением

$$\text{tr}(P_1(x)) = \text{tr}(P_2(x)),$$

где $P_1(x), P_2(x) \in \mathbb{F}_q[x]$.

Вспомогательные результаты (теорема 6.2, следствие 6.3) описывают некоторые алгебраические свойства этого отношения эквивалентности. Центральным сущностным элементом этой конструкции является понятие циклотомически приведенного полинома (*cr*-полинома), представляющего собой сумму мономов (с коэффициентами из соответствующих подполей поля $\mathbb{F}_q$), степени которых являются минимальными представителями циклотомических классов по модулю $p^l - 1$. В теореме 6.5 доказано, что каждый полином из $\mathcal{K}$ эквивалентен по следу некоторому *cr*-полиному. В соответствии с теоремой 6.5 для любого полиному $P(x) \in \mathcal{K}$ выполнено неравенство

$$\text{Deg}(P) \leq \deg(P),$$

где $\text{Deg}(P)$ — алгебраическая степень *cr*-полинома, эквивалентного по следу данному полиному $P(x)$, $(\text{Deg}(P), p) = 1$. Спектр значений $\text{Deg}(P)$ для полиномов $P(x) \in \mathcal{K}$ меньше, чем спектр значений $\deg(P)$. В частности, число различных значений, которые может принимать $\text{Deg}(P)$, совпадает с числом циклотомических классов. Последовательное применение теоремы 6.5 и оценки Вейля позволяет улучшить оценку Вейля. В теореме 6.6 (приведенная оценка Вейля) доказано, что любого полинома $P(x)$ из $\mathcal{K}$ и нетривиального аддитивного характера χ поля $\mathbb{F}_q$ выполнены следующие неравенства:

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| \leq (\text{Deg}(P) - 1) q^{1/2},$$

если $\text{Deg}(P) \neq 0$, и

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| = q,$$

если $\text{Deg}(P) = 0$. При этом оценка Вейля улучшается в трех направлениях:

- (1) расширяется область применения оценки, так как нет требования взаимной простоты $\deg(P)$ и p ;

- (2) расширяется область, в которой оценка эффективнее тривиальной, так как очевидно, что в ряде случаев одновременно выполняются оба неравенства $\deg(P) \geq q^{1/2}$ и $\text{Deg}(P) \leq q^{1/2}$;
- (3) как правило, $\text{Deg}(P) < \deg(P)$, поэтому приведенная оценка точнее; более того, как показывают примеры, отношение $\deg(P) / \text{Deg}(P)$ может иметь порядок даже q^ϵ .

Для дифференциально-разностных методов (см. [MeOV 96], [Шна 03], [ЛССЯ 15]) обращения дискретных функций, обычно рассматриваемых на элементарных абелевых 2-группах, предложен общий подход для групповых функций, определенных на произвольных конечных абелевых группах G и H . Для множества функций H^G исследуются их свойства (метрические), определяющие их положения относительно "линейных" функций $\text{Hom}(G, H) \subset H^G$. Для групповой функции f из H^G рассмотрены $\deg(f)$, $\mu l(f)$, $\text{ih}(f)$, характеризующие "нелинейность" данного отображения и эффективность соответствующего метода обращения. Получены соотношения (лемма 7.5, теорема 7.6, теорема 7.7, следствие 7.8), связывающие эти параметры.

На основе дифференциально-разностного подхода для произвольной булевой функции рассмотрены понятия невырожденной функции и структуры вырождения функции. Необходимо отметить, что введенное понятие невырожденности в случае квадратичной функции совпадает с классическим свойством невырожденности (т.е. совпадает с максимальной нелинейностью). Показано, что любая булева функция RM -эквивалентна некоторой невырожденной форме (теорема 8.6, следствие 8.8). В лемме 8.9 получены алгебраические соотношения, позволяющие реализовать приведение булевой функции к невырожденной нормальной форме.

В работе [ЛФЯ 18,2] введено понятие Δ -эквивалентности булевых функций, исходя из того, какую функцию автокорреляции они имеют. Весьма полезным свойством данного отношения эквивалентности оказывается то, что внутри каждого класса Δ -эквивалентности остаются неизменными многие характери-

стики булевых функций, имеющие важное значение в криптографии и теории кодирования.

Среди таких характеристик, например, нелинейность булевой функции, максимальный порядок корреляционной иммунности, глобальные лавинные характеристики. В заключение главы 1 в теореме 10.6 рассмотрены связи глобальных лавинных характеристик булевых функций (σ_f, σ_g) с их обобщенной глобальной лавинной характеристикой $(\sigma_{f,g})$, а в теореме 10.7 доказывается неизменность обобщенной глобальной лавинной характеристики для любой пары булевых функций, взятых из двух фиксированных классов Δ -эквивалентности.

Как правило, классификации семейств булевых функций строятся на основе отношений эквивалентности, задаваемых некоторыми группами преобразований пространств Хэмминга. Однако, в ряде разделов математики (комбинаторная геометрия, теория игр, теория кодирования и др.) исследуются группирования изучаемых объектов в качестве точек тех или иных метрических пространств. Одним из "геометрических мест точек", возникающих в подобных исследованиях, является гиперсфера в многомерном евклидовом пространстве. Например, в теории кодирования (см. [Сид 08]) изучаются изометрические вложения некоторых классов кодов на сферу в евклидовом или унитарном пространствах. Такие исследования позволяют по-новому взглянуть на классические математические объекты и расширить используемый аппарат.

В работе [ЛФЯ 18,1] предложен новый подход (кластеризация) к изучению некоторых метрических характеристик булевых функций, основанный на "переносе" пространства булевых функций $\mathcal{F}_n$ от n переменных на $(2^n - 1)$ -мерную сферу в 2^n -мерном евклидовом пространстве с помощью преобразования Фурье (Адамара). Один из основных вопросов в исследовании свойств данной кластеризации — это описание пустых секций (т.е. пересечений ортантов со сферой). В теореме 9.1 доказано, что секции, соответствующие булевым функциям, обладающим линейными трансляторами, пусты. Для произвольной квадратичной функции доказан критерий (лемма 9.2) пустоты, соответствующей ей секции.

Во второй главе рассмотрены вопросы характеристики булевых функций с помощью семейств их подфункций.

С целью изучения наследования комбинаторных и спектральных свойств булевых функций их подфункциями введено понятие (H, u) -стабильности $(H \subset \mathbb{F}_2^n, u \in \mathbb{F}_2^n)$ булевой функции. Доказан критерий (H, u) -стабильности функции (теорема 12.8). На основе этого критерия предложен алгоритм построения для функции f семейства $\mathcal{H}_{f,u}$ подпространств из $\mathbb{F}_2^n$, для которых f является (H, u) -стабильной. Использование понятия (H, u) -стабильности позволяет получить (теорема 12.15) новую характеристику (критерий) свойства корреляционной иммунности (наряду с имеющимися уже теоретико-информационной, весовой и спектральной характеристиками).

В исследованиях различных аспектов задач обращения булевых отображений важную роль играют их аффинные сужения, то есть сужения, совпадающие с аффинными функциями. Их значимость определяется возможностью сведения исходной нелинейной задачи обращения к некоторой линейной задаче. Соответствующие области сужения обычно называют локальными аффинностями булевых отображений.

Вообще говоря, область сужения может быть выбрана произвольным образом. Однако, с точки зрения изучения алгебраических, комбинаторных, метрических и криптографических свойств булевых функций и отображений целесообразно выбирать области сужения, имеющие достаточно простое (эффективное) описание. Наиболее удобными вариантами являются подмножества пространства Хэмминга, описываемые системами линейных уравнений, то есть смежные классы по подпространствам пространства Хэмминга. Для краткости их обычно называют плоскостями. Рассмотрены некоторые общие свойства (предложения 13.3, 13.6, 13.8) семейств локальных аффинностей.

Простейшие описания локальных аффинностей булевой функции могут быть получены с помощью фиксации константами некоторых переменных. Эти семейства локальных аффинностей играют важную роль в комбинаторных ал-

горитмах обращения дискретных функций, содержащих этапы перебора части описывающих функцию параметров.

Для булевой функции $f \in \mathcal{F}_n$ важной величиной, характеризующей семейство ее локальных аффинностей, получаемых фиксацией переменных, является уровень аффинности $la(f)$ — минимальное число переменных k , $0 \leq k \leq n - 1$, фиксация которых переводит функцию f в $\mathcal{A}_{n-k}$. Обобщенным уровнем аффинности $\mathcal{L}a(f)$ называют минимальную возможную коразмерность локальных аффинностей функции f . Подробному изучению свойств этих параметров посвящено значительное количество работ. Например, в [БуЛо 05,1], [Бур 08], [Лог 08], [Лог 10] рассмотрены связи этих параметров с различными криптографическими свойствами булевых функций. В частности, в [БуЛо 05,1] полностью описан класс булевых функций, обладающих максимальным возможным значением уровня аффинности. В [Бур 08], [Лог 08] получены нижние оценки уровня аффинности (обобщенного уровня аффинности) для почти всех булевых функций при стремлении к ∞ числа переменных. В работе [Лог 10] для $la(f)$ и $\mathcal{L}a(f)$ получены верхние оценки для почти всех булевых функций при стремлении к ∞ числа переменных. Результаты [Бур 08] и [Лог 10] позволяют доказать (теорема 14.10), что асимптотически при $n \rightarrow \infty$ для почти всех булевых функций f из $\mathcal{F}_n$ выполнены неравенства

$$\begin{aligned} n - \lfloor \log_2 n \rfloor &\leq la(f) \leq n - \lceil \log_2 n \rceil + 1, \\ n - \lfloor \log_2 n \rfloor &\leq \mathcal{L}a(f) \leq n - \lceil \log_2 n \rceil + 1. \end{aligned}$$

Эти неравенства выделяют два возможных случая $n = 2^b$ и $n \neq 2^b$ (b — натуральное число). В случае, когда $n = 2^b$, для почти всех булевых функций имеется два возможных значения уровня (обобщенного уровня) аффинности: $n - b$, $n - b + 1$. А в случае, если n не является степенью 2, для почти всех функций из $\mathcal{F}_n$ имеется одно возможное значение для уровня (обобщенного уровня)

аффинности:

$$n - \lfloor \log_2 n \rfloor = n - \lceil \log_2 n \rceil + 1.$$

Различные нормальные формы булевых функций (дизъюнктивная нормальная форма - ДНФ, конъюнктивная нормальная форма - КНФ, алгебраическая нормальная форма - АНФ, числовая нормальная форма - ЧНФ и т.п.) использовались и используются в исследованиях разнообразных свойств булевых функций и отображений. Предпочтение той или иной нормальной форме отдается в зависимости от вида используемой в исследовании математической модели (математического аппарата) и характера решаемой в ходе исследования задачи. Каждая из нормальных форм имеет свои особенности. Например, представление булевой функции с помощью ДНФ или КНФ не является однозначным, а представление с помощью АНФ (в соответствующем фактор-кольце) является однозначным.

В исследованиях, связанных с анализом информационной безопасности, активнее других используется АНФ. Ранее (в параграфе 6) была введена новая невырожденная нормальная форма (ННФ) булевых функций.

Аффинная нормальная форма (АффНФ) булевой функции из $\mathcal{F}_n$ определяется относительно разбиения пространства Хэмминга $\mathbb{F}_2^n$ на локальные аффинности этой функции. АффНФ булевой функции является алгебраической суммой произведений сужений функции на индикаторные функции локальных аффинностей разбиения. Аналогично определяется АффНФ для булевых отображений. Необходимо отметить также, что представление булевой функции в виде АффНФ не является однозначным. Данная форма существенно зависит от используемого разбиения пространства Хэмминга на локальные аффинности.

Структура и параметры АффНФ булевой функции могут быть использованы для вычисления преобразования Фурье этой функции. В теореме 15.6 получен общий вид коэффициента Фурье булевой функции, зависящий от параметров ее АффНФ. Данный вид нормальной формы позволяет описывать неко-

торые классы криптографических функций. В частности, на основе так называемых центрально дуальных разбиений на локальные аффинности (теорема 15.9) с помощью АффНФ описан подкласс бент-функций, для которых в явном виде получены выражения для АффНФ соответствующих им дуальных бент-функций.

Аффинная нормальная форма может быть использована при разработке алгоритмов решения задач обращения дискретных функций.

Мощности (размерности) локальных аффинностей конкретных булевых функций существенно зависят от особенностей функциональных классов, к которым они принадлежат. Например, для платовидных функций (в этот класс входят и бент-функции) имеется ограничение сверху на размерность локальной аффинности, определяемое порядком ее платовидности. В теореме 15.12 показано, что размерность локальной аффинности любой платовидной функции порядка $2r$, $0 \leq r \leq n$ не превосходит $n - r$.

В заключение главы 2 рассмотрены возможности "нелинейной" аппроксимации булевых функций на основе понятий биортогонального базиса $\{e_u(x)\}_{u \in \mathbb{F}_2^n}$ и обобщенного кода Адамара $H(e_u(x))$. В работе [ЛСЯ 04,3] было показано, что возможности "нелинейной" аппроксимации не меньше, чем у "линейной". Для конкретного "нелинейного" базиса, являющегося комбинацией линейных и бент-функций, получено выражение (теорема 16.4) для радиуса покрытия обобщенного кода Адамара, порожденного указанным выше базисом. Интересно то, что этот параметр совпал с радиусом покрытия кода Риды-Маллера первого порядка той же длины. В лемме 16.5 получено соотношение между коэффициентами Уолша-Адамара булевой функции и коэффициентами базисного разложения этой функции относительно указанного выше комбинированного "нелинейного" базиса. Это соотношение будет полезно для выяснения преимуществ той или иной аппроксимации,

В главе 3 рассмотрены некоторые теоретико-автоматные модели обращения дискретных функций.

Среди различных возможных постановок задачи обращения дискретной функции (см. параграфы 17, 18) имеется вариант, использующий теоретико-автоматную математическую модель. В условиях этой математической модели "обращение" может быть определено как нахождение по известной выходной последовательности конечного автомата однозначно восстанавливаемых фрагментов соответствующей неизвестной входной последовательности этого автомата. При этом начальное состояние также считаем неизвестным. Имеющиеся результаты показывают, что в худшем случае число пар (начальное состояние, входная последовательность), задающих данную выходную последовательность, может быть достаточно большим. Однако, даже в этом случае одинаковые фрагменты этих входных последовательностей могут существенно уменьшить трудоемкости методов анализа средств обеспечения информационной безопасности.

Описание процесса восстановления этих фрагментов может быть осуществлено также с помощью конечного автомата.

Для конечного автомата Мили

$$\mathcal{M} = (A, Q, B, \varphi, \psi)$$

определяется ассоциированный с ним инициальный ЧО-автомат

$$\mathcal{M}^{-1} = (B, S, A', \zeta, \eta, s_0),$$

где $A' = A \cup \{*\}$ ($*$ — выходной символ, вырабатываемый автоматом $\mathcal{M}^{-1}$, если соответствующий входной символ автомата $\mathcal{M}$ определяется неоднозначно, $S = 2^Q$, $s_0 = Q$. Функции переходов и выходов автомата $\mathcal{M}^{-1}$ (ζ и η) однозначно определяются функциями φ и ψ .

Возможности однозначного восстановления с помощью ЧО-автомата $\mathcal{M}^{-1}$ входных символов автомата $\mathcal{M}$ существенным образом зависят от строения и особенностей его графа $\Gamma_{\mathcal{M}^{-1}}$. Некоторые структурные свойства этого гра-

фа (сильная связность, синхронизируемость, минимальные мощности вершин и др.) описаны в теоремах 19.3 и 19.7, леммах 19.2 и 19.6, следствиях 19.4 и 19.5. Эти результаты существенно используются далее для расчета параметров обращения дискретной функции, реализуемой автоматом $\mathcal{M}$.

Величина (параметр) $d_{\mathcal{M}}$, равный минимальный мощности вершин в графе $\Gamma_{\mathcal{M}^{-1}}$, имеет важное значение для восстановления фрагментов входного слова автомата $\mathcal{M}$. В общем случае (для произвольного автомата Мили) поведение этой величины имеет достаточно сложный характер.

Для автомата без потери информации $\mathcal{M}$ получены интерпретации величины $d_{\mathcal{M}}$ через слипшиеся состояния автомата $\mathcal{M}$ (лемма 20.1) и через минимальный ранг некоторой полугруппы, ассоциированной с автоматом $\mathcal{M}$ (лемма 20.2).

Для характеристики процесса обращения конечного БПИ-автомата $\mathcal{M}$ использована теоретико-вероятностная модель конечных цепей Маркова. Показано (лемма 20.3), что при случайном и равновероятном выборе для автомата $\mathcal{M}$ пары (начальное состояние, входная последовательность) цепь Маркова $\mathcal{C}^{\mathcal{M}^{-1}}$, индуцируемая частично обратным автоматом $\mathcal{M}^{-1}$ на множестве 2^Q , является однородной, а множество S^0 ($S^0 \in 2^Q$) состояний минимальной мощности автомата $\mathcal{M}^{-1}$ является классом эргодических состояний.

Рассмотрена величина $\rho^{\mathcal{M}}$, описывающая асимптотическое поведение математического ожидания $\rho_l^{\mathcal{M}}$ случайной величины, равной доле символов входного слова длины l БПИ-автомата $\mathcal{M}$, однозначно восстанавливаемых автоматом $\mathcal{M}^{-1}$. В условиях леммы 20.3 получены значения $\rho^{\mathcal{M}}$ для случаев $d_{\mathcal{M}} = 1$ и $d_{\mathcal{M}} = \#Q$. Показано также (теорема 20.6), что для любого подавтомата $\mathcal{M}'$ БПИ-автомата $\mathcal{M}$ выполнено неравенство $\rho^{\mathcal{M}'} \geq \rho^{\mathcal{M}}$.

Для БПИ-автоматов рассмотрен также вариант частичного обращения, для которого позиция (локализация) однозначно восстанавливаемого фрагмента в прообразе точно определяется появлением в соответствующем выходном

слове специальных подслов-индикаторов. Этот вариант частичного обращения в работе [Лог 07] был назван локальным обращением.

Для конечного БПИ-автомата Мили $\mathcal{M}$ вводится понятие ассоциированного с ним автомата без выхода $\mathcal{B}(\mathcal{M})$ (определение 21.8). Доказано (теорема 21.10), что приведенный конечный БПИ-автомат Мили $\mathcal{M}$ обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат $\mathcal{B}(\mathcal{M})$ — синхронизируем. Это утверждение показывает глубокую сущностную связь свойства локальной обратимости БПИ-автоматов со свойством синхронизируемости ассоциированных с ними автоматов без выхода и обосновывает принципиальную возможность построения эффективных методов обращения автоматов этого класса.

Аналогичное утверждение доказано для класса двоичных векторных автоматов (регистров сдвига) с фильтрующими булевыми функциями (теорема 22.6). Содержательный смысл этого утверждения обусловлен отличием параметров локального обращения для этого класса автоматов от параметров, определяемых теоремой 21.10.

Ранее в работе [ЛоСм 13] были описаны семейства фильтрующих булевых функций, для которых соответствующие регистры сдвига обладают свойством локальной обратимости. В диссертации в классе монотонных булевых функций выделены новые семейства булевых функций, которые, будучи фильтрующими для регистров сдвига, определяют автоматы, обладающие свойством локального обращения (теоремы 22.16, 22.17).

Дискретные совершенно уравновешенные функции над конечным алфавитом A начали систематически исследоваться в работах [Hed 69], [Сум 94]. Наряду с другими результатами в этих работах получены критерии совершенно уравновешенных дискретных функций, связывающие совершенно уравновешенные функции с функциями дефекта нуль и с функциями без потери информации.

Почти очевидной является эквивалентность совершенной уравновешенности фильтрующей функции $f \in A^{A^n}$, $\#A = q$ и свойства автомата $SR(n, f)$

сохранять равномерное распределение входных последовательностей (предложение 25.1). В теореме 25.2 показано, что средняя на символ взаимная информация входного слова любой длины и соответствующего выходного слова автомата $RS(n, f)$, при условии равномерного распределения входного слова, равна $\log_2 q$ тогда и только тогда, когда f — совершенно уравновешенная булева функция. По существу, это еще одна теоретико-информационная характеристика класса совершенно уравновешенных функций.

Основные результаты опубликованы в следующих работах:

[ЛПЯ 95] Логачев О.А., Проскурин Г.В., Яценко В.В. Локальное обращение конечного автомата с помощью автоматов. // Дискр. математика, том 7, вып. 2, 1995, с. 19-33.

[ЛСЯ 97] Логачев О.А., Сальников А.А., Яценко В.В. Бент-функции на конечной абелевой группе. // Дискр. математика, том 9, вып. 4, 1997, с. 3-20.

[ЛЯ 98] Логачев О.А., Яценко В.В. Коды типа Риды-Маллера на конечной абелевой группе. // Проблемы передачи информации, том 34, вып. 2, 1998, с. 32-46.

[ЛСЯ 98] Логачев О.А., Сальников А.А., Яценко В.В. Спаривание конечных модулей, дуальность линейных кодов и тождества Мак-Вильямс. // Пробл. передачи информации, том 34, вып. 3, 1998, с. 50-59.

[ЛСЯ 99] Логачев О.А., Сальников А.А., Яценко В.В. О свойствах сумм Вейля на конечных полях и конечных абелевых группах. // Дискр. математика, том 11, вып. 2, 1999, с. 66-85.

[ЛСЯ 00,1] Логачев О.А., Сальников А.А., Яценко В.В. Невырожденная нормальная форма булевых функций. // Докл. РАН, том 373, № 2, 2000, с. 164-167.

[ЛСЯ 00,2] Логачев О.А., Сальников А.А., Яценко В.В. Об одном свойстве ассоциированных представлений группы $GL(n, k)$. // Дискретн. математика, том 12, вып. 2, 2000, с. 154-159.

[ЛСЯ 01] Логачев О.А., Сальников А.А., Ященко В.В. Некоторые характеристики "нелинейности" групповых отображений. // Дискр. анализ и иссл. операций, серия 1, том 8, №1, 2001, с. 40-54.

[ЛСЯ 02] Логачев О.А., Сальников А.А., Ященко В.В. О наследовании свойств при сужениях булевых функций. // Дискретн. математика, том 14, вып. 2, 2002, с. 9-19.

[ЛСЯ 04,1] Логачев О.А., Сальников А.А., Ященко В.В. Корреляционная иммунность и реальная секретность. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, с. 165-170.

[ЛСЯ 04,2] Логачев О.А., Сальников А.А., Ященко В.В. Комбинирующие k -аффинные функции. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, с. 176-178.

[ЛСЯ 04,3] Логачев О.А., Сальников А.А., Ященко В.В. Аппроксимация булевых функций элементами биортогонального базиса. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, С. 171-175.

[БуЛо 05,2] Буряков М.Л., Логачев О.А. Об уровне аффинности булевых функций. // Дискр. математика, том 17, вып.4, 2005, с. 98-107.

[Лог 07] Логачев О.А.. О локальной обратимости одного класса булевых отображений. // Материалы 9 Международного Семинара "Дискретная математика и ее приложения". Москва, 18-23 июня 2007 г. Изд. мех.-мат. факультета МГУ, Москва, 2007, с. 440-442.

[ЛоНа 07] Логачев О.А., Назарова Д.С. Локальное аффинное обращение. // Математика и безопасность информационных технологий. М.: МЦНМО, 2007, с. 227-248.

[LYD 08] O.A. Logachev, V.V. Yashchenko, and M.P. Denisenko. Local Affinity of Boolean Mappings. // Boolean Functions in Cryptology and Information Security. NATO Advanced Study Institute, Zvenigorod, Russia, 8-18 September, 2007. IOS Press, 2008, pp. 148-172.

[LSSY 09] O. A. Logachev, A.A. Salnikov, S.V. Smyshlyaev, and V.V. Yashchenko. Symbolic Dynamics, Codes, and Perfectly Balanced Functions. // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. NATO Advanced Research Workshop, Veliko Tarnovo, Bulgaria, 6-9 October, 2008. IOS Press, 2009, pp. 222-233.

[Лог 08] Логачев О.А. Нижняя граница уровня аффинности для почти всех булевых функций. // Дискр. математика, том 20, вып. 4, 2008, с. 85-88.

[Лог 10] Логачев О.А. О значениях уровня аффинности для почти всех булевых функций. // Прикл. дискр. математика, №3, 2010, с. 17-21.

[ЛоСм 13] Логачев О.А., Смышляев С.В. О неавтономных двоичных регистрах сдвига, обладающих свойством синхронизации. //Электроника инфо, №6, Минск, 2013, с. 183-185.

[Лог 17] Логачев О.А. Критерий совершенной уравновешенности сдвиг-композиции функций над конечным алфавитом. // Дискретн. математика, том 29, вып. 4, 2017, с. 59-65.

[Лог 18,1] Логачев О.А. О локальной обратимости конечных автоматов без потери информации. // Прикл. дискр. математика, №39, 2018, с. 78-93.

[Лог 18,2] Логачев О.А. Теоретико-информационная характеристика совершенно уравновешенных функций. // Информатика и ее применения, том 12, вып. 4, 2018, с. 70-74.

[ЛФЯ 18,1] Логачев О.А., Федоров С.Н., Яценко В.В. Булевы функции как точки на гиперсфере в евклидовом пространстве. // Дискр. математика, том 30, вып. 1, 2018, с. 39-55.

[ЛФЯ 18,2] Логачев О.А., Федоров С.Н., Яценко В.В. О Δ - эквивалентности булевых функций. // Дискретн. математика, том 30, вып. 4, с. 29-40.

Соавторами работы [ЛПЯ 95] из данного списка рассмотрены вопросы обоснования использования для анализа задач частичного обращения конечных автоматов их диаграмм обращения (теоремы 1, 2, 3 по тексту статьи). Остальные результаты данной работы получены автором диссертации.

Соавторами работы [ЛСЯ 97] из данного списка рассмотрены вопросы исследования свойств кусочно-аффинных функций (теоремы 9, 10, 11; леммы 4 и 5; следствия 3, 4 и 5 по тексту статьи). Остальные результаты данной работы получены автором диссертации.

Соавтором работы [ЛЯ 98] из данного списка предложены понятия A_0 -группы и оператора "фиксации части переменных" J . Остальные результаты данной работы получены автором диссертации.

В работе [ЛСЯ 98] из данного списка автору диссертации принадлежат доказательства Теоремы 1, Следствия 1 (по тексту статьи).

В работе [ЛСЯ 99] из данного списка автору диссертации принадлежат доказательства Теоремы 1, Следствия 1, Теоремы 2, Теоремы 4 (по тексту статьи).

В работе [ЛСЯ 00,1] из данного списка автору диссертации принадлежат доказательства Теоремы 1, Леммы 1, Теоремы 2, Леммы 2, Теоремы 3, Следствия 1 (по тексту статьи).

В работе [ЛСЯ 00,2] из данного списка автору диссертации принадлежит доказательство Леммы 3 (по тексту статьи).

Соавторами работы [ЛСЯ 01] из данного списка получены результаты, связанные с оценкой элементов весовой таблицы в случае, когда разветвляющей является элементарная абелева 2-группа (теорема 4; следствия 2, 3, и 4 по тексту статьи). Остальные результаты данной работы получены автором диссертации.

В работе [ЛСЯ 02] из данного списка автору диссертации принадлежат доказательства Теоремы 1, Лемм 1, 2, 3, 5, 6, Следствий 1, 2 Замечания 1 (по тексту статьи).

Соавторами работы [ЛСЯ 04,1] из данного списка получено доказательство Предложения 2 (по тексту статьи). Остальные результаты данной работы получены автором диссертации.

Соавторами работы [ЛСЯ 04,2] из данного списка проведено обоснование теоретико-вероятностной модели, в условиях которой рассчитывались парамет-

ры частичного обращения комбинирующего генератора с устойчивой функцией усложнения. Остальные результаты данной работы получены автором диссертации.

Соавторами работы [ЛСЯ 04,3] из данного списка получена верхняя оценка радиуса покрытия кода Адамара (теорема 1 по тексту статьи). Остальные результаты данной работы получены автором диссертации.

В работе [БуЛо 05,2] из данного списка автору диссертации принадлежат постановки задач и разработки подходов к доказательствам утверждений Теорем 4,5,6 (по тексту статьи).

Соавтором работы [ЛоНа 07] из данного списка получены результаты, связанные с расчетом параметров алгоритма локального обращения фильтрующих генераторов с симметрическими функциями (теорема 1 по тексту статьи). Остальные результаты данной работы получены автором диссертации.

Соавторами работы [LYD 08] из данного списка предложены и обоснованы некоторые понятия (определения 3, 4, 5 по тексту статьи) и подготовлены примеры (примеры 1, 2, 3, 4, 6 по тексту статьи) для демонстрации свойств этих понятий. Остальные результаты данной работы получены автором диссертации.

Соавторами работы [LSSY 09] из данного списка доказаны утверждения теорем 7, 8, 9, 10, 11, а также лемм 1, 2 (по тексту статьи). Остальные результаты данной работы получены автором диссертации.

Соавтором работы [ЛоСм 13] из данного списка доказано утверждение теоремы 14 (по тексту статьи). Остальные результаты данной работы получены автором диссертации.

В работе [ЛФЯ 18,1] из данного списка автору диссертации принадлежит доказательство утверждения Теоремы 3 (по тексту статьи).

В работе [ЛФЯ 18,2] из данного списка автору диссертации принадлежат доказательства Теоремы 6, Следствия, Теоремы 7 (по тексту статьи).

В работе использована двойная нумерация определений, утверждений, формул и пр., первый номер указывает на параграф, второй — порядковый

в параграфе. Завершение доказательств отмечено символом $\square$. В начале диссертации приведены основные обозначения.

Автор признателен руководству Института проблем информационной безопасности МГУ имени М.В. Ломоносова и всем коллегам за постоянное внимание к данной работе. Особую благодарность за помощь и ценные замечания выражаю М.И. Анохину, Н.П. Варновскому, М.П. Денисенко, А.А. Сальникову, Ю.В. Таранникову, В.В. Яценко. Автор признателен также заведующему кафедрой Информационной безопасности ВМК МГУ имени М.В. Ломоносова академику Соколову И.А. за полезные обсуждения и рекомендации.

Глава 1. Алгебраические, комбинаторные и метрические характеристики дискретных функций, используемые в методах (алгоритмах) обращения

§1 Групповые дискретные функции

Дискретные функции, используемые при синтезе средств обеспечения информационной безопасности, как правило, обладают следующими свойствами: их области определения и значения являются конечными алгебраическими системами ([Мал 70]), а вычисления значений функций должны быть эффективными (с точки зрения обеспечения необходимых скоростей обработки и преобразования информации). Соответствующие этим алгебраическим системам операции естественным образом используются при синтезе функций. Наиболее часто встречающиеся варианты алгебр — это конечные абелевы группы, конечные коммутативные кольца, конечномерные векторные пространства над полями Галуа.

Исторически сложилось так, что первыми в области обеспечения информационной безопасности исследовались математические модели на основе самой простой нетривиальной булевой алгебры и булевых функций. По времени это совпало с периодом бурного развития во второй половине 20-го столетия таких математических дисциплин, как теория информации, теория кодирования, математическая криптография благодаря работам ряда выдающихся ученых (К.Э. Шеннон, В.А. Котельников, А.Н. Колмогоров и др.). В книгах [MeOV 96], [CuSt 09], [ЛССЯ 15] представлены разнообразные семейства математических моделей информационной безопасности на основе булевых функций и отображений. Эти модели актуальны и в настоящее время. В алгебраическом плане они представляют собой отображения элементарных абелевых 2-групп.

В 1976г. в работе [DiHe 76] были предложены новые принципы обеспечения информационной безопасности. Используемые для их описания семейства дискретных функций - это дискретные экспоненты, т.е. функции из $G^{\mathbb{Z}_m}$, где G — некоторая "большая" конечная циклическая группа порядка m . Необходимо отметить, что с тех пор в ходе синтеза и анализа протоколов, обеспечивающих информационную безопасность, рассматривались различные варианты групп G : симметрическая, знакопеременная, регулярная, $\mathbb{Z}_p^*$ (p — простое), $\mathbb{Z}_N^*$ (N — натуральное), $\mathbb{F}_q^*$, $(\mathbb{F}_q/c(\lambda))^*$ ($c(\lambda)$ — неприводимый полином) и др. (см. [Bac 03]). В последнее время актуальным является синтез и анализ протоколов, использующих групповую функцию циклической подгруппы в группе точек эллиптической кривой (см. [Wash 08]). Синтезу дискретных функций на некоммутативных группах посвящено значительное число книг и статей (см., например, [MyShU 08], [MyShU 11], [Poc 07], [ГКН 08], [Глу 10] и др.). Существуют в определенной мере обоснованные предложения по использованию других алгебраических систем — модулей, колец, луп и т.п. (см. [Ром 13]).

Пусть $f : G \rightarrow H$ — некоторая групповая функция, используемая в протоколе, обеспечивающем информационную безопасность. В процессе анализа этого протокола для функции f рассматривается широкий спектр математических задач, решение которых позволяет выявить или доказать наличие у f необходимых свойств.

Неформально можно выделить два важнейших класса таких задач.

Первый класс — задачи распознавания (следует отметить отличие данного класса от класса вычислительных задач в теории сложности вычислений (см. [ArBa 09])) с аналогичным названием, являющимся переводом английского термина "decision problems"). Предположим, что $G = M \times K$, где M, K — некоторые конечные группы. Приведем два типа задач из этого класса.

1. Пусть k — неизвестный элемент группы K и $b \in \{0,1\}$ — неизвестный бит. По условию задачи известны:

- полное описание функции f ;

- элементы m_0 и m_1 из группы M ;
- значение функции $h = f(m_b, k)$.

Требуется определить b с трудоемкостью существенно меньшей, чем перебор элементов группы K , и надежностью не меньше ε , $0 < \varepsilon < 1$.

- Пусть k — случайная величина, равномерно распределенная на группе K , т.е. $k \in_{\mathcal{U}} K$, m — фиксированный элемент из группы M . Рассмотрим случайные величины $\xi = f(m, k) \in_{\omega} N$ и $\eta \in_u N$. Требуется построить критерий, различающий распределения этих случайных величин.

Второй класс — задачи обращения. По условию задачи известно полное описание функции $f : G \rightarrow N$ и значение $h = f(x) \in N$, где x — некоторый неизвестный элемент из G . Требуется реализовать одну из следующих возможностей:

- найти элемент x ;
- найти произвольный $x' \in f^{-1}(h)$;
- описать (в виде математических соотношений) полный прообраз $f^{-1}(h)$ элемента h из N ;
- определить некоторую частичную информацию (математические соотношения) об элементах из $f^{-1}(h)$, т.е. математические соотношения, не позволяющие однозначно восстанавливать элементы из $f^{-1}(h)$, но определяющие некоторые свойства элементов из $f^{-1}(h)$.

Между этими классами задач (распознавания и обращения) имеются вполне определенные связи, поскольку их (задач) формулировки суть формализация соответствующих угроз информационной безопасности. Однако этот аспект лежит вне рамок настоящей работы. Нас будут интересовать лишь задачи обращения групповых дискретных функций.

Необходимо отметить математическую дисциплину, имеющую существенные связи с задачами обращения дискретных функций. Моментом зарождения

теории выводывания (learning theory¹) принято считать 1984 г., когда вышла в свет основополагающая работа Вальянта [Val 84]. Вместе с тем задачи, которыми занимается теория выводывания, настолько естественны и универсальны для различных математических дисциплин, что многие из этих задач исследовались специалистами задолго до 1984 г. Ей уделяется значительное внимание на крупнейших международных конференциях по математической кибернетике. Хорошим введением в теорию выводывания является обзор [Angl 92], а также вышедшие позднее публикации [Ant 10], [SST 10]. Не вдаваясь в подробности связей теории выводывания с интересующей нас областью исследования, можно сказать, что многие задачи обращения и распознавания для дискретных функций могут быть сформулированы как задачи выводывания.

§2 Комплекснозначные функции на конечных абелевых группах и их свойства

Основным объектом исследований, рассматриваемым в параграфах 2, 3, 4, является множество комплекснозначных функций на конечных абелевых группах. Нам будет удобнее (в указанных параграфах) использовать мультипликативную форму групповых операций, как это реализовано, например, в [HeRo 63], [Ser 67].

Пусть G — конечная абелева группа с мультипликативной операцией, порядок G равен n , экспонента группы G (максимальный порядок элементов из G) равна q , $e = e_G$ — единица группы G .

Пусть T — группа вращений окружности, т.е.

$$T = \{ \exp(2\sigma i x); 0 \leq x < 1 \},$$

¹Дословный перевод "learning theory" как "теория обучения" представляется крайне неудачным, т.к. вступает в противоречие с отсутствием процесса обучения (взаимодействия учитель-ученик) в постановках задач. В русскоязычной литературе термин для теории выводывания еще не сформировался.

T_q — подгруппа T , состоящая из корней степени q из единицы. Как обычно, через T^G обозначим множество функций на G со значениями в T , являющееся подмножеством линейного пространства $\mathbb{C}^G$ — всех комплекснозначных функций на G . На $\mathbb{C}^G$ обычным образом вводится скалярное произведение

$$(f_1, f_2) = \sum_{x \in G} f_1(x) \bar{f}_2(x), \quad f_1, f_2 \in \mathbb{C}^G,$$

где $\bar{f}_2(x)$ — число, комплексно-сопряженное к числу $f_2(x)$. Легко видеть, что если $f \in T^G$, то $(f, f) = n$.

Если зафиксировать некоторую нумерацию элементов G , то множество T^G можно отождествить с множеством T^n и представить как множество строк (векторов) длины n с компонентами из T или как n -мерный тор (произведение n экземпляров окружности T).

Множество $T_q^G \subset T^G$ функций на G со значениями в T_q является конечной абелевой группой относительно покомпонентного умножения функций (строк). Порядок группы T_q^G равен q^n , экспонента — q . Подгруппой группы T_q^G является группа $\hat{G} = \text{Hom}(G, T_q)$ — группа характеров группы G , т.е. гомоморфизмов $\chi : G \rightarrow T_q$.

Группа $\hat{G}$ изоморфна группе G . Зафиксируем некоторый изоморфизм и будем считать, что все характеры $\chi_u \in \hat{G}$ занумерованы элементами $u \in G$. Напомним основные соотношения ортогональности, которым удовлетворяют характеры

$$\sum_{x \in G} \chi_u(x) = \begin{cases} 0, & \text{если } u \neq e, \\ n, & \text{если } u = e, \end{cases}$$

$$\sum_{u \in G} \chi_u(x) = \begin{cases} 0, & \text{если } x \neq e, \\ n, & \text{если } x = e, \end{cases}$$

$$(\chi_u, \chi_v) = \begin{cases} 0, & \text{если } u \neq v, \\ n, & \text{если } u = v. \end{cases}$$

Квадратную $n \times n$ матрицу, являющуюся таблицей значений характеров группы G , будем обозначать

$$H_G = [\chi_u(x)]_{\substack{u \in G \\ x \in G}}.$$

В случае, когда G — элементарная абелева 2-группа порядка $n = 2^k$, матрица H_G является хорошо известной в теории кодирования матрицей Адамара-Сильвестра [MWS 77]. Соотношения ортогональности приводят к следующему матричному равенству

$$H_G \cdot H_G^* = n \text{Id}_n,$$

где Id_n — единичная матрица размера $n \times n$, H_G^* — транспонированная и комплексно-сопряженная к H_G матрица.

Матрица H_G задает преобразование Фурье функций из $\mathbb{C}^G$:

$$\widehat{f}(u) = \sum_{x \in G} f(x) \overline{\chi_u(x)}.$$

Обратное преобразование находится с помощью соотношений ортогональности

$$f(x) = n^{-1} \sum_{u \in G} \widehat{f}(u) \chi_u(x).$$

При этом выполняется равенство Парсеваля

$$\sum_{u \in G} \left| \widehat{f}(u) \right|^2 = n \sum_{x \in G} |f(x)|^2,$$

которое для $f \in T^G$ имеет вид

$$\sum_{u \in G} \left| \widehat{f}(u) \right|^2 = n^2.$$

Приведем некоторые полезные свойства преобразования Фурье. Для любого характера его преобразование Фурье сосредоточено в одной точке, т.е.

$$\widehat{\chi}_u(v) = \begin{cases} 0, & \text{если } u \neq v, \\ n, & \text{если } u = v. \end{cases}$$

Для $f \in \mathbb{C}^G$ и любого $u \in G$ обозначим через

$${}_uf(x) = f(ux)$$

функцию, полученную сдвигом аргумента функции f . Тогда

$$\left(\widehat{{}_uf}\right)(v) = \chi_v(u)\widehat{f}(v).$$

Рассмотрим действие автоморфизмов группы G на аргумент функции $f \in \mathbb{C}^G$ и обозначим через f^α , $\alpha \in \text{Aut}(G)$ получаемую при этом функцию

$$f^\alpha(x) = f(x^\alpha),$$

где x^α — образ элемента $x \in G$ при действии автоморфизма $\alpha \in \text{Aut}(G)$. Стандартным образом определим автоморфизм $\widetilde{\alpha} \in \text{Aut}(G)$, сопряженный к автоморфизму α , так что для любого характера χ_u выполнено

$$\chi_{u\widetilde{\alpha}}(x) = \chi_u^\alpha(x) = \chi_u(x^\alpha).$$

При этом для коэффициентов Фурье получим равенство

$$\widehat{f}^\alpha(u) = \widehat{f}\left(u^{\widetilde{\alpha^{-1}}}\right).$$

Свертка преобразований Фурье определяется следующим равенством:

$$\left(\widehat{f_1} * \widehat{f_2}\right)(u) = n^{-1} \sum_{v \in G} \widehat{f_1}(v) \widehat{f_2}(uv^{-1}).$$

Тогда преобразование Фурье произведения двух функций равно свертке преобразований Фурье

$$\widehat{(f_1 \cdot f_2)}(u) = \left(\widehat{f_1} * \widehat{f_2}\right)(u).$$

Применив преобразование Фурье к обеим частям тождества $f(x)\overline{f}(x) = 1$ и воспользовавшись легко проверяемым тождеством $\widehat{\overline{f}}(u) = \overline{\widehat{f}}(u^{-1})$ получим "соотношение ортогональности" для коэффициентов Фурье любой функции $f \in T^G$:

$$\sum_{u \in G} \widehat{f}(u) \overline{\widehat{f}}(uv^{-1}) = \begin{cases} 0, & \text{если } v \neq e, \\ n^2, & \text{если } v = e. \end{cases}$$

В теории кодирования [MWS 77] и криптологии [ЛССЯ 15] изложенные результаты первоначально (исторически) применялись для случая, когда G — элементарная абелева 2-группа, которую можно интерпретировать как векторное пространство V_k размерности k над полем из двух элементов. Тогда $q = 2$, $n = 2^k$ и $T_q = \{-1, +1\}$. В этом случае рассматриваются функции вида $(-1)^{f(x)}$, где f — некоторая булева функция от k переменных.

Таблица значений булевых функций (от k переменных) — это векторы (строки) длины 2^k , состоящие из нулей и единиц. Кодом Рида-Маллера $RM(k, r)$, $0 \leq r \leq k$ называется множество строк длины 2^k , соответствующих булевым функциям, алгебраическая степень которых не превосходит r . Коды Рида-Маллера образуют класс двоичных линейных блочных кодов, реализующих широкий спектр скоростей передачи информации. Обладая богатым набором разнообразных алгебраических свойств, а также семейством эффективных алгоритмов декодирования (как детерминированных, так и вероятностных), этот класс линейных блочных кодов активно используется в теоретиче-

ских исследованиях по обоснованию свойств различных средств обеспечения информационной безопасности.

Использование групповых функций (отображений) в качестве математических моделей, описывающих функционирование средств информационной безопасности, обуславливает важность развития математического аппарата анализа соответствующих функций. В частности, представляет большой интерес введение и развитие на множествах групповых отображений аналогов аппарата, используемого в исследованиях свойств кодов Рида-Маллера.

Основными элементами рассмотренных аналогов будут некоторые свойства "нелинейности" групповых отображений, обобщающие классические понятия параметров нелинейности для колец полиномов.

Нам потребуются следующие понятия. Линейными функциями в T_q^G будем называть характеры группы G , т.е. $\mathcal{L}(G) = \text{Hom}(G, T_q) = \hat{G}$. Аффинными функциями в T_q^G будем называть множество всех сдвигов характеров группы G :

$$\mathcal{A}(G) = \{f \in T_q^G : \exists u, v \in G, f(x) = \chi_u(vx), \forall x \in G\}.$$

Ясно, что аффинные функции в T_q^G получаются из характеров (линейных функций) умножением на константу: $f \in \mathcal{A}(G)$ тогда и только тогда, когда $f(x) = f(e)\chi_u(x)$ для некоторого $u \in G$ при всех $x \in G$. Ясно также, что $|\mathcal{A}(G)| = qn$. Из определения множества $\mathcal{A}(G)$ и соотношений ортогональности для характеров легко получить для любых $f_1, f_2 \in \mathcal{A}(G)$

$$(f_1, f_2) = \begin{cases} 0, & \text{если } \overline{f_1(e)}f_1 \neq \overline{f_2(e)}f_2, \\ f_1(e)\overline{f_2(e)}n, & \text{в противном случае.} \end{cases}$$

Обозначим через S_G симметрическую группу всех перестановок элементов G . Как и ранее, для любой $f \in T_q^G$ и любой $\sigma \in S_G$ определим функцию $f^\sigma \in T_q^G$ равенством $f^\sigma(x) = f(x^\sigma)$, где x^σ — образ элемента $x \in G$ при действии перестановки $\sigma \in S_G$. Для любого множества (кода) $K \subset T_q^G$ группу автоморфизмов

$\text{Aut}(K)$ определим равенством:

$$\text{Aut}(K) = \{\sigma \in S_G : f^\sigma \in K, \forall f \in K\}.$$

Назовем аффинной группой преобразований группы G следующую группу:

$$\text{Aff}(G) = \{\sigma \in S_G : x^\sigma = e^\sigma x^\varphi, \varphi \in \text{Aut}(G)\}.$$

Все множество T^G разбивается на орбиты относительно действия группы $\text{Aff}(G)$, которые мы будем называть аффинными классами по аналогии с соответствующим понятием для булевых функций. Функции из одной орбиты будем называть аффинно эквивалентными (или просто эквивалентными). Характеристики функций, которые постоянны на орбите, т.е. которые равны для аффинно эквивалентных функций, мы будем называть аффинными инвариантами.

Рассмотрим пример аффинного инварианта. Для фиксированного аффинного класса $K \subset T^G$ и фиксированной функции $f \in T^G$ рассмотрим мультимножество чисел $\{(f, g), g \in K\}$. Обозначим через $\mathcal{B}(f, K)$ мультимножество различных значений $(f, g), g \in K$ с указанием, сколько раз это значение встречается, когда g пробегает K .

Теорема 2.1. *Мультимножество $\mathcal{B}(f, K)$ является аффинным инвариантом для любого аффинного класса K .*

Доказательство. Для любого $\sigma \in \text{Aff}(G)$ имеем

$$(f^\sigma, g) = \sum_{x \in G} f(x^\sigma) \overline{g(x)} = \sum_{y \in G} f(y) \overline{g(y^{\sigma^{-1}})} = (f, g^{\sigma^{-1}}).$$

Таким образом, для аффинно эквивалентных функций f и $f^\sigma, \sigma \in \text{Aff}(G)$ мультимножества $\{(f, g), g \in K\}$ и $\{(f^\sigma, g), g \in K\}$ отличаются только перестановкой элементов. Следовательно, $\mathcal{B}(f, K)$ и $\mathcal{B}(f^\sigma, K)$ совпадают. $\square$

Введем понятие производной функции $f \in T^G$ по направлению $u \in G$, задавая функцию $\frac{df}{du}(x)$ следующим равенством:

$$\frac{df}{du}(x) = \overline{f(x)}f(ux)$$

для любых $x \in G$. Очевидно, что для любого $u \in G$ оператор дифференцирования $\frac{d}{du} : T^G \rightarrow T^G$ является гомоморфизмом группы T^G . Отметим следующие простейшие соотношения для производных

$$\frac{df}{de}(x) \equiv 1 \text{ для любой } f \in T^G;$$

$$\frac{dc}{du}(x) \equiv 1 \text{ для любых } c \in T \text{ и } u \in G;$$

$$\frac{d\chi}{du}(x) \equiv \chi(u) \text{ для любых } u \in G \text{ и } \chi \in \widehat{G}.$$

Для произвольной функции $f \in T^G$ через $L_f \subseteq G$ обозначим множество

$$L_f = \left\{ u \in G : \frac{df}{du}(x) \equiv \text{const} \right\}.$$

Справедливо следующее утверждение.

Лемма 2.2. *Для любой $f \in T^G$ множество L_f является подгруппой группы G .*

Доказательство. По определению производной имеем

$$f(ux) = \frac{df}{du}(x) \cdot f(x)$$

для любых $u, x \in G$. Применяя это равенство, последовательно получаем

$$\begin{aligned} f(uvx) &= \frac{df}{du}(vx) \cdot f(vx) = \\ &= \frac{df}{du}(vx) \cdot \frac{df}{dv}(x) \cdot f(x). \end{aligned}$$

Поэтому

$$\frac{df}{d(uv)}(x) = \frac{df}{du}(vx) \cdot \frac{df}{dv}(x)$$

для любых $u, v, x \in G$. Если теперь $u, v \in L_f$, то, очевидно, и $u \cdot v \in L_f$. Включение $e \in L_f$ вытекает из простейших свойств производной. $\square$

Подгруппу L_f будем называть группой гомоморфных трансляторов функции f (группой линейных трансляторов для булева случая).

В общей ситуации, когда группа L_f нетривиальна, т.е. $L_f \neq G$ и $L_f \neq \{e\}$, функцию f можно разложить по группе L_f в следующем смысле. Пусть группа G представима в виде прямого произведения $G = U \times V$. Будем говорить, что $f \in T^G$ разложима по группе U с выделением характера, или что от функции f отщепляется характер группы U , если для всех $u \in U, v \in V$ выполнено равенство

$$f(u, v) = \chi(u)g(v)$$

с некоторым характером χ группы U и функцией $g \in T^V$.

Теорема 2.3. Пусть $G = U \times V$. От функции $f \in T^G$ отщепляется характер группы U в том и только в том случае, когда U — подгруппа группы L_f .

Доказательство. Пусть от f отщепляется характер группы U . Вычислим производную f по направлению $w \in U$:

$$\begin{aligned} \frac{df}{dw}(u, v) &= \overline{f(u, v)} f(wu, v) = \\ &= \overline{\chi(u)g(v)} \chi(wu)g(v) = \chi(w). \end{aligned}$$

Поэтому $w \in L_f$ для любого $w \in U$, и тем самым $U < L_f$.

Пусть теперь $U < L_f$. Покажем, что функция $\overline{f(e, e)} f(w, e), w \in L_f$ является характером группы L_f , а значит, и группы U . По определению L_f при любых

$w \in L_f$ и $z \in U$ имеем

$$f((w,e)(z,e)) = \overline{f(e,e)}f(w,e)f(z,e),$$

и поэтому

$$\overline{f(e,e)}f((w,e)(z,e)) = \left(\overline{f(e,e)}f(w,e)\right)\left(\overline{f(e,e)}f(z,e)\right),$$

т.е. $\overline{f(e,e)}f(w,e)$ — характер L_f . Положим для любых $u \in U, v \in V$

$$\overline{f(e,e)}f(u,e) = \chi(u),$$

$$f(e,v) = g(v).$$

Тогда получаем

$$\begin{aligned} f(u,v) &= f((u,e)(e,v)) = \\ &= \overline{f(e,e)}f(u,e)f(e,v) = \chi(u)g(v) \end{aligned}$$

и тем самым от функции f отщепляется характер группы U . □

Одним из следствий теоремы 2.3 является необходимый признак нетривиальности группы L_f — наличие какого-то количества нулей среди коэффициентов Фурье функции f . Это связано с тем, что преобразование Фурье любого характера имеет только одно ненулевое значение.

Как и в теореме 2.3, пусть $G = U \times V$, где $U = L_f$. Обозначим через $\chi_f(u) = \chi_{(a_0,e)}(u)$ характер группы L_f , построенный в теореме 2.3:

$$\chi_f(u) = \chi_{(a_0,e)}(u) = \overline{f(e,e)}f(u,e).$$

Лемма 2.4. При описанных обозначениях для всех $(a,b) \in G, a \neq a_0$ выполнено равенство

$$\widehat{f}(a,b) = 0.$$

Доказательство. Воспользовавшись разложимостью функции f , преобразуем формулу для коэффициента Фурье:

$$\begin{aligned}\widehat{f}(a,b) &= \sum_{(u,v) \in G} f(u,v) \overline{\chi_{(a,b)}(u,v)} = \\ &= \sum_{(u,v) \in G} \chi_f(u) g(v) \overline{\chi_{(a,b)}(u,v)} = \\ &= \sum_{y \in V} g(v) \overline{\chi_{(e,b)}(e,v)} \sum_{u \in U} \chi_f(u) \overline{\chi_{(a,e)}(u,e)}.\end{aligned}$$

Из-за соотношений ортогональности для характеров внутренняя сумма в условиях леммы 2.4 равна нулю. $\square$

Возвращаясь теперь к аффинным классам, выясним, как связаны группы линейных трансляторов для аффинно эквивалентных функций.

Теорема 2.5. Пусть $\sigma \in \text{Aff}(G)$ имеет вид

$$x^\sigma = e^\sigma x^\varphi, x \in G$$

где $\varphi \in \text{Aut}(G)$. Тогда для любой функции $f \in T^G$ выполнено $L_{f^\sigma} = (L_f)^\varphi$, где $(L_f)^\varphi = \{z \in G : z = u^\varphi, u \in L_f\}$.

Доказательство. Для любых $x, u \in G$ имеем

$$(ux)^\sigma = e^\sigma(ux)^\varphi = e^\sigma u^\varphi x^\varphi = u^\varphi x^\sigma.$$

Далее преобразуем формулу для производной

$$\begin{aligned}\frac{df^\sigma}{du}(x) &= \overline{f^\sigma(x)} f^\sigma(ux) = \overline{f(x^\sigma)} f((ux)^\sigma) = \\ &= \overline{f(x^\sigma)} f(u^\varphi x^\sigma) = \frac{df}{du^\varphi}(x^\sigma).\end{aligned}$$

Таким образом,

$$\frac{df^\sigma}{du} = \left(\frac{df}{du^\varphi} \right)^\sigma,$$

что доказывает утверждение теоремы. □

При использовании аппарата производных и работе со скалярным произведением функций из T^G оказывается полезным следующее тождество.

Лемма 2.6. *Для любых $f_1, f_2 \in T^G$ выполнено тождество*

$$\sum_{u \in G} \left(\frac{df_1}{du}, \frac{df_2}{du} \right) = |(f_1, f_2)|^2.$$

Доказательство. Справедлива следующая цепочка равенств

$$\begin{aligned}\sum_{u \in G} \left(\frac{df_1}{du}, \frac{df_2}{du} \right) &= \sum_{u \in G} \sum_{x \in G} \overline{f_1(x)} f_1(ux) f_2(x) \overline{f_2(ux)} = \\ &= \sum_{x \in G} \overline{f_1(x)} f_2(x) \sum_{u \in G} f_1(ux) \overline{f_2(ux)} = \\ &= (f_1, f_2) \overline{(f_1, f_2)} = |(f_1, f_2)|^2.\end{aligned}$$

□

§3 Групповые коды Рида-Маллера и их свойства

Пусть G и T_q конечные абелевы группы, обладающие параметрами, описанными в параграфе 2. Семейство кодов типа Рида-Маллера $RM_r(G)$ порядка r на группе G будем определять рекуррентным способом. Положим

$$\begin{aligned}
\text{RM}_{-1}(G) &= \{f \in T_q^G : f(x) \equiv 1\}, \\
\text{RM}_0(G) &= \{f \in T_q^G : f(x) \equiv \text{const}\}, \\
\text{RM}_1(G) &= \{f \in T_q^G : \exists u, v \in G, f(x) = \chi_u(vx), \forall x \in G\}.
\end{aligned}$$

Далее для $r = 2, 3, \dots$ по определению положим

$$\text{RM}_r(G) = \left\{ f \in T_q^G : \frac{df}{du} \in \text{RM}_{r-1}(G), \forall u \in G \right\}.$$

При этом для некоторых групп может оказаться, что $\text{RM}_N(G) = T_q^G$ для подходящего N , а для некоторых групп в множестве T_q^G содержатся функции, не принадлежащие ни одному коду типа Рида-Маллера.

Код $\text{RM}_1(G)$ является прямым аналогом множества аффинных булевых функций, составляющих "классический" код Рида-Маллера первого порядка. Рассмотрим некоторые свойства кода $\text{RM}_1(G)$, которые подтверждают данную аналогию.

Элементы $\text{RM}_1(G)$ как функции на G естественно называть аффинными функциями на G , поскольку $\text{RM}_1(G) = \mathcal{A}(G)$ по определению.

Теорема 3.1. $\text{Aut}(\text{RM}_1(G)) = \text{Aff}(G)$.

Доказательство. Включение $\text{Aff}(G) \subseteq \text{Aut}(\text{RM}_1(G))$ вытекает из существования сопряженного автоморфизма $\tilde{\varphi} \in \text{Aut}(G)$, поскольку для любой функции $f \in \text{RM}_1(G)$ и любого $\sigma \in \text{Aff}(G)$ получаем

$$\begin{aligned}
f^\sigma(x) &= f(x^\sigma) = f(e)\chi_u(x^\sigma) = f(e)\chi_u(e^\sigma x^\varphi) = \\
&= f(e)\chi_u(e^\sigma)\chi_u(x^\varphi) = f(e)\chi_u(e^\sigma)\chi_{u\tilde{\varphi}}(x) \in \text{RM}_1(G).
\end{aligned}$$

Пусть теперь $\sigma \in \text{Aut}(\text{RM}_1(G))$. Тогда $\chi(x^\sigma) \in \text{RM}_1(G)$ для любого характера χ , т.е. существует такой характер $\chi^{(\sigma)}$, что

$$\chi(x^\sigma) = \chi(e^\sigma) \chi^{(\sigma)}(x)$$

для всех $x \in G$.

Используя это равенство, путем несложных преобразований получим при любых $x, y \in G$ равенство

$$\begin{aligned} \chi((xy)^\sigma) &= \chi(e^\sigma) \chi^{(\sigma)}(xy) = \chi(e^\sigma) \chi^{(\sigma)}(x) \chi^{(\sigma)}(y) \\ &= \overline{\chi(e^\sigma)} \left(\chi(e^\sigma) \chi^{(\sigma)}(x) \right) \left(\chi(e^\sigma) \chi^{(\sigma)}(y) \right) = \\ &= \overline{\chi(e^\sigma)} \chi(x^\sigma) \chi(y^\sigma) = \chi\left((e^\sigma)^{-1} x^\sigma y^\sigma\right). \end{aligned}$$

Поскольку это равенство выполнено для любого характера χ , то

$$(xy)^\sigma = (e^\sigma)^{-1} x^\sigma y^\sigma.$$

Последнее равенство означает, что перестановка $\varphi \in S_G$, задаваемая условием

$$x^\varphi = (e^\sigma)^{-1} x^\sigma,$$

является автоморфизмом группы G , и тем самым $\sigma \in \text{Aff}(G)$. □

Докажем утверждение, показывающее максимальность группы гомоморфных трансляторов только для функций из $\text{RM}_1(G)$.

Теорема 3.2. $\text{RM}_1(G) = \{f \in T_q^G : L_f = G\}$.

Доказательство. Из определения $\text{RM}_1(G)$ и простейших свойств производной легко получить, что если $f \in \text{RM}_1(G)$, то $L_f = G$.

Пусть теперь $f \in T_q^G$ и $L_f = G$. Это значит, что при всех $x, u \in G$ выполнено равенство

$$\frac{df}{du}(x) = \frac{df}{du}(e) = \overline{f(e)}f(u).$$

Подставляя данное соотношение в определение производной, получим при всех $x, u \in G$

$$f(ux) = \overline{f(e)}f(u)f(x)$$

и тем самым

$$\overline{f(e)}f(ux) = \left(\overline{f(e)}f(u)\right) \left(\overline{f(e)}f(x)\right).$$

Это равенство означает, что $\overline{f(e)}f(x)$ — характер группы G и поэтому $f \in \text{RM}_1(G)$. $\square$

Необходимо отметить, что утверждение теоремы 3.2 можно записать следующим образом:

$$\text{RM}_1(G) = \left\{ f \in T_q^G : \frac{df}{du} \in \text{RM}_0(G), \forall u \in G \right\}.$$

Для изучения свойств кодов $\text{RM}_r(G)$ удобно рассмотреть более общую конструкцию.

Множество функций $\Phi \subseteq T_q^G$ назовем A_0 -группой, если выполнены следующие свойства:

1. Φ является подгруппой группы T_q^G ;
2. Φ замкнуто относительно действия аффинной группы преобразований, т.е. если $f \in \Phi$, то $f^\sigma \in \Phi$ для всех $\sigma \in \text{Aff}(G)$;
3. Φ замкнуто относительно "сужений" или, другими словами, "фиксации части переменных".

Под "фиксацией части переменных" понимается следующая операция: пусть группа G представима в виде прямого произведения $G = U \times V$; тогда из

функции $f(u, v) \in \Phi$ путем фиксации части переменных получаются функции $f_u^{u^0}(u, v) = f(u^0, v)$ и $f_v^{v^0}(u, v) = f(u, v^0)$ для любых $u^0 \in U, v^0 \in V$.

Легко видеть, что множества $RM_{-1}(G), RM_0(G), RM_1(G)$ являются A_0 -группами.

Определим теперь оператор J , действующий на множествах функций, с помощью следующего равенства:

$$J\Phi = \left\{ f \in T_q^G : \frac{df}{du} \in \Phi, \forall u \in G \right\}.$$

Этот оператор описывает рекуррентный переход в определении кодов типа Рида-Маллера над группой G , поскольку теперь можно записать:

$$RM_r(G) = JRM_{r-1}(G), \quad r = 0, 1, 2, \dots$$

Легко видеть, что для A_0 -групп выполнено включение $\Phi \subseteq J\Phi$.

Теорема 3.3. *Оператор J переводит A_0 -группу в A_0 -группу.*

Доказательство. Пусть Φ — A_0 -группа. Проверим свойства A_0 -группы для $J\Phi$.

1. Пусть $f_1, f_2 \in J\Phi$, т.е. $\frac{df_1}{du}, \frac{df_2}{du} \in \Phi$ для всех $u \in G$. Тогда

$$\frac{d(f_1 \cdot f_2)}{du} = \frac{df_1}{du} \cdot \frac{df_2}{du} \in \Phi$$

для всех $u \in G$, и тем самым $f_1 \cdot f_2 \in J\Phi$.

2. Пусть $f \in J\Phi$ и $\sigma \in \text{Aff}(G)$, причем

$$x^\sigma = e^\sigma x^\varphi, \quad \varphi \in \text{Aut}(G)$$

для любого $x \in G$.

В параграфе 2 при доказательстве теоремы 2.5 получено тождество

$$\frac{df^\sigma}{du} = \left(\frac{df}{du^\varphi} \right)^\sigma.$$

Поскольку $\frac{df}{du^\varphi} \in \Phi$, и Φ — A_0 -группа, то $\frac{df}{du^\varphi} \in \Phi$, и тем самым для любого $u \in G$ имеем $\frac{df^\sigma}{du} \in \Phi$, т.е. $f^\sigma \in J\Phi$.

3. Это свойство выполнено для $J\Phi$ в силу следующего очевидного соображения: операции "взятия производной" и "фиксации части переменных" для любой функции коммутируют.

Тем самым для $J\Phi$ выполнены все три свойства A_0 -группы. $\square$

Следствие 3.4. Коды $RM_r(G)$, $r = -1, 0, 1, 2, \dots$ являются A_0 -группами для всех r .

Замечание 3.5. Для A_0 -группы Φ в определении $J\Phi$ требование $\frac{df}{du} \in \Phi$ для всех $u \in G$ можно заменить требованием $\frac{df}{du} \in \Phi$ для всех u из некоторого базиса G .

Действительно, в параграфе 2 уже использовалось тождество

$$\frac{df}{d(uv)}(x) = \frac{df}{du}(vx) \frac{df}{dv}(x).$$

Поэтому если Φ — A_0 -группа, и $\frac{df}{du}, \frac{df}{dv} \in \Phi$, то и $\frac{df}{d(uv)} \in \Phi$, что показывает справедливость утверждения замечания.

Представим теперь определение кода $RM_{r-1}(G)$ в следующем более удобном виде:

$$RM_{r-1}(G) = J^{r-1}RM_0(G) = J^rRM_{-1}(G),$$

или в развернутой форме:

$$RM_{r-1}(G) = \left\{ f \in T_q^G : \frac{d}{du^1} \frac{d}{du^2} \cdots \frac{d}{du^r} f \equiv 1 \text{ для всех } u^1, \dots, u^r \in G \right\}.$$

Отсюда видно, что для изучения свойств кодов $RM_r(G)$ необходимо рассмотреть полугруппу операторов на T_q^G , порожденную операторами дифференцирования. Для этого оказывается полезной следующая более общая конструкция.

Рассмотрим $\mathbb{Z}_q G$ — групповое кольцо группы G над кольцом $\mathbb{Z}_q$ (см. [Цим 11]). Элементами $\mathbb{Z}_q G$ являются всевозможные формальные суммы вида $\sum_{u \in G} \lambda_u u$, где $\lambda_u \in \mathbb{Z}_q$, $u \in G$, и произведение в $\mathbb{Z}_q G$ вычисляется по обычным правилам умножения многочленов с последующим приведением подобных членов.

Определим действие $\mathbb{Z}_q G$ на T_q^G следующим образом. Если $a \in \mathbb{Z}_q G$, $a = \sum_{u \in G} \lambda_u u$, то

$$(af)(x) = \prod_{u \in G} (f(ux))^{\lambda_u^{-1}}.$$

Очевидно, что при таком определении оператор a является гомоморфизмом группы T_q^G , а умножению операторов соответствует умножение в кольце $\mathbb{Z}_q G$. Рассмотренные ранее операторы сдвига и дифференцирования вкладываются в эту конструкцию, поскольку

$$\begin{aligned} {}_u f(x) &= (u^{-1} f)(x), \\ \frac{d}{du} f(x) &= ((u^{-1} - 1) f)(x), \end{aligned}$$

где 1 — единица кольца $\mathbb{Z}_q G$, $u \in G$. Здесь мы воспользовались тождеством $\overline{f(x)} = (f(x))^{-1}$ для любой $f \in T_q^G$.

Работа с элементами группового кольца упрощает вычисления с операторами дифференцирования и позволяет легко получать тождества для производных, используя соотношения в кольце $\mathbb{Z}_q G$.

Пример 3.6. Ранее (в данном параграфе) было использовано тождество для производных

$$\frac{df}{d(u^1 u^2)}(x) = \frac{df}{du^1}(u^2 x) \frac{df}{du^2}(x).$$

Легко видеть, что оно является следствием тождества в $\mathbb{Z}_q G$:

$$u^1 u^2 - 1 = u^2(u^1 - 1) + (u^2 - 1).$$

Пусть теперь $u \in G$ имеет порядок t . Тогда

$$\sum_{i=0}^{t-1} u^i (u^{-1} - 1) = (u^{-1} - 1) \sum_{i=0}^{t-1} u^i = 0.$$

Поэтому для любой функции $f \in T_q^G$ получаем тождество

$$\prod_{i=1}^{t-1} \frac{df}{du} (u^i x) \equiv 1.$$

Заметим, что последнее тождество является характеристическим для функций, являющихся производными других функций.

Лемма 3.7. *Функцию $f \in T_q^G$ можно представить в виде производной некоторой функции $g \in T_q^G$ по некоторому направлению $u \in G$, $u^t = e$, в том и только в том случае, если*

$$\prod_{i=0}^{t-1} f(u^i x) \equiv 1$$

при всех $x \in G$.

Доказательство. Необходимость очевидна.

Для доказательства достаточности рассмотрим дифференциальное уравнение

$$\frac{dg}{du}(x) = f(x)$$

при известной функции $f \in T_q^G$.

Разложим G на смежные классы по циклической группе $\langle u \rangle$ и зафиксируем какую-нибудь полную систему представителей смежных классов — $y^1, y^2, \dots, y^k \in G$, $n = kt$. Тогда очевидно, что дифференциальное уравнение эквивалентно совокупности k подсистем (из t уравнений каждая) от непересекающихся множеств неизвестных значений $g(x)$ для любого $x \in G$. При этом j -ая подсистема ($j = 1, 2, \dots, k$) имеет вид:

$$\begin{aligned}
\overline{g(y_j)}g(uy_j) &= f(y_j), \\
\overline{g(uy_j)}g(u^2y_j) &= f(uy_j), \\
&\dots\dots\dots \\
\overline{g(u^{t-1}y_j)}g(y_j) &= f(u^{t-1}y_j).
\end{aligned}$$

Условия леммы — это в точности необходимые и достаточные условия разрешимости этих систем. Общее решение задается следующим равенством:

$$g(u^{i+1}y_j) = g(y_j)f(u^iy_j)f(u^{i-1}y_j)\dots f(y_j),$$

$j = 1, \dots, k, i = 0, \dots, t-2$, причем k начальных значений $g(y_j), j = 1, \dots, k$ можно выбирать произвольным образом. $\square$

Используя операции в групповом кольце $\mathbb{Z}_qG$, мы можем теперь записать определение кода $RM_{r-1}(G)$ в виде

$$RM_{r-1}(G) = \left\{ f \in T_q^G : \prod_{i=1}^r \left((u^i)^{-1} - 1 \right) f \equiv 1, \forall u^1, \dots, u^r \in G \right\}.$$

Через $G(u^1, \dots, u^r) \in \mathbb{Z}_qG$ обозначим следующий элемент группового кольца:

$$G(u^1, \dots, u^r) = \prod_{i=1}^r \left((u^i)^{-1} - 1 \right) = \sum_{u \in G} \lambda_u u.$$

При определенных таким образом параметрах λ_u получим, что функция f принадлежит $RM_{r-1}(G)$ тогда и только тогда, когда для f выполнены следующие соотношения (в теории кодирования такие соотношения принято называть проверками):

$$\prod_{u \in G} (f(ux))^{\lambda_u - 1} \equiv 1$$

для всех наборов $\lambda_u, u \in G$, которые соответствуют элементам $G(u^1, \dots, u^r)$ для любых $u^1, \dots, u^r \in G$.

Легко видеть, что равенство

$$\text{RM}_N(G) = T_q^G$$

выполнено для некоторого N в том и только в том случае, если в групповом кольце $\mathbb{Z}_q G$ выполнено тождество

$$G(u^1, \dots, u^N) = 0$$

для всех $u^1, \dots, u^N \in G$.

В силу коммутативности кольца $\mathbb{Z}_q G$ такое N существует тогда и только тогда, когда каждый элемент вида $u - 1, u \in G$ является нильпотентным элементом кольца $\mathbb{Z}_q G$.

Лемма 3.8. *Любой элемент $u - 1, u \in G$ является нильпотентным элементом кольца $\mathbb{Z}_q G$ в том и только том случае, когда число q имеет вид p^s , p — простое, s — натуральное.*

Доказательство. Пусть для некоторого N в $\mathbb{Z}_q G$ выполнено тождество $(u - 1)^N = 0$ для любого $u \in G$, и пусть p — некоторый простой делитель q . При некотором натуральном s выполнено $N \leq p^s$, и поэтому $(u - 1)^{p^s} = 0$ для любого $u \in G$.

Последнее тождество выполнено в $\mathbb{Z}_q G$, а поэтому и в $\mathbb{Z}_p G$. Но в $\mathbb{Z}_p G$ выполнено также $(u - 1)^p = u^p - 1$ для любого $u \in G$. Из последних двух тождеств следует, что $u^{p^s} = e$ для всех u в группе G , и поэтому $q = p^{s_1}, s_1 \leq s$.

Пусть теперь $q = p^s$. Известно (следует из теоремы Лукаса), что биномиальные коэффициенты $\binom{p^s}{k}, 1 \leq k < p^s$, делятся на p . Поэтому получаем

$$(u - 1)^{p^s} = pQ(u)$$

для любого $u \in G$ с некоторым многочленом $Q(u)$. Возводя последнее равенство в степень s , получаем нужное тождество в $\mathbb{Z}_q G$:

$$(u - 1)^{sp^s} = p^s Q^s(u) = 0.$$

□

Следствие 3.9. *Любая функция из T_q^G принадлежит некоторому коду типа Рид-Маллера на группе G в том и только том случае, когда q имеет вид p^s , p — простое, s — натуральное.*

Если же q не удовлетворяет условиям следствия 3.9, то среди функций из T_q^G могут быть и неподвижные точки операторов дифференцирования $\frac{d}{du}$.

Лемма 3.10. *Пусть порядок элемента $u^0 \in G$ равен t , t — делитель q . Дифференциальное уравнение $\frac{df}{du^0}(x) = f(x)$ для любого $x \in G$ имеет нетривиальное решение $f \in T_q^G$ тогда и только тогда, когда числа q и $2^t - 1$ имеют общий нетривиальный делитель.*

Доказательство. Воспользовавшись рассуждениями леммы 3.7, легко получить, что утверждение леммы выполнено тогда и только тогда, когда выполнены тождества

$$f(x)f(u^0x) \dots f((u^0)^{t-1}x) \equiv 1$$

$$f((u^0)^i x') \equiv (f(x))^{2^i}, i = 1, \dots, t-1.$$

Подставляя второе равенство в первое, получаем

$$(f(x))^{2^i-1} \equiv 1.$$

Поскольку значения $f(x)$ лежат в T_q , последнее тождество возможно для нетривиальных значений $f(x)$ тогда и только тогда, когда числа q и $2^i - 1$ имеют общий нетривиальный делитель.

□

Пример 3.11. Числа q, t , удовлетворяющие условиям леммы 3.10, можно построить с помощью теоремы Эйлера. Пусть m — произвольное нечетное число. Положим $t = \Phi(m)$ (Φ — функция Эйлера), $q = \text{Н.О.К.}(t, m)$. Тогда q делится на t и m . Следовательно, по теореме Эйлера $2^t - 1$ также делится на m .

В заключение данного параграфа обратимся опять к A_0 -группам. Рассмотрим возможность доказательства для них некоторых свойств, аналогичных свойствам кода $\text{RM}_1(G)$.

Пусть Φ — A_0 -группа. Для любой функции $f \in T^G$ через $L_f^\Phi \subseteq G$ обозначим следующее множество

$$L_f^\Phi = \left\{ u \in G : \frac{df}{du} \in \Phi \right\}.$$

При этом $L_f^{\text{RM}_0(G)} = L_f$ — группа линейных трансляторов функции f , рассмотренная в параграфе 2. Дословно повторяя рассуждение леммы 2.2 и при этом используя тот факт, что Φ — A_0 -группа, легко доказать следующее утверждение.

Лемма 3.12. *Множество L_f^Φ для любой $f \in T^G$ и любой A_0 -группы Φ является подгруппой G .*

Очевидно также, что если $\Phi_1 \subseteq \Phi_2$, то для любой $f \in T^G$ выполнено включение подгрупп $L_f^{\Phi_1} \subseteq L_f^{\Phi_2}$.

Обратившись теперь к оператору J , заметим, что для любой A_0 -группы Φ выполнено

$$J\Phi = \{ f \in T_q^G : L_f^\Phi = G \}.$$

При $\Phi = \text{RM}_0(G)$ это равенство является содержанием теоремы 3.2.

Аналогично теореме 2.5 получаем следующее утверждение.

Теорема 3.13. Пусть $\sigma \in \text{Aff}(G)$ имеет вид $x^\sigma = e^\sigma x^\varphi$, $\varphi \in \text{Aut}(G)$. Тогда для любой функции $f \in T^G$ и любой A_0 -группы Φ выполнено $L_{f^\sigma}^\Phi = (L_f^\Phi)^\varphi$, где

$$(L_f^\Phi)^\varphi = \{z \in G : z = u^\varphi, u \in L_f^\Phi\}.$$

§4 Понятие дуальности для конечных модулей. Обобщённые тождества Мак-Вильямс

В настоящем параграфе рассмотрены свойства дуальности конечных модулей — как аналогов линейных кодов. Отметим, что некоторые приводимые ниже результаты при определённых предположениях могут быть доказаны и для случая бесконечных колец и модулей.

Пусть R — некоторое фиксированное конечное коммутативное кольцо с единицей. Будем рассматривать конечные двусторонние R -модули, т.е. не будем различать умножение элементов кольца и модуля слева и справа. Для модуля U через $\text{Sub}(U)$ обозначим множество всех подмодулей модуля U , которое является полной модулярной решёткой относительно частичного порядка — "теоретико-множественное включение" подмодулей (см. [Лам 71]). Будем называть элементы множества $\text{Sub}(U)$ не только подмодулями U , но и линейными кодами, или просто кодами в U .

Отображение $\varphi : \text{Sub}(U) \rightarrow \text{Sub}(V)$ для двух модулей U и V называется изотонным, если оно сохраняет порядок, т.е. из $A_1 \subseteq A_2$ следует $\varphi(A_1) \subseteq \varphi(A_2)$, и антиизотонным, если оно обращает порядок, т.е. из $A_1 \subseteq A_2$ следует $\varphi(A_1) \supseteq \varphi(A_2)$.

Взаимно однозначное изотонное (антиизотонное) отображение называется изоморфизмом (антиизоморфизмом, или дуальным изоморфизмом) решёток (см. [Бирк 84]). Операцией замыкания (см. [Бирк 84]) на подмножествах некоторого множества называется отображение $A \rightarrow A^c$ такое, что

$$A \subseteq A^c; (A^c)^c = A^c,$$

$$(A_1 \subseteq A_2) \Rightarrow (A_1^c \subseteq A_2^c).$$

Замкнутыми относительно данной операции замыкания называются множества A , такие, что $A^c = A$. Важнейшим свойством операции замыкания является то, что все замкнутые подмножества данного множества образуют полную решётку (см. [Бирк 84]).

Теперь, следуя Г.Биркгофу, но применительно к модулям, опишем общую конструкцию, которая позволяет получить из произвольного отношения два взаимно обратных антиизоморфизма. Биркгоф называет эти антиизоморфизмы полярностями. В теории кодирования полярности, в частности, приводят к дуальным кодам.

Пусть $\perp$ — некоторое билинейное бинарное отношение между элементами двух модулей U и V . Это значит, что если $u^1 \perp v^1, u^2 \perp v^1, u^1 \perp v^2$ для некоторых $u^1, u^2 \in U, v^1, v^2 \in V$, то $(u^1 + u^2) \perp v^1, u^1 \perp (v^1 + v^2), (ru^1) \perp v^1, u^1 \perp (rv^1)$ при любом $r \in \mathbb{R}$. Для любых подмодулей $A \in \text{Sub}(U), B \in \text{Sub}(V)$ определим дуальные подмодули ("поляры" в терминологии Биркгофа) $A^* \in \text{Sub}(V), B^+ \in \text{Sub}(U)$ следующими равенствами:

$$A^* = \{v \in V : u \perp v, \forall u \in A\},$$

$$B^+ = \{u \in U : u \perp v, \forall v \in B\}.$$

Отображения $A \rightarrow A^*, B \rightarrow B^+$ для любого $\perp$ обладают следующими полезными свойствами (см. [Бирк 84]):

1. Оба отображения антиизотонны;
2. $A \subseteq (A^*)^+, B \subseteq (B^+)^*$;
3. $((A^*)^+)^* = A^*, ((B^+)^+)^* = B^+$;

4. Отображения $A \rightarrow (A^*)^+$, $B \rightarrow (B^+)^*$ являются операциями замыкания;
5. Отображения (полярности) $A \rightarrow A^*$, $B \rightarrow B^+$ на полных решётках замкнутых подмодулей (кодов) являются взаимно обратными и определяют антиизоморфизм этих решёток.

Для фиксированного билинейного бинарного отношения $\perp$ будем называть $\perp$ -замкнутыми кодами в U, V такие подмодули $A \in \text{Sub}(U)$, $B \in \text{Sub}(V)$, что

$$A = (A^*)^+, B = (B^+)^*.$$

Пример 4.1. Для модуля M через $\widehat{M}$ обозначим модуль рациональных характеров модуля M , т.е. гомоморфизмов $\chi : M \rightarrow \mathbb{Q}/\mathbb{Z}$. Известно, что $\widehat{\widehat{M}} \cong M$. Пусть теперь $U = M \times U_1$, $V = \widehat{M} \times V_1$ и отношение $\perp$ для любых $(m, u) \in M \times U_1$ и любых $(\chi, v) \in \widehat{M} \times V_1$ определено условием

$$(m, u) \perp (\chi, v) \Leftrightarrow \chi(m) = 0.$$

Легко видеть, что полные решетки $\perp$ -замкнутых кодов — это в точности $\text{Sub}(M)$ и $\text{Sub}(\widehat{M})$. К описанному примеру сводится довольно большой класс полярностей, рассмотренных в [ЛСЯ 98].

Естественно ожидать, что некоторые характеристики пар взаимно дуальных $\perp$ -замкнутых кодов связаны друг с другом. Целый ряд таких связей для конкретных классов кодов давно известен в теории кодирования под названием тождеств Мак-Вильямс. Соотношения типа тождества Мак-Вильямс доказываются для достаточно широкого класса алгебраических объектов (в том числе и бесконечных): полных весовых функций произвольных групповых кодов, весовых функций Ли для групповых кодов, схем отношений.

В рассматриваемой нами ситуации линейных кодов в модулях U и V формализуем понятие "характеристики кода". Достаточно широкий класс характеристик может быть выражен следующим образом.

Пусть X — некоторое фиксированное комплексное векторное пространство. Рассмотрим функции на модуле со значениями в этом пространстве. Если $\rho : U \rightarrow X$ — такая функция, а $A \in \text{Sub}(U)$ — код, то элемент

$$\rho \langle A \rangle = \sum_{u \in A} \rho(u),$$

$\rho \langle A \rangle \in X$, будем называть ρ -структурой кода A . Ряд практически интересных характеристик кодов может быть задан в таком виде при подходящем выборе пространства X и функции ρ . Элемент $\rho \langle A \rangle \in X$ может быть представлен в виде целочисленной линейной комбинации элементов $x \in X$ вида

$$\rho \langle A \rangle = \sum_{u \in A} \rho(u) = \sum_{x \in X} \# \{u \in A : \rho(u) = x\} \cdot x$$

и поэтому фактически задает частоты распределений кодовых точек $u \in A$ по блокам ядерного разбиения функции ρ , определяемого равенством

$$U = \bigcup_{x \in X} \rho^{-1}(x).$$

Хотя ранее в этом параграфе мы сделали предположение о конечности рассматриваемых модулей, необходимо отметить, что указанное выше соотношение может быть использовано и в случае бесконечных модулей, когда выполняется условие локальной конечности для любого $x \in X$ величины $\# \{u \in A : \rho(u) = x\}$.

Пример 4.2. ([ЗиЭр 96]). Пусть на модуле U задана норма w , которая принимает k различных значений (будем считать, что они занумерованы числами от 1 до k). Функцию ρ зададим следующим образом: если $w(u) = i$, то $\rho(u) = (0, \dots, 1, \dots, 0)$, где единица стоит на i -ом месте. В этом случае ρ -структура $\rho \langle A \rangle$ кода A является весовым распределением кода A .

Пример 4.3. ([Неч 95]). ρ — структура $\rho \langle A \rangle$ кода A является общей весовой функцией кода $A < G^N$, $G = \{s_1, \dots, s_m\}$, в случае, когда функция ρ определена следующим образом:

$$\rho([g_1, \dots, g_N]) = x_1^{\sigma_1([g_1, \dots, g_N])} \dots x_m^{\sigma_m([g_1, \dots, g_N])}, \forall [g_1, \dots, g_N] \in G^N,$$

где

$$\sigma_j([g_1, \dots, g_N]) = \# \{i \in \overline{1, N} : g_i = s_j\}.$$

Пусть теперь билинейное бинарное отношение $\perp$ индуцировано некоторым билинейным отображением $\perp: U \times V \rightarrow S$, где S — некоторый конечный R -модуль, т.е.

$$u \perp v \Leftrightarrow \perp(u, v) = 0.$$

В этом случае связь между модулями U и V удаётся выразить на языке комплексных характеров и получить некоторые полезные тождества. Пусть χ — некоторый комплексный характер модуля S , т.е. $\chi: S \rightarrow \mathbb{C}^*$ — гомоморфизм из аддитивной группы модуля S в мультипликативную группу поля комплексных чисел. Тогда при любом $v \in V$ отображение

$$u \rightarrow \chi(\perp(u, v)) = (\chi \circ \perp_v)(u)$$

является комплексным характером модуля U , и при любом $u \in U$ отображение

$$v \rightarrow \chi(\perp(u, v)) = (\chi \circ {}_u\perp)(v)$$

является комплексным характером модуля V . Для данного $A \in \text{Sub}(U)$ характер χ_A назовем различающим модуль A , если все характеры $\chi_A \circ \perp_v$, $v \in V \setminus A^*$ являются нетривиальными на A (другими словами, не аннулируют A). Аналогичным образом определяется характер χ_B , различающий модуль B . Справедливо следующее утверждение.

Лемма 4.4 ([ЗиЭр 96]). Пусть $\perp : U \times V \rightarrow S$ — билинейное отображение. Тогда для любых конечных $A \in \text{Sub}(U)$, $B \in \text{Sub}(V)$ и любых различающих характеров χ_A, χ_B выполнены равенства

$$\sum_{u \in A} \chi_A(\perp(u, v)) = \begin{cases} \#A, & \text{если } v \in A^*, \\ 0 & \text{в противном случае,} \end{cases}$$

$$\sum_{v \in B} \chi_B(\perp(u, v)) = \begin{cases} \#B, & \text{если } u \in B^+, \\ 0 & \text{в противном случае.} \end{cases}$$

Рассмотрим теперь произвольную функцию $\rho : V \rightarrow X$ и определим для нее дуальную $\rho_A^+ : U \rightarrow X$, $A \in \text{Sub}(U)$, равенством

$$\rho_A^+(u) = \sum_{v \in V} \chi_A(\perp(u, v)) \rho(v).$$

Аналогично определим дуальную $\varphi_B^* : V \rightarrow X$, $B \in \text{Sub}(U)$, для функции $\varphi : U \rightarrow X$

$$\varphi_B^* = \sum_{u \in U} \chi_B(\perp(u, v)) \varphi(u).$$

Справедливо следующее утверждение.

Теорема 4.5. Дуальные структуры для дуальных кодов связаны тождествами:

$$\rho_A^+ \langle A \rangle = \#A \cdot \rho \langle A^* \rangle, \forall A \in \text{Sub}(U),$$

$$\varphi_B^* \langle B \rangle = \#B \cdot \varphi \langle B^+ \rangle, \forall B \in \text{Sub}(V).$$

Доказательство. Докажем, например, первое равенство (второе доказывается аналогично). Пусть $A \in \text{Sub}(U)$. Запишем выражение для ρ_A^+ — структуры

кода A и преобразуем его, воспользовавшись леммой 4.4,

$$\begin{aligned}\rho_A^+ \langle A \rangle &= \sum_{u \in A} \rho_A^+(u) = \sum_{u \in A} \sum_{v \in V} \chi_A(\perp(u, v)) \rho(v) = \\ &= \sum_{v \in V} \rho(v) \sum_{u \in A} \chi_A(\perp(u, v)) = \#A \cdot \rho \langle A^* \rangle.\end{aligned}$$

□

Докажем обычные тождества Мак-Вильямс, например, для двоичных линейных кодов ([MWS 77]), как следствие данной теоремы.

Следствие 4.6. Пусть A — двоичный линейный $[N, k]$ -код, $A^\perp$ — ортогональный к нему $[N, N - k]$ -код. Тогда

$$W_{A^\perp}(\lambda_1, \lambda_2) = \frac{1}{2^k} W_A(\lambda_1 + \lambda_2, \lambda_1 - \lambda_2),$$

где

$$W_C(\lambda_1, \lambda_2) = \sum_{u \in C} \lambda_1^{N - \text{wt}(u)} \lambda_2^{\text{wt}(u)}$$

для $C = A, A^\perp$; $\text{wt}(u)$ — вес Хэмминга вектора u .

Доказательство. Рассмотрим конструкцию примера 4.3, где в качестве группы G выступает аддитивная группа поля из двух элементов $\mathbb{F}_2$. В качестве билинейного отображения $\perp$ рассмотрим скалярное умножение векторов длины N , т.е. $\perp(u, v) = \langle u, v \rangle$, а в качестве характера χ — канонический аддитивный характер поля $\mathbb{F}_2$, $\chi(b) = (-1)^b$. Функция ρ имеет вид

$$\rho(u) = \lambda_1^{N - \text{wt}(u)} \lambda_2^{\text{wt}(u)}.$$

В этих обозначениях дуальным к A кодом A^* будет ортогональное подпространство, т.е. $A^* = A^\perp$, а дуальная к ρ функция ρ^+ определяется равенством

$$\rho^+(u) = \sum_{v \in V_N} (-1)^{\langle u, v \rangle} \lambda_1^{N - \text{wt}(u)} \lambda_2^{\text{wt}(u)},$$

где $V_N = \mathbb{F}_2^N$.

Преобразуем выражение для функции ρ^+ . Имеем

$$\begin{aligned} \rho^+(u) &= \sum_{v \in V_N} (-1)^{u_1 v_1 + \dots + u_N v_N} \prod_{i=1}^N \lambda_1^{1-v_i} \lambda_2^{v_i} = \\ &= \sum_{v_1=0}^1 \sum_{v_2=0}^1 \dots \sum_{v_N=0}^1 \prod_{i=1}^N (-1)^{u_i v_i} \lambda_1^{1-v_i} \lambda_2^{v_i}. \end{aligned}$$

Так как в данном случае сумма произведений равна произведению сумм, то последнее выражение равно

$$\rho^+(u) = \prod_{i=1}^N \sum_{w=0}^1 (-1)^{u_i w} \lambda_1^{1-w} \lambda_2^w.$$

Если $u_i = 0$, то внутренняя сумма равна $\lambda_1 + \lambda_2$. Если $u_i = 1$, то она равна $\lambda_1 - \lambda_2$. Таким образом,

$$\rho^+(u) = (\lambda_1 + \lambda_2)^{N - \text{wt}(u)} (\lambda_1 - \lambda_2)^{\text{wt}(u)}.$$

Из теоремы 4.5 следует, что

$$\rho_A^+ = \#A \rho \langle A^* \rangle,$$

или в наших обозначениях

$$W_{A^\perp}(\lambda_1, \lambda_2) = 2^{-k} W_A(\lambda_1 + \lambda_2, \lambda_1 - \lambda_2),$$

где

$$W_C(\lambda_1, \lambda_2) = \sum_{u \in C} \lambda_1^{N - \text{wt}(u)} \lambda_2^{\text{wt}(u)}.$$

□

§5 Бент-функции на конечной абелевой группе

Пусть G — конечная абелева группа с мультипликативной операцией и параметрами, рассмотренными в §2. В различных ситуациях возникает множество функций из T^G , выделяемых условием

$$\widehat{f}(e) = \sum_{x \in G} f(x) = 0.$$

Обозначим это множество через $UF(G)$ и будем называть функции из этого множества уравновешенными функциями. Другими словами, уравновешенными будем называть те функции из T^G , для которых в разложение по характерам не входит тривиальный характер $\chi_e(x)$.

Для функций из $UF(G) \cap T_q^G$ можно получить более содержательное описание, поскольку в этом случае $\widehat{f}(e)$ выражается через частоты значений из T_q , принимаемых функцией $f \in T_q^G$:

$$\widehat{f}(e) = \sum_{t \in T_q} b^f(t) \cdot t,$$

где

$$b^f(t) = \# \{x \in G : f(x) = t\}.$$

Зафиксируем некоторый порождающий элемент θ циклической группы T_q . Положим

$$b_k^f = b^f(\theta^k), k = 0, 1, \dots, q-1.$$

Рассмотрим полином

$$p^f(z) = \sum_{k=0}^{q-1} b_k^f z^k.$$

По построению $\widehat{f}(e) = p^f(\theta)$ и, значит,

$$f \in \text{UF}(G) \cap T_q^G$$

тогда и только тогда, когда θ — корень полинома $p^f(z)$. Но все элементы $t \in T_q$ являются корнями уравнения $z^q - 1 = 0$. Следовательно, если $f \in \text{UF}(G) \cap T_q^G$, то полиномы $p^f(z)$ и $z^q - 1$ имеют общий нетривиальный делитель.

Пример 5.1. Интересным и содержательным примером являются такие функции, для которых $p^f(z)$ делится на $\sum_{k=0}^{q-1} z^k$, то есть функции, для которых $b^f(t)$ — постоянная, не зависящая от t , и тем самым равная n/m . Такие функции обычно называют также равновероятными [ЛССЯ 15] или функциями, сохраняющими равномерное распределение.

Заметим, что если для функции $f \in T^G$ выполнено условие $\widehat{f}(a) = 0$, то $\overline{\chi_a(x)} f(x) \in \text{UF}(G)$.

Как уже ранее было отмечено в §2, все множество T^G разбивается на орбиты относительно действия группы $\text{Aff}(G)$.

Определение 5.2. Функцию $f \in T^G$, для которой при всех $a \in G$ выполнено $|\widehat{f}(a)|^2 = n$, будем называть бент-функцией на группе G . Множество всех бент-функций на группе G обозначим через $\text{BF}(G)$.

Очевидно, что множества $\text{UF}(G)$ и $\text{BF}(G)$ замкнуты относительно действия группы $\text{Aff}(G)$, то есть состоят из какого-то количества аффинных классов.

Коды $\text{RM}_r(G)$ типа Рида-Маллера порядка $r = 0, 1, \dots$, на группе G определены в §3 рекуррентным образом:

$$\begin{aligned}\mathrm{RM}_r(\mathrm{G}) &= \{f \in \mathrm{T}_q^{\mathrm{G}} : df/du \in \mathrm{RM}_{r-1}(\mathrm{G}), \forall u \in \mathrm{G}\}, \\ \mathrm{RM}_{-1}(\mathrm{G}) &= \{f \in \mathrm{T}_q^{\mathrm{G}} : f(x) \equiv 1\}.\end{aligned}$$

При этом уместны аналогии с булевым случаем. Функции из $\mathrm{RM}_0(\mathrm{G})$ — это константы, функции из $\mathrm{RM}_1(\mathrm{G})$ — это аффинные функции на G , так как они получаются из характеров (линейных функций) умножением на константу: $f \in \mathrm{RM}_1(\mathrm{G})$ тогда и только тогда, когда $f(x) = f(e)\chi_u(x)$ для некоторого $u \in \mathrm{G}$ при всех $x \in \mathrm{G}$. Функции из $\mathrm{RM}_2(\mathrm{G})$ — это квадратичные функции на G , так как любая их производная — аффинная функция.

Выполняется аналог критерия Ротхауза [Rot 76] для функций из $\mathrm{BF}(\mathrm{G})$.

Теорема 5.3. *Справедливо равенство*

$$\mathrm{BF}(\mathrm{G}) = \left\{ f \in \mathrm{T}^{\mathrm{G}} : \frac{df}{du} \in \mathrm{UF}(\mathrm{G}), \forall u \in \mathrm{G} \setminus e \right\}.$$

Доказательство. Вычислим преобразование Фурье функции $\frac{df}{du}$ и приведем его к более удобному виду

$$\begin{aligned}\widehat{\frac{df}{du}}(v) &= \sum_{x \in \mathrm{G}} \overline{f(x)} f(ux) \overline{\chi_v(x)} = \\ &= \sum_{x \in \mathrm{G}} \frac{1}{n} \sum_{w \in \mathrm{G}} \overline{\widehat{f}(w)} \overline{\chi_w(x)} \frac{1}{n} \sum_{z \in \mathrm{G}} \widehat{f}(z) \chi_z(ux) \overline{\chi_v(x)} = \\ &= \frac{1}{n^2} \sum_{w, z \in \mathrm{G}} \overline{\widehat{f}(w)} \widehat{f}(z) \chi_z(u) \sum_{x \in \mathrm{G}} \overline{\chi_w(x)} \chi_z(x) \overline{\chi_v(x)} = \\ &= \frac{1}{n} \sum_{w \in \mathrm{G}} \overline{\widehat{f}(w)} \widehat{f}(wv) \chi_{wv}(u).\end{aligned}$$

Отсюда получаем, что при всех $u \in G$ выполнено

$$\widehat{\frac{df}{du}}(e) = \frac{1}{n} \sum_{w \in G} \left| \widehat{f}(w) \right|^2 \chi_w(u).$$

Теперь достаточно воспользоваться свойствами группы характеров и получить, что условие $\left| \widehat{f}(w) \right|^2 = n$ для всех $w \in G$ эквивалентно условию $\widehat{\frac{df}{du}}(e) = 0$ для всех $u \in G, u \neq e$. $\square$

На случай элементарной абелевой p -группы критерий Ротхауза обобщен в [Амб 94].

Еще одну форму этого критерия можно получить, рассмотрев следующую числовую характеристику функций из T^G :

$$\Delta^2 f = \sum_{u \neq e} \left| \widehat{\frac{df}{du}}(e) \right|^2.$$

Очевидно, что $\Delta^2 f$ является аффинным инвариантом. Воспользовавшись соотношением для $\widehat{\frac{df}{du}}(e)$ из теоремы 5.3 легко получить следующие соотношения

$$\begin{aligned} \widehat{\frac{df}{du}}(e) &= \frac{1}{n} \sum_{w \in G} \left(\left| \widehat{f}(w) \right|^2 - n \right) \chi_w(x), u \neq e \\ 0 &= \frac{1}{n} \sum_{w \in G} \left(\left| \widehat{f}(w) \right|^2 - n \right). \end{aligned}$$

В силу ортогональности матрицы H_G отсюда следует, что

$$\sum_{u \neq e} \left| \widehat{\frac{df}{du}}(e) \right|^2 = \frac{1}{n} \sum_{w \in G} \left(\left| \widehat{f}(w) \right|^2 - n \right)^2.$$

Следствие 5.4. *Справедливо равенство*

$$\text{BF}(G) = \{ f \in T^G : \Delta^2 f = 0 \}.$$

Таким образом, аффинный инвариант $\Delta^2 f$ можно рассматривать как меру удаления функции $f \in T^G$ от множества $BF(G)$.

Пример 5.5. Легко видеть, что для любых $t \in T, u \in G, \chi \in \widehat{G}, f \in T^G$ выполнено равенство

$$\widehat{\frac{d(t\chi f)}{du}}(e) = \chi(u) \widehat{\frac{df}{du}}(e)$$

и поэтому

$$\Delta^2(t\chi f) = \Delta^2 f.$$

В частности, отсюда следует, что для всех $f \in BF(G)$ функции $t\chi f$ также являются бент-функциями на группе G .

Рассмотрим еще один вариант критерия для бент-функции на группе G .

Теорема 5.6. *Функция $f \in T^G$ является бент-функцией тогда и только тогда, когда система из n функций*

$$f'_u(x) = \frac{df}{du}(x), u \in G,$$

образует ортогональный базис в $\mathbb{C}^G$.

Доказательство. Легко видеть, что условия ортогональности

$$(f'_u, f'_v) = 0, u, v \in G, u \neq v,$$

эквивалентны условию

$$\sum_{x \in G} \frac{df}{du}(x) = 0, u \in G, u \neq e,$$

которое в силу теоремы 5.3 выполнено только для бент-функций на группе G . □

Базисы в $\mathbb{C}^G$, выделяемые теоремой 5.6, имеют специальный вид. Для их описания введем следующее понятие.

Определение 5.7. Систему из n функций $b_u(x)$, $u \in G$, назовем бент-базисом, если она удовлетворяет следующим условиям:

- (1) $(b_u, b_v) = n$ при $u = v$ и $(b_u, b_v) = 0$ при $u \neq v$,
- (2) $b_v^u = \bar{b}_u b_{uv}$ при $u, v \in G$, где $f^u(x) = f(ux)$ — оператор сдвига для любой $f \in \mathbb{C}^G$.

Из определения можно получить следующие свойства любого бент-базиса:

- (a) $b_e(x) \equiv 1$, для доказательства достаточно в (2) положить $u = e$;
- (b) из (1) с учетом (a) следует, что

$$\sum_{x \in G} b_u(x) = \begin{cases} 0, & \text{если } u \neq e, \\ n, & \text{если } u = e; \end{cases}$$

- (c) $b_u(x) \in \mathbb{T}^G$ при всех $u \in G$, для доказательства достаточно в (2) положить $v = e$ и воспользоваться (a);
- (d) при всех $x \in G$

$$\left| \sum_{u \in G} b_u(x) \right|^2 = n,$$

для доказательства достаточно провести следующие простые выкладки с учетом свойств (2) и (b):

$$\begin{aligned} \sum_{u \in G} \overline{b_u(x)} \sum_{v \in G} b_v(x) &= \sum_{u, v \in G} \overline{b_u(x)} b_v(x) = \\ &= \sum_{w \in G} \sum_{u \in G} \overline{b_u(x)} b_{uw}(x) = \\ &= \sum_{w \in G} \sum_{u \in G} b_u(x) = \\ &= \sum_{w \in G} \sum_{y \in G} b_w(y) = n. \end{aligned}$$

Необходимо отметить, что ортогональный базис вида $\frac{df}{du}$, $u \in G$, соответствует не единственной бент-функции. Он не меняется при умножении функции f на любую константу из T . Чтобы исключить эту неоднозначность, введем условие нормировки $f(e) = 1$. Обозначим через $BB(G)$ множество всех бент-базисов в $\mathbb{C}^G$, а через $BNF(G)$ — множество всех бент-функций из $BF(G)$, удовлетворяющих условию нормировки. Справедливо следующее утверждение.

Теорема 5.8. *Отображение $\kappa_G : BNF(G) \rightarrow BB(G)$ вида*

$$f \in BNF(G) \xrightarrow{\kappa_G} \left\{ \frac{df}{du}(x), u \in G \right\} \in BB(G)$$

является взаимно однозначным и

$$\kappa^{-1} : BB(G) \rightarrow BNF(G)$$

имеет вид

$$\{b_u, u \in G\} \in BB(G) \xrightarrow{\kappa^{-1}} f(x) = b_x(e) \in BNF(G).$$

Доказательство. Пусть $f \in BNF(G)$. Тогда в соответствии с утверждением теоремы 5.6 система функций $\frac{df}{du}(x)$, $u \in G$ образует ортогональный базис в $\mathbb{C}^G$, то есть выполнено условие (1) в определении бент-базиса.

Условие (2) проверяется непосредственно. Действительно,

$$\begin{aligned} {}_u b_v(x) &= {}_u \left(\overline{f(x)} f(vx) \right) = \\ &= \left(f(x) \overline{f(ux)} \right) \left(\overline{f(x)} f(uvx) \right) = \\ &= (\overline{b_u} b_{uv})(x). \end{aligned}$$

Пусть $\{b_u(x), u \in G\}$ — некоторый базис из $BB(G)$. Положим $f(x) = b_x(e)$. Тогда $f \in T^G$, $f(e) = 1$ в силу свойств (а) и (с) бент-базиса. Покажем, что $\frac{df}{du}(x) = b_u(x)$. Действительно, для всех $u, x \in G$

$$\begin{aligned}\frac{df}{du}(x) &= \overline{f(x)}f(\sigma x) = \overline{b_x(e)}b_{ux}(e) = \\ &= {}_x b_u(e) = b_u(x).\end{aligned}$$

В силу свойства (1) бент-базиса и теоремы 5.6 функция $f(x)$ является бент-функцией. $\square$

Зафиксируем какую-нибудь бент-функцию f на группе G . Теперь любую функцию из $\mathbb{C}^G$ можно разложить по базису из производных $\frac{df}{du}, u \in G$. При этом естественно возникает понятие бент-преобразования, задаваемого матрицей

$$\mathcal{D}_f(G) = \left[\frac{df}{du}(x) \right]_{\substack{x \in G \\ u \in G}}$$

аналогично преобразованию Фурье, задаваемому матрицей $H(G)$. В силу теоремы 5.6 функция $f(x)$ принадлежит $BF(G)$ тогда и только тогда, когда

$$\mathcal{D}_f(G) \mathcal{D}_f^*(G) = n \text{Id}_n,$$

то есть, тогда и только тогда, когда для матрицы $\mathcal{D}_f(G)$ при $f \in BF(G)$ выполнено такое же соотношение ортогональности, что и для матрицы $H(G)$. Естественно, для произвольных бент-преобразований справедливы все результаты теории преобразования Фурье, которые используют только ортогональность матрицы $H(G)$.

Для примера приведем простейшие факты о бент-преобразовании $g(x) \rightarrow \check{g}(u)$, заданном с помощью матрицы $\mathcal{D}_f(G)$, $f \in BF(G)$:

$$\check{g}(u) = \sum_{x \in G} g(x) \overline{\frac{df}{du}(x)}, u \in G,$$

$$g(x) = \frac{1}{n} \sum_{u \in G} \check{g}(x) \overline{\frac{df}{du}(x)}, u \in G$$

$$\sum_{u \in G} |\check{g}(u)|^2 = n^2.$$

В связи с теоремой 5.3 естественно для произвольной функции $f \in T^G$ определить множество

$$PC(f) = \left\{ u \in G : \frac{df}{du} \in UF(G) \right\}.$$

Из рассуждений, связанных с теоремой 5.3, легко получить следующий результат.

Следствие 5.9. *Справедливо равенство*

$$PC(f) = \left\{ u \in G : \sum_{v \in G} \left| \widehat{f}(v) \right|^2 \chi_v(u) = 0 \right\}.$$

В булевом случае следствие 5.9 совпадает с теоремой 2 работы [Ящ 97,2].

С помощью условий на $PC(f)$ можно вводить различные множества функций и естественно ожидать, что чем больше множество $PC(f)$, тем ближе в определенном смысле функция f к множеству бент-функций. Приведем описание двух естественных множеств функций, рассмотренных в булевом случае в [Ящ 97,2].

Пусть $Q < G$ — подгруппа группы G . Через $Q^\perp$ обозначим дуальную к Q подгруппу (в другой терминологии — аннулятор подгруппы Q):

$$Q^\perp = \{ u \in G : \chi_u(x) = 1, x \in Q \}.$$

Как обычно, G/Q — это фактор-группа группы G по подгруппе Q .

Теорема 5.10. Пусть $Q < G$. Для функции $f \in T^G$ выполнено включение $Q \setminus e \subseteq PC(f)$ тогда и только тогда, когда коэффициенты Фурье функции f удовлетворяют системе линейных уравнений

$$\sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2 = n^2 / \#Q, v \in G/Q^\perp.$$

Доказательство. В силу следствия 5.9 коэффициенты Фурье любой функции $f \in T^G$ удовлетворяют системе линейных уравнений

$$\sum_{x \in G} \left| \widehat{f}(x) \right|^2 \chi_x(y) = 0, y \in PC(f).$$

Разложив G на смежные классы по $Q^\perp$, представим эти уравнения в виде

$$\sum_{v \in G/Q^\perp} \sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2 \chi_{uv}(y) = 0, y \in PC(f).$$

Поскольку $Q \setminus e \subseteq PC(f)$ и $\chi_u(y) = 1$ для всех $u \in Q^\perp, y \in Q$, получаем, что

$$\sum_{v \in G/Q^\perp} \chi_u(y) \sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2 = 0, \sigma \in Q \setminus e.$$

Добавляя теперь равенство Парсеваля, получаем следующую невырожденную систему из $\#Q$ уравнений относительно $\#Q$ неизвестных $\sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2, v \in G/Q^\perp$:

$$\begin{aligned} \sum_{v \in G/Q^\perp} \chi_v(y) \left(\sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2 \right) &= 0, y \in Q \setminus e, \\ \sum_{v \in G/Q^\perp} \left(\sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2 \right) &= n^2. \end{aligned}$$

Эта система имеет единственное решение

$$\sum_{u \in Q^\perp} \left| \widehat{f}(uv) \right|^2 = n^2 / \#Q, v \in G/Q^\perp.$$

Обратное утверждение теоремы очевидно. $\square$

Следствие 5.11. Пусть $Q < G, u^0 \in G/Q, y^0 \in e$. Для функции $f \in T^G$ выполнено включение $PC(f) \supseteq u^0Q$ тогда и только тогда, когда коэффициенты Фурье функции f удовлетворяют системе линейных уравнений

$$\sum_{u \in Q^\top} \left| \widehat{f}(uv) \right|^2 \chi_u(u^0) = 0, v \in G/Q^\perp.$$

Доказательство. Аналогично доказательству теоремы 5.10. $\square$

Рассмотрим некоторые полезные утверждения, описывающие свойства бент-функций на группе G .

Лемма 5.12. Для любой функции f из $BF(G)$ группа гомоморфных трансляторов тривиальна, то есть $L_f = \{e\}$.

Доказательство. Непосредственно вытекает из определений множеств $L_f, UF(G), BF(G)$. $\square$

Рассмотрим теперь "квадратичные" функции из $RM_2(G)$. Для них любая производная является сдвигом или тривиального, или нетривиального характера. Поэтому вся группа распадается на две части:

$$G = L_f \cup PC(f).$$

Квадратичные булевы функции ($G = \mathbb{F}_2^n$), удовлетворяющие условиям леммы 5.12, это невырожденные квадратичные формы. Они были первыми примерами бент-функций. Для случая $G = \mathbb{Z}_p$, где p — простое число, лемма 5.12 утверждает, что все функции из $RM_2(G) \setminus RM_1(G)$ являются бент-функциями.

Интересной особенностью бент-функций является то, что для них можно определить понятие дуальной функции, которая задает преобразование Фурье исходной функции. Пусть $f \in \text{BF}(G)$, тогда $\left|\widehat{f}(u)\right|^2 = n$ для всех $u \in G$ и дуальная функция $\widetilde{f}(u) \in T^G$ определяется равенством

$$\sqrt{n}\widetilde{f}(u) = \widehat{f}(u), u \in G.$$

Теорема 5.13. Пусть $f \in \text{BF}(G)$, тогда $\widetilde{f}$ также является бент-функцией. Причем

$$\widetilde{\widetilde{f}}(x) = f(x^{-1}), x \in G.$$

Доказательство. Утверждение теоремы вытекает из определения дуальной бент-функции и известного свойства преобразования Фурье.

$$\widehat{\widetilde{f}}(x) = n f(x^{-1}).$$

□

Важный пример явного выражения дуальной бент-функции будет приведен ниже.

Введем следующее понятие. Зафиксируем некоторую константу $\varepsilon \in T$. Функцию $f \in \text{BF}(G)$ назовем ε -самодуальной, если

$$\widetilde{f}(u) = \varepsilon f(u), u \in G.$$

Функции, являющиеся ε -самодуальными, — это собственные векторы матрицы $H(G)$ с собственным значением $\varepsilon\sqrt{n}$. В силу теоремы 5.13 для ε -самодуальной бент-функции f выполнены тождества

$$\varepsilon^2 f(x) = f(x^{-1}), \varepsilon^4 = 1.$$

Определим множество обобщенных бент-функций $\text{OBF}(G) \subset \mathbb{C}^G$, отказавшись в определении бент-функции от ограничения $f \in T^G$ и рассматривая все функции из $\mathbb{C}^G$ так, что

$$\text{OBF}(G) = \left\{ f \in \mathbb{C}^G : \left| \widehat{f}(u) \right| = \sqrt{n}, u \in G \right\}.$$

Для любой обобщенной бент-функции определена дуальная функция из T^G , причем очевидны следующие утверждения.

Лемма 5.14. *Переход к дуальной функции устанавливает взаимно однозначное соответствие между множествами функций $\text{OBF}(G)$ и T^G .*

Лемма 5.15. *Обобщенная бент-функция $f(x)$ является бент-функцией тогда и только тогда, когда дуальная функция $\widetilde{f}(u)$ удовлетворяет соотношениям ортогональности*

$$\sum_{u \in G} \widetilde{f}(u) \overline{\widetilde{f}(uv^{-1})} = \begin{cases} 0, & \text{если } v \neq e, \\ n, & \text{если } v = e. \end{cases}$$

В условиях леммы 5.14 дуальная функция $\widetilde{f}(u)$ также является бент-функцией (в силу теоремы 5.13) и поэтому лемма 5.15 дает другой вариант доказательства теоремы 5.3.

Напомним, что функция $f \in T^G$ называется разложимой, если для некоторого представления группы G в виде прямого произведения $G = U \times V$ функция f имеет вид

$$f(u, v) = g(u)h(v), (u, v) \in G, g \in T^U, h \in T^V,$$

то есть представляется в виде произведения функций-компонент, определенных на U и V соответственно. Например, характеры группы G являются разложимыми функциями для любого представления в виде $G = U \times V$. Очевидно, что любая производная разложимой функции есть произведение производных

компонент, и преобразование Фурье разложимой функции есть произведение преобразований Фурье компонент. Отсюда вытекает следующее утверждение.

Теорема 5.16. *Если $f \in T^G$ — разложимая функция и $f(u, v) = g(u)h(v)$, то $f \in UF(G)$ тогда и только тогда, когда или $g \in UF(U)$, или $h \in UF(V)$, и $f \in BF(G)$ тогда и только тогда, когда и $g \in BF(G)$, и $h \in BF(G)$.*

§6 σ -полиномы и приведенная оценка Вейля

Для конкретных областей обеспечения информационной безопасности в качестве математических моделей, как правило, рассматривают специфические семейства групповых функций. В частности, для теории кодирования и криптографии важную роль играет семейство групповых комплекснозначных функций (см. [Terr 01], [Сид 08], [ЛиНи 88]), являющихся композицией некоторого характера χ аддитивной абелевой группы конечного поля $\mathbb{F}_q$ ($G = (\mathbb{F}_q, +)$, $q = p^l$, p — простое) и полиномиального отображения $P : \mathbb{F}_q \rightarrow \mathbb{F}_q : f(x) = \chi(P(x))$.

Пусть $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ — функция абсолютного следа из $\mathbb{F}_q$ в $\mathbb{F}_p$, определяемая для любого $\alpha \in \mathbb{F}_q$ равенством $\text{tr}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{l-1}}$. Тогда функция χ_1 , определяемая для любого $\alpha \in \mathbb{F}_q$ равенством

$$\chi_1(\alpha) = \exp(2\pi i \text{tr}(\alpha)/p),$$

называется каноническим аддитивным характером поля $\mathbb{F}_q$, здесь $i = \sqrt{-1}$. Все остальные аддитивные характеры поля $\mathbb{F}_q$ задаются для любых $\alpha, b \in \mathbb{F}_q$ равенством

$$\chi_b(\alpha) = \chi_1(b\alpha).$$

Важнейшие алгебраические, комбинаторные и криптографические свойства функции $f(x) = \chi(P(x))$ выражаются с помощью величины

$$W(\chi, P) = \sum_{x \in \mathbb{F}_q} \chi(P(x)),$$

называемой суммой Вейля. Заметим также, что сумма Вейля представляет собой частный вид так называемой тригонометрической суммы (см. [ЛиНи 88]). Задача точного вычисления этих сумм для многочленов общего положения чрезвычайно сложна. Поэтому ограничиваются оценкой модуля $W(\chi, P)$ или вычислением $W(\chi, P)$ для некоторых классов полиномов. Тривиальной является оценка

$$|W(\chi, P)| \leq q.$$

Она достигается на полиномах $P(x)$, для которых $\text{tr}(P(x))$ есть некоторая постоянная величина. Нетривиальной является оценка Вейля

$$|W(\chi, P)| \leq (n-1)q^{1/2},$$

доказанная в предположениях, что $P \in \mathbb{F}_q[x]$ — полином степени $n \geq 1$, $(n, q) = 1$ и χ — нетривиальный аддитивный характер. Подчеркнем, что оценка Вейля зависит только от мощности поля и степени полинома. В известных примерах точного вычисления суммы Вейля используются и другие параметры полинома, кроме степени. Естественно ожидать, что при уточнении оценки Вейля в нее также будут вводиться новые параметры.

Свойства сумм Вейля тесно связаны с числом решений уравнения Артина-Шрейера

$$y^q - y = P(x), P \in \mathbb{F}_q[x]$$

и уравнения

$$\text{tr}_s(P(x)) = b, P \in \mathbb{F}_{q^s}[x], b \in \mathbb{F}_q,$$

где

$$\mathrm{tr}_s(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{s-1}} -$$

относительный след поля $\mathbb{F}_{q^s}$ над полем $\mathbb{F}_q$. Эти уравнения играют особую роль в теории чисел. Приведем один пример такой связи.

Предложение 6.1 ([ЛиНи 88]). *Пусть*

$$\begin{aligned} W_s(\chi, P) &= \sum_{x \in \mathbb{F}_{q^s}} \chi^{(s)}(P(x)), \\ N_s(P, b) &= \# \{x : \mathrm{tr}_s(P(x)) = b\}, \end{aligned}$$

где $\chi^{(s)}$ — поднятие характера χ , то есть

$$\chi^{(s)} = \chi(\mathrm{tr}_s(\alpha)).$$

Тогда

$$\begin{aligned} W_s(\chi, P) &= \sum_{b \in \mathbb{F}_q} N_s(P, b) \chi(b), \\ N_s(P, b) &= \frac{1}{q} \sum_{\chi \in \widehat{G}} W_s(\chi, P) \overline{\chi}(b). \end{aligned}$$

Поскольку нас интересуют свойства сумм Вейля, можно определить на $\mathbb{F}_q[x]$ эквивалентности, задаваемые соответствующими суммами, и сократить число полиномов, подлежащих изучению. Вначале сделаем несколько элементарных замечаний.

Во-первых, отметим, что если два полинома $P_1(x), P_2(x) \in \mathbb{F}_q[x]$ задают одно и то же отображение поля $\mathbb{F}_q$ в себя, то есть $P_1(x) = P_2(x)$ для любого x из $\mathbb{F}_q$, то их суммы Вейля также совпадают: $W(\chi, P_1) = W(\chi, P_2)$ для любого характера χ . Это равносильно тому, что суммы Вейля полиномов, сравнимых в кольце $\mathbb{F}_q[x]$ по идеалу, порожденному полиномом $x^q - x$, совпадают. В частности, алгебраические степени рассматриваемых полиномов могут не превышать

$q - 1 :$

$$\deg P(x) \leq q - 1.$$

Во-вторых, при изучении сумм значений аддитивного характера можно ограничиться рассмотрением полиномов степени не выше $q - 2$ с нулевым свободным членом. В самом деле, пусть

$$P(x) = a_0 + P_1(x) + a_{q-1}x^{q-1}, \quad a_0, a_{q-1} \in \mathbb{F}_q,$$

где $\deg(P_1(x)) \leq q - 2$, $P_1(0) = 0$. Ясно, что

$$\begin{aligned} W(\chi, P) &= \sum_{x \in \mathbb{F}_q} \chi(a_0 + P_1(x) + a_{q-1}x^{q-1}) = \\ &= \chi(a_0) \left(\chi(0) + \sum_{x \in \mathbb{F}_q^*} \chi(P_1(x) + a_{q-1}x^{q-1}) \right) = \\ &= \chi(a_0) + \chi(a_0 + a_{q-1}) \sum_{x \in \mathbb{F}_q^*} \chi(P_1(x)) = \\ &= \chi(a_0) - \chi(a_0 + a_{q-1}) + \chi(a_0 + a_{q-1}) \sum_{x \in \mathbb{F}_q} \chi(P_1(x)). \end{aligned}$$

Таким образом, показано, что

$$W(\chi, P) = c + dW(\chi, P_1),$$

где $c = \chi(a_0) - \chi(a_0 + a_{q-1})$ и $d = \chi(a_0 + a_{q-1})$.

Обозначим через $\mathcal{K} \subset \mathbb{F}_q[x]$ множество полиномов степени не выше $q - 2$ с нулевым свободным членом.

Теперь рассмотрим менее тривиальную эквивалентность: будем называть полиномы $P_1(x)$ и $P_2(x)$ эквивалентными по следу, если для всех $x \in \mathbb{F}_q$ выполнено $\text{tr}(P_1(x)) = \text{tr}(P_2(x))$. Поскольку tr — линейное отображение, т.е. гомоморфизм аддитивной группы кольца $\mathbb{F}_q[x]$, то полиномы $P_1[x]$ и $P_2[x]$ эк-

вивалентны по следу тогда и только тогда, когда $P_1[x] - P_2[x]$ принадлежит ядру указанного гомоморфизма. Как известно (см., например, [Степ 91]), полином $P(x)$ принадлежит этому ядру тогда и только тогда, когда для каждого $x \in \mathbb{F}_q$ он может быть представлен в виде $P(x) = \Phi(x) - \Phi^p(x)$ с некоторым $\Phi(x) \in \mathbb{F}_q[x]$. Теперь опишем образ гомоморфизма tr . Зафиксируем некоторый базис поля $\mathbb{F}_q$ и будем рассматривать $\mathbb{F}_q$ как векторное пространство над $\mathbb{F}_p$. Поскольку значение $\text{tr}(P(x))$ принадлежит простому полю $\mathbb{F}_p$, очевидно, что

$$\text{tr}(P(x)) \in \mathbb{F}_p[x_1, \dots, x_l],$$

где $x_1, \dots, x_l$ — координаты x в выбранном нами базисе. С другой стороны, для каждого полинома $Q \in \mathbb{F}_p[x_1, \dots, x_l]$ можно построить такой полином $P \in \mathbb{F}_q[x]$, что

$$\text{tr}(P(x)) = Q(x_1, \dots, x_l).$$

Теперь воспользуемся теоремой о гомоморфизмах и получим следующее утверждение.

Теорема 6.2. *Факторгруппа аддитивной группы кольца $\mathbb{F}_q[x]$ по ядру гомоморфизма $\text{tr} : \mathbb{F}_q[x] \rightarrow \mathbb{F}_p[x_1, \dots, x_l]$ изоморфна аддитивной группе кольца $\mathbb{F}_p[x_1, \dots, x_l]$.*

Кратной суммой Вейля на конечном поле $\mathbb{F}_p$ будем называть сумму

$$W(\chi, Q) = \sum_{x_1, \dots, x_l \in \mathbb{F}_p} \chi(Q(x_1, \dots, x_l)),$$

где χ — нетривиальный аддитивный характер поля $\mathbb{F}_p$, а $Q(x_1, \dots, x_l)$ — некоторый полином из $\mathbb{F}_p[x_1, \dots, x_l]$.

Следствие 6.3. *Множество значений сумм Вейля $W(\chi, P)$, когда полином P пробегает кольцо $\mathbb{F}_q[x]$, совпадает с множеством значений кратных сумм Вейля $W(\chi, Q)$, когда полином $Q(x_1, \dots, x_l)$ пробегает кольцо $\mathbb{F}_p[x_1, \dots, x_l]$.*

Напомним предварительно понятие циклотомического класса ([MWS 77]). Множество вычетов по модулю $p^l - 1$ относительно операции умножения на p распадается на подмножества, называемые циклотомическими классами по модулю $p^l - 1$. Циклотомический класс C_s , в котором s — наименьшее число, состоит из чисел

$$\{s, sp, sp^2, \dots, sp^{l_s-1}\},$$

где l_s — наименьшее целое положительное число такое, что $sp^{l_s} \equiv s \pmod{p^l-1}$. Число s будем называть представителем циклотомического класса C_s . Множество всех ненулевых представителей обозначим $Cl(p, l)$.

Мощность l_s циклотомического класса C_s делит число l , поэтому в поле $\mathbb{F}_q$ существует (единственное) подполе $\mathbb{F}_{p^{l_s}}$ порядка p^{l_s} . Относительный след поля $\mathbb{F}_q$ над полем $\mathbb{F}_{p^{l_s}}$ — это линейное отображение, ядро которого состоит из элементов вида $b - b^{p^{l_s}}, b \in \mathbb{F}_q$. В каждом смежном классе аддитивной группы поля $\mathbb{F}_q$ по этому ядру имеется единственный элемент вида $c_s \zeta_s, c_s \in \mathbb{F}_{p^{l_s}}, \zeta_s$ — некоторый фиксированный элемент из $\mathbb{F}_q$, относительный след которого отличен от нуля. Если l/l_s не делится на p , то в качестве ζ_s можно взять единицу.

Определение 6.4. *Полином $\Phi(x) \in \mathcal{K}$ будем называть циклотомически приведенным, или cr -полиномом, если он имеет вид*

$$\Phi(x) = \sum_{s \in Cl(p, l)} c_s \zeta_s x^s, \quad c_s \in \mathbb{F}_{p^{l_s}}.$$

Теорема 6.5. *Каждый полином из $\mathcal{K}$ эквивалентен по следу некоторому циклотомически приведенному полиному.*

Доказательство. Пусть

$$P(x) = \sum_{i=1}^{p^l-2} a_i x^i \in \mathcal{K}.$$

Представим $P(x)$ в виде

$$P(x) = \sum_{s \in \sigma_l} \sum_{j=0}^{l_s-1} a_{sp^j} x^{sp^j} = \sum_{s \in \sigma_l} P_s(x).$$

Зафиксируем $s \in \sigma_l$ и рассмотрим полином $P_s(x)$, который естественно называть циклотмически однородным

$$P_s(x) = \sum_{j=0}^{l_s-1} a_{sp^j} x^{sp^j}.$$

Подберем такой полином

$$\Phi_s(x) = \sum_{j=0}^{l_s-1} b_{sp^j} x^{sp^j}$$

и такой элемент $c_s \in \mathbb{F}_{p^{l_s}}$, что

$$P_s(x) + \Phi_s(x) - \Phi_s^p(x) = c_s \zeta_s x^s. \quad (6.1)$$

Это будет означать, что следы полиномов $P_s(x)$ и $c_s \zeta_s x^s$ при любом x из $\mathbb{F}_q$ совпадают, или, что полиномы $P_s(x)$ и $c_s \zeta_s x^s$ эквивалентны по следу. Уравнение (6.1) равносильно системе

$$\begin{aligned} a_s + b_s - b_{sp^{l_s-1}}^p &= c_s \zeta_s, \\ a_{sp} + b_{sp} - b_s^p &= 0, \\ &\dots \\ a_{sp^{l_s-1}} + b_{sp^{l_s-1}} - b_{sp^{l_s-2}}^p &= 0. \end{aligned} \quad (6.2)$$

Выберем элемент $b_s = b \in \mathbb{F}_q$ произвольным образом. Тогда остальные коэффициенты b_{sp^j} и элемент c_s определяются из системы (6.2) однозначно:

$$\begin{aligned}
b_{sp} &= -a_{sp} + b^p, \\
b_{sp^2} &= -a_{sp^2} + b_{sp}^p = -a_{sp^2} - a_{sp}^p + b^{p^2}, \\
&\dots \\
b_{sp^{l_s-1}} &= -a_{sp^{l_s-1}} + b^p)sp^{l_s-1} = -a_{sp^{l_s-1}} - \dots - a_{sp}^{p^{l_s-2}} + b^{p^{l_s-1}}, \\
c_s \zeta_s &= a_s + b - b_{sp^{l_s-1}}^p = a_s + \dots + a_{sp}^{p^{l_s-1}} + b - b^{p^{l_s}}.
\end{aligned}$$

Отсюда видно, что когда элемент b пробегает поле $\mathbb{F}_q$, элемент $c_s \zeta_s$ пробегает фиксированный, в зависимости от $a_s + a_{sp^{l_s-1}} + \dots + a_{sp}^{p^{l_s-1}}$, смежный класс аддитивной группы поля $\mathbb{F}_q$ по ядру относительно следа по подполю $\mathbb{F}_{p^{l_s}}$. Поэтому можно выбрать $b \in \mathbb{F}_q$ так, что $c_s \in \mathbb{F}_{p^{l_s}}$.

Проделав эти вычисления для каждого $s \in \sigma_l$, получим искомое утверждение. $\square$

То, что при изучении тригонометрических сумм достаточно рассматривать многочлены, у которых от нуля отличны лишь коэффициенты при степенях, являющихся минимальными представителями циклотомических классов, специалисты понимали и ранее (см., например, [MZK 95], где такие полиномы называют каноническими). Теорема 6.5 показывает, что в ряде случаев можно дополнительно сократить множество рассматриваемых полиномов за счет специального выбора коэффициентов при таких степенях.

В частности, два различных канонических полинома могут оказаться эквивалентными по следу. Непонимание этого приводит к ошибкам (см. [MZK 95], лемма 1).

В соответствии с теоремой 6.5 корректным является следующее обозначение: для любого полинома $P(x) \in \mathcal{K}$ через $\text{Deg}(P)$ обозначим алгебраическую степень нелинейности cr -полинома, эквивалентного по следу данному полиному

$P(x)$. Очевидно, что для любого полинома $P(x) \in \mathcal{K}$

$$\text{Deg}(P) \leq \deg(P)$$

и число $\text{Deg}(P)$ взаимно просто с p . Отметим, что спектр значений $\text{Deg}(P)$ для полиномов $P(x) \in \mathcal{K}$ меньше, чем спектр значений $\deg(P)$. В частности, число различных значений, которые может принимать $\text{Deg}(P)$, совпадает с числом циклотомических классов. Последовательное применение теоремы 6.5 и оценки Вейля позволяет улучшить оценку Вейля.

Теорема 6.6 (приведенная оценка Вейля). *Пусть $P(x)$ — полином из кольца $\mathbb{F}_q[x]$ степени не выше $q-2$ с нулевым свободным членом и χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$. Тогда*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| \leq (\text{Deg}(P) - 1) q^{1/2},$$

если $\text{Deg}(P) \neq 0$ и

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| = q,$$

если $\text{Deg}(P) = 0$.

Доказательство. Если $\text{Deg}(P) = 0$, то утверждение теоремы очевидно. Предположим, что $\text{Deg}(P) \neq 0$. Применим к полиному $P(x)$ теорему 6.5 и построим sr -полином $\tilde{P}(x)$ степени нелинейности $\text{Deg}(P)$ такой, что

$$\text{tr}(P(x)) = \text{tr}(\tilde{P}(x))$$

для любого $x \in \mathbb{F}_q$. Тогда для любого характера χ

$$W(\chi, P) = W(\chi, \tilde{P}).$$

Поскольку $\text{Deg}(P)$ взаимно просто с p , к полиному $\tilde{P}(x)$ можно применить оценку Вейля и получить требуемое неравенство

$$|W(\chi, P)| = |W(\chi, \tilde{P})| \leq (\text{Deg}(P) - 1) q^{1/2}.$$

□

В приведенной оценке Вейля используется новый параметр полинома, $\text{Deg}(P)$, вычисление которого для конкретного полинома P , очевидно, не представляет особого труда. При этом оценка Вейля улучшается в трех направлениях:

- (1) расширяется область применения оценки, так как нет требования взаимной простоты $\text{deg}(P)$ и p ;
- (2) расширяется область, в которой оценка эффективнее тривиальной, так как очевидно, что в ряде случаев одновременно выполняются оба неравенства $\text{deg}(P) \geq q^{1/2}$ и $\text{Deg}(P) \leq q^{1/2}$;
- (3) как правило, $\text{Deg}(P) < \text{deg}(P)$, поэтому приведенная оценка точнее; более того, как показывают примеры, отношение $\text{deg}(P) / \text{Deg}(P)$ может иметь порядок даже q^ϵ .

Наиболее наглядно этот эффект виден на примере циклотомически однородного полинома, который в соответствии с теоремой 6.5 эквивалентен одночлену. Пусть для некоторого $s \in \sigma_l$

$$P_s(x) = \sum_{j=0}^{l_s-1} a_{sp^j} x^{sp^j},$$

тогда полином $P_s(x)$ эквивалентен по следу $c_s \zeta_s x^s$ для некоторого $c_s \in \mathbb{F}_{p^{l_s}}$, зависящего от a_{sp^j} , $j = 0, \dots, l_s - 1$. Если $a_{sp^{l_s-1}} = \dots = a_{sp^{k+1}} = 0$, $a_{sp^k} \neq 0$, то $\text{deg}(P) = sp^k$, и если $c_s \neq 0$, то $\text{Deg}(P) = s$. В этом случае

$$\frac{\text{deg}(P)}{\text{Deg}(P)} = p^k, 0 \leq k \leq l_s - 1.$$

В качестве следствия теоремы 6.6 можно сформулировать такое утверждение: необходимым условием достижимости обычной оценки Вейля для полинома $P(x)$ является равенство $\deg(P) = \text{Deg}(P)$.

§7 Некоторые характеристики "нелинейности" групповых отображений

В данном параграфе удобно будет использовать аддитивную запись для групповых операций, не оговаривая, о какой конкретно группе идет речь, кроме тех случаев, когда такая вольность в обозначениях может вызвать неоднозначное толкование.

Пусть G и H — конечные абелевы группы. Множество всех отображений группы G в группу H будем обозначать через $H^G = \{f : G \rightarrow H\}$. Множество H^G является конечной абелевой группой с операцией поточечного сложения отображений. Иногда отображения $f : G \rightarrow H$ удобно представлять в виде наборов длины $\#G$ с координатами из группы H , которые занумерованы элементами группы G (такое представление обычно называют табличным).

В группе отображений H^G выделим подгруппу гомоморфизмов, обозначаемую $\text{Hom}(G, H)$ [Sho 08]. Нас будут интересовать свойства (иногда их называют метрическими) отображений $f : G \rightarrow H$, связанных с расположением их по отношению к $\text{Hom}(G, H)$. Для придания точного смысла соответствующим утверждениям введем некоторые характеристики отображений.

Сначала введем на H^G подходящие эквивалентности.

Определение 7.1. *Отображения f и g из H^G назовем α -эквивалентными, если имеются автоморфизмы $\omega^1 \in \text{Aut}(G)$, $\omega^2 \in \text{Aut}(H)$ и такие элементы $u \in G, v \in H$, что*

$$\omega^2(f(x)) + v = g(\omega^1(x) + u)$$

для любого $x \in G$.

Замечание 7.2. В данном параграфе мы будем использовать знак $+$ для групповых операциях в G и H . Всякий раз из контекста будет ясно, об операции в какой группе идет речь.

Легко проверить, что введенное в определении 7.1 отношение является отношением эквивалентности. В случае отображений линейных векторных пространств над конечным полем α -эквивалентность совпадает с аффинной эквивалентностью (два отображения векторных пространств называются аффинно эквивалентными, если одно может быть получено из другого с помощью невырожденной аффинной замены переменных и композиции с невырожденным аффинным отображением). Естественно считать, что α -эквивалентные отображения "одинаково расположены" относительно $\text{Hom}(G, H)$. Например, аффинно эквивалентные булевы функции расположены на одинаковом расстоянии (по Хэммингу) от множества аффинных функций.

Классы α -эквивалентных отображений будем называть α -классами. Характеристики отображений, которые постоянны на каждом α -классе (т.е. равны для α -эквивалентных отображений), будем называть α -инвариантами. Для приложений α -инварианты представляют большой интерес. Примеры α -инвариантов будут приведены ниже.

Любое отображение $f \in H^G$ естественным образом определяет ядерное разбиение группы G на непересекающиеся прообразы $f^{-1}(v)$ элементов v из H , которые называются блоками ядерного разбиения. Набор мощностей блоков $\{\#f^{-1}(v) \mid v \in H\}$ будем называть весом отображения f , а числа $\#f^{-1}(v)$ — элементами веса. Очевидно, что мультимножество элементов веса отображения $f \in H^G$ является α -инвариантом. Поскольку $G = \bigcup_{v \in H} f^{-1}(v)$, то $\sum_{v \in H} \#f^{-1}(v) = \#G$. Сюръективные отображения, у которых все элементы веса равны, называются уравновешенными.

Определение 7.3. *Отображение $g : G' \rightarrow H'$ биморфно отображению $f : G \rightarrow H$, если существуют такие сюръективные гомоморфизмы $\omega^1 \in \text{Hom}(G, G')$, $\omega^2 \in \text{Hom}(H, H')$ и константы $u' \in G'$ и $v' \in H'$, что диаграмма*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \omega^1, u' \downarrow & & \uparrow \omega^2, v' \\ G' & \xrightarrow{g} & H' \end{array}$$

коммутативна, т.е.

$$\omega^2(f(x)) + v' = g(\omega^1(x) + u'). \quad (7.1)$$

Естественно считать, что если отображение $g : G' \rightarrow H'$ биморфно отображению $f : G \rightarrow H$, то отображения f и g "одинаково расположены" относительно $\text{Hom}(G, H)$ и $\text{Hom}(G', H')$ соответственно. Свойства отображений, которые сохраняются при биморфизмах, будем называть категориальными. Именно категориальные свойства связаны с "расположением" отображений относительно $\text{Hom}(G, H)$.

Пример 7.4. Простейшими представителями категориальных свойств групповых отображений являются:

1. $f(x) = \text{const}$ при любом $x \in G$,
2. $f \in \text{Hom}(G, H)$,
3. уравновешенность.

Необходимо отметить, что для булевых отображений категориальными являются, в частности, свойства, сводимые к свойствам координатных функций (см. [Ящ 97,1]). Известно, что свойства булевых отображений, перечисленные в примере 7.4, являются сводимыми.

Производной отображения $f \in H^G$ (для аддитивной записи групповых операций) по направлению $u \in G$ называется отображение

$$\frac{df}{du}(x) = f(x + u) - f(x), \quad (7.2)$$

справедливое при любом $x \in G$.

При этом производная по нулевому направлению является отображением, тождественно равным нулю. В мультипликативном случае, когда группа H совпадает с мультипликативной группой комплексных корней из единицы, свойства аппарата производных рассмотрены в §§2,3,4. Многие из обнаруженных свойств производных достаточно легко переносятся на случай произвольной группы H .

Пусть отображение $g : G' \rightarrow H'$ биморфно отображению $f : G \rightarrow H$, причем биморфизм реализуется с помощью пары гомоморфизмов (ω^1, ω^2) и пары констант (u', v') (см. 7.3). Несложно проверить, что в этом случае в любом направлении $c \in G$ справедливо следующее равенство производных

$$\omega^2 \left(\frac{df}{dc}(x) \right) = \frac{dg}{dw^2(c)} (\omega^1(x) + u').$$

Другими словами, в этом случае производная отображения g по направлению $\omega^1(c) \in G'$ биморфна производной отображения f по направлению $c \in G$. Отсюда следует, что если свойства отображений вводятся с помощью категориальных свойств производных, то они оказываются категориальными.

Воспользовавшись аппаратом производных (как ранее в §3) введем вложенную систему подгрупп в группе всех отображений H^G . Первым шагом в такой конструкции является отображение, тождественно равное нулю на G . Положим

$$RM_{-1}(G, H) = \{f \in H^G : f(x) = 0 \forall x \in G\}.$$

Далее семейство отображений определяется индуктивно

$$\text{RM}_{j+1}(G, H) = \left\{ f \in H^G : \frac{df}{du} \in \text{RM}_j(G, H) \ \forall u \in G \right\},$$

$$j = -1, 0, 1, 2, \dots$$

Нетрудно понять, что для каждого $j = 0, 1, 2, \dots$ семейство отображений $\text{RM}_j(G, H)$ является подгруппой группы H^G и $\text{RM}_j(G, H) \subseteq \text{RM}_{j+1}(G, H)$.

Легко проверить, что $\text{RM}_0(G, H)$ суть константы, а $\text{RM}_1(G, H)$ суть гомоморфизмы и их сдвиги:

$$\text{RM}_1(G, H) = \{ f \in H^G : f(x) = \omega(x) + v \ \forall x \in G, \quad \text{где } \omega \in \text{Hom}(G, H), v \in H \}. \quad (7.3)$$

Кроме того, очевидно, что свойство отображений "лежать в множестве $\text{RM}_j(G, H)$ " является категориальным при любом j .

Существуют группы G и H такие, что не всякое отображение из H^G лежит в некотором семействе $\text{RM}_j(G, H)$ (см. §3). Если же для отображения $f \in H^G$ существует номер j такой, что $f \in \text{RM}_j(G, H)$, то всякое отображение, α -эквивалентное отображению f , лежит в том же семействе $\text{RM}_j(G, H)$. В этом случае положим по определению

$$\deg(f) = \min \{ j : f \in \text{RM}_j(G, H) \},$$

$$\deg(0) = -\infty.$$

Очевидно, что $\deg(f)$ является α -инвариантом и определенным образом характеризует отклонение отображения f от $\text{RM}_1(G, H)$. Отметим, что определение $\deg(f)$ эквивалентно следующему включению:

$$f \in \text{RM}_{\deg(f)}(G, H) \setminus \text{RM}_{\deg(f)-1}(G, H).$$

Если $f \notin \text{RM}_j(G, H)$ для любого j , то для удобства можно положить $\deg(f) = \infty$. Конечность величины $\deg(f)$ является категориальным свойством.

В ряде случаев при изучении отображения $f \in H^G$ оказываются полезными следующие подмножества группы G :

$$L_f^j = \left\{ u \in G : \frac{df}{du} \in \text{RM}_j(G, H) \right\},$$

$$j = 0, 1, 2, \dots$$

Из легко проверяемого равенства

$$\frac{df}{d(u+v)}(x) = \frac{df}{du}(x) + \frac{df}{dv}(x+u)$$

следует, что все подмножества L_f^j являются подгруппами группы G . Следуя традиции, элементы группы L_f^0 будем называть гомоморфными трансляторами. Из введенных определений следует, что $L_f^j = G$ тогда и только тогда, когда $f \in \text{RM}_{j+1}(G, H)$. Очевидно, что при каждом $j = 0, 1, 2, \dots$ мощность группы L_f^j является α -инвариантом.

Веса всех производных отображения $f \in H^G$ по ненулевым направлениям можно расположить в виде таблицы R^f , состоящей из $\#G - 1$ строк и $\#H$ столбцов, в которой строка с номером $x \in G \setminus \{0\}$ состоит из элементов отображения $\frac{df}{dx}$, т.е. при каждом $x \in G \setminus \{0\}$ и $y \in H$

$$R_{x,y}^f = \# \left(\frac{df}{dx} \right)^{-1} (y).$$

Элементы таблицы R^f связаны определенными соотношениями. В частности, для любого $x \in G$ справедливо равенство

$$\sum_{y \in H} R_{x,y}^f = \#G. \quad (7.4)$$

В случае, когда отображение f является составной частью криптографического преобразования, таблица R^f имеет многочисленные приложения в дифференциальном (разностном) криптоанализе (см. основополагающую работу [BiSh 91,1]). Обычно таблицу R^f называют таблицей разностей. При оценке эффективности дифференциального метода криптографического анализа используется максимальный элемент таблицы разностей

$$\mu l(f) = \max_{\substack{x \in G \setminus \{0\} \\ y \in H}} R_{x,y}^f.$$

Легко проверить, что мультимножество элементов таблицы разностей отображения $f \in H^G$, а значит, и ее максимальный элемент $\mu l(f)$ являются α -инвариантами. Величина $\mu l(f)$ определенным образом характеризует отклонение отображения f от семейства $RM_1(G, H)$ (для функций $g \in RM_1(G, H)$ в каждой строке таблицы разностей содержится ровно один ненулевой элемент, равный $\#G$, поэтому выполнено равенство $\mu l(g) = \#G$).

Из введенных определений следует, что для некоторого элемента таблицы разностей R^f равенство $R_{u,v}^f = \#G$ выполнено тогда и только тогда, когда в строке с номером u таблицы R^f все элементы нулевые, кроме $R_{u,v}^f$. Значит элемент $u \in G$ является гомоморфным транслятором отображения f . В смысле характеристики μl максимально удаленными от $RM_1(G, H)$ и наиболее устойчивыми относительно дифференциального метода криптоанализа являются отображения, минимизирующие величину $\mu l(f)$. Из равенства 7.4 следует, что для любого отображения $f \in H^G$ выполнено неравенство $\mu l(f) \geq \#G/\#H$ (это неравенство нетривиально только в случае, когда $\#G \geq \#H$). Если $\#H$ делит $\#G$, то для достижимости указанной оценки необходимо выполнение равенств

$$R_{u,v}^f = \#G/\#H$$

при всех $u \in G \setminus \{0\}$ и $v \in H$, которые означают, что все производные отображения f по ненулевым направлениям являются уравновешенными отображениями.

В случае когда f — булева функция, последнее свойство эквивалентно тому, что функция f является бент-функцией (критерий Ротхауза, см. [Rot 76]). Следует подчеркнуть, что свойство "уравновешенность всех производных отображения по ненулевым направлениям" является, очевидно, категориальным свойством.

При синтезе отображений, используемых в средствах обеспечения информационной безопасности, часто используют так называемый метод "разветвления отображений". С примером одного из вариантов реализации этого метода можно ознакомиться в Приложении Б.

Кратко опишем указанный метод и введем параметры, описывающие свойства синтезируемых отображений. Важную роль в анализе математических моделей средств, обеспечивающих информационную безопасность, играют разнообразные соотношения между этими параметрами.

Пусть кроме групп G и H задана еще одна конечная группа K . Пусть также заданы $\rho \in \text{Hom}(G, K)$ и семейство отображений (не обязательно различных) $\{g_k \in \text{RM}_1(G, H) : k \in K\}$, заиндексированных элементами группы K . Отображение $f \in H^G$ определим равенством

$$f(x) = g_{\rho(x)}(x). \quad (7.5)$$

Будем говорить, что f — гомоморфное разветвление с разветвляющей группой K и разветвляющим отображением ρ . При этом отображения $g_k \in \text{RM}_1(G, H)$, $k \in K$, будем называть разветвляемыми.

Нетрудно понять, что любое отображение $f \in H^G$ можно представить в виде гомоморфного разветвления. Действительно, достаточно положить $K = G$, $\rho(x) = x$ и $g_k(x) \equiv f(k)$ для всех $x, k \in G$. Очевидно, что при изучении

гомоморфных разветвлений в качестве группы K достаточно рассматривать образ группы G при действии отображения $\rho : K = \text{Im}_\rho(G)$. Поэтому ниже (в данном параграфе) всюду будем считать, что гомоморфизм ρ сюръективен.

Отметим, что представление отображения в виде гомоморфного разветвления, вообще говоря не однозначно. Минимальный порядок разветвляющей группы по всем возможным представлениям отображения $f \in H^G$ в виде гомоморфного разветвления назовем индексом гомоморфности отображения f и будем обозначать через $\text{ih}(f)$. Легко видеть, что индекс гомоморфности отображения является α -инвариантом. Параметр $\text{ih}(f)$, как $\deg(f)$ и $\mu l(f)$, определенным образом характеризуют отклонение отображения f от семейства $\text{RM}_1(G, H)$ (для отображений $f \in \text{RM}_1(G, H)$, очевидно, выполнено равенство $\text{ih}(f) = 1$). В этом смысле максимально удаленными от $\text{RM}_1(G, H)$ являются отображения, максимизирующие величину $\text{ih}(f)$.

Между параметрами $\deg(f)$, $\mu l(f)$ и $\text{ih}(f)$ существуют определенные связи. Приведем пример связи между $\deg(f)$ и $\text{ih}(f)$ в случае функций на векторных пространствах. Пусть G — векторное пространство размерности s над конечным полем $\mathbb{F}$. Рассмотрим частный случай представления отображения $f : G \rightarrow \mathbb{F}$ в виде гомоморфного разветвления, т.е. случай, когда в представлении 7.5 группа K является также векторным пространством над полем $\mathbb{F}$ (такие разветвления называются линейными). В случае, когда $\#K = \text{ih}(f)$, размерность пространства K называется индексом линейности отображения f и обозначается $\text{ill}(f)$, т.е. $\text{ill}(f) = \dim K$. Введенные параметры $\text{ill}(f)$ и $\text{ih}(f)$ связаны равенством $\text{ih}(f) = p^{\text{ill}(f)}$, где p — характеристика поля $\mathbb{F}$.

Поскольку в этом случае любая функция $f \in \text{RM}_1(G, H)$ однозначно представима в виде

$$f(z_1, \dots, z_s) = a_1 z_1 + \dots + a_s z_s + b,$$

нетрудно убедиться в справедливости следующего утверждения.

Лемма 7.5. Пусть G — векторное пространство над полем $\mathbb{F}$, $p = \text{char}\mathbb{F}$. Тогда, если для отображения $f : G \rightarrow \mathbb{F}$ имеет место равенство $\text{ill}(f) = t$, то с помощью некоторой аффинной замены переменных отображение f может быть представлено в виде

$$\begin{aligned} f(x_1 \dots x_{s-t}, y_1 \dots y_t) = \\ = g_1(y_1 \dots y_t)x_1 + \dots + g_{s-t}(y_1 \dots y_t)x_{s-t} + h(y_1 \dots y_t). \end{aligned} \quad (7.6)$$

В этом случае справедливо неравенство

$$\deg(f) \leq 1 + (p - 1)\text{ill}(f).$$

Рассмотрим задачу о соотношении индекса гомоморфности и максимального элемента таблицы разностей. Ниже (в данном параграфе) мы получим оценки для $\text{ih}(f)$ при заданном $\mu l(f)$, и наоборот — оценки для $\mu l(f)$ при заданном $\text{ih}(f)$.

Теорема 7.6. Если $f \in H^G$, то

$$\mu l(f) \geq \frac{\#G}{\text{ih}(f)}. \quad (7.7)$$

Доказательство. Пусть отображение $f \in H^G$ представлено в виде гомоморфного разветвления (7.5) и порядок группы K минимален, т.е. $\#K = \text{ih}(f)$. В соответствии с равенством (7.3) каждое из отображений $g_k \in \text{RM}_1(G, H)$, $k \in K$, представим в виде

$$g_k(x) = \lambda_k(x) + m_k, \quad (7.8)$$

где $k \in K$, $\lambda_k \in \text{Hom}(G, H)$, $m_k \in H$. Рассмотрим выражение для производной отображения f по направлению $u \in G$:

$$\begin{aligned}
\frac{df}{du}(x) &= f(x+u) - f(x) = g_{\rho(x+u)}(x+u) - g_{\rho(x)}(x) = \\
&= \lambda_{\rho(x)+\rho(u)}(x) + \lambda_{\rho(x)+\rho(u)}(u) + m_{\rho(x)+\rho(u)} - \\
&\quad - \lambda_{\rho(x)}(x) - m_{\rho(x)}.
\end{aligned} \tag{7.9}$$

Сначала рассмотрим случай, когда ядро гомоморфизма ρ нетривиально, т.е. $\ker(\rho) \neq \{0\}$ и $\#G > \#K$. Пусть направление $u \in G \setminus \{0\}$ принадлежит ядру $\ker(\rho)$, т.е. $\rho(u) = 0$. Тогда из (7.9) следует, что

$$\frac{df}{du}(x) = \lambda_{\rho(x)}(u).$$

Для такого $u \in G \setminus \{0\}$, в частности, имеем

$$\ker(\rho) \subseteq \left\{ x \in G : \frac{df}{du}(x) = \lambda_0(u) \right\}.$$

Значит, для элемента $R_{u, \lambda_0(u)}^f$ таблицы разностей справедливо неравенство

$$R_{u, \lambda_0(u)}^f \geq \#\ker(\rho). \tag{7.10}$$

Поскольку

$$\#G = \#K \cdot \#\ker(\rho) = \text{ih}(f) \cdot \#\ker(\rho), \tag{7.11}$$

то неравенство (7.10) эквивалентно неравенству

$$R_{u, \lambda_0(u)}^f \geq \frac{\#G}{\text{ih}(f)}.$$

Отсюда с учетом неравенства

$$\mu l(f) \geq R_{u, \lambda_0(u)}^f$$

следует неравенство (7.7).

В случае, когда ядро гомоморфизма ρ тривиально, т.е. $\ker(\rho) = \{0\}$ и $\#G = \#K = \text{ih}(f)$, неравенство (7.7) становится очевидным. $\square$

Оценку (7.7), вообще говоря, нельзя улучшить, поскольку для $f \in \text{RM}_1(G, H)$ она достижима. Из теоремы 7.6 вытекает, что отображения с небольшими значениями $\mu l(f)$ надо искать среди отображений с большими значениями $\text{ih}(f)$.

Практический интерес представляет получение верхних оценок для элементов таблицы разностей $R_{u,v}^f$. При этом существенную роль играют условия, накладываемые на отображение f .

Теорема 7.7. *Если группа гомоморфных трансляторов отображения $f \in H^G$ тривиальна, то при любых $u \in G \setminus \{0\}$ и $v \in H$ справедливо неравенство*

$$R_{u,v}^f \leq \#G - \frac{d-1}{d} \cdot \frac{\#G}{\text{ih}(f)}, \quad (7.12)$$

где d — нетривиальный делитель числа $\#G/\text{ih}(f)$.

Доказательство. По определению для любых $u \in G \setminus \{0\}$ и $v \in H$ элемент таблицы разностей $R_{u,v}^f$ совпадает с числом решений относительно неизвестного $x \in G$ уравнения

$$\frac{df}{du}(x) = v. \quad (7.13)$$

Пусть, как и при доказательстве теоремы 7.6, отображение $f \in H^G$ представлено в виде гомоморфного разветвления (7.5), причем это представление выбрано таким образом, что мощность группы K минимальна, т.е. $\#K = \text{ih}(f)$. Далее пусть каждое разветвляемое отображение $g_k \in \text{RM}_1(G, H)$, где $k \in K$, представимо в виде (7.8). Тогда производная отображения f представляется в виде (7.9) и уравнение (7.13) принимает вид

$$\lambda_{\rho(x)+\rho(u)}(x) + \lambda_{\rho(x)+\rho(u)}(u) + m_{\rho(x)+\rho(u)} - \lambda_{\rho(x)}(x) - m_{\rho(x)} = v. \quad (7.14)$$

Положим $\rho(u) = r \in K$ и введем новый параметр $\rho(x) = k \in K$. Тогда рассматриваемое уравнение (7.13) эквивалентно объединению (в смысле объединения множества решений) следующих $\#K$ систем уравнений

$$\begin{cases} (\lambda_{k+r} - \lambda_k)(x) = v + m_k - m_{k+r} - \lambda_{k+r}(u) \\ \rho(x) = k. \end{cases} \quad (7.15)$$

Заметим, что систему уравнений (7.15) можно рассматривать как одно уравнение вида $\omega(x) = b$, где $\omega \in \text{Hom}(A, B)$, $A = G \times G$, $B = H \times K$ и $b \in B$. Гомоморфизм ω совпадает с покоординатным действием пары гомоморфизмов $(\lambda_{k+r} - \lambda_k, \rho)$ на $G \times G$. В этом смысле систему уравнений (7.15) можно считать "неоднородной линейной". Значит, в случае совместности системы (7.15) все ее решения образуют некоторый смежный класс по подгруппе $\ker(\rho) \cap \ker(\lambda_{k+r} - \lambda_k)$.

Обозначим через $S(u, v)$ множество значений параметра $k \in K$, при котором система (7.15) совместна, а через $T_{k, u, v}$ число решений системы (7.15). Поскольку при различных $k \in K$ множества решений системы (7.15) не пересекаются, то

$$R_{u, v}^f = \sum_{k \in K} T_{k, u, v}. \quad (7.16)$$

Для $T_{k, u, v}$ справедливо равенство

$$T_{k, u, v} = \begin{cases} \#(\ker(\rho) \cap \ker(\lambda_{k+r} - \lambda_k)), & \text{если } k \in S(u, v), \\ 0 & \text{в противном случае.} \end{cases}$$

Если $k \in S(u, v)$, то либо $\ker(\rho) \subseteq \ker(\lambda_{k+r} - \lambda_k)$ и тогда $T_{k, u, v} = \#\ker(\rho) = \#G/\text{ih}(f)$, либо $\ker(\rho) \not\subseteq \ker(\lambda_{k+r} - \lambda_k)$ и тогда $T_{k, u, v}$ не превосходит максимального порядка подгруппы группы $\ker(\rho)$. Поэтому $T_{k, u, v} \leq \frac{1}{d} \#G/\text{ih}(f)$, где d — наименьший нетривиальный делитель числа $\#G/\text{ih}(f)$.

Теперь зафиксируем $u \in G \setminus \{0\}$, $v \in H$ и рассмотрим два случая.

1. $\ker(\rho) \subseteq \ker(\lambda_{k+r} - \lambda_k)$ для любого $k \in S(u, v)$. В силу равенства (7.16) в этом случае получаем

$$R_{u,v}^f = \#S(u, v) \cdot \frac{\#G}{\text{ih}(f)}.$$

Если $S(u, v) = K$, то $\#S(u, v) = \text{ih}(f)$ и поэтому $R_{u,v}^f = \#G$. Значит u — гомоморфный транслятор отображения f .

Если же $S(u, v) \neq K$, то $\#S(u, v) \leq \text{ih}(f) - 1$. Поэтому

$$R_{u,v}^f \leq \#G - \frac{\#G}{\text{ih}(f)} < \#G - \frac{d-1}{d} \cdot \frac{\#G}{\text{ih}(f)}.$$

2. $\ker(\rho) \not\subseteq \ker(\lambda_{k'+r} - \lambda_{k'})$ при некотором $k' \in S(u, v)$. Тогда

$$T_{k',u,v} \leq \frac{1}{d} \cdot \frac{\#G}{\text{ih}(f)}.$$

В этом случае число таких k из множества $S(u, v)$, что $T_{k,u,v} = \#G/\text{ih}(f)$, не превосходит $\text{ih}(f) - 1$. Поэтому

$$R_{u,v}^f \leq (\text{ih}(f) - 1) \cdot \frac{\#G}{\text{ih}(f)} + \frac{1}{d} \cdot \frac{\#G}{\text{ih}(f)} = \#G - \frac{d-1}{d} \cdot \frac{\#G}{\text{ih}(f)}.$$

Таким образом, в любом случае либо отображение f имеет нетривиальный гомоморфный транслятор, либо выполнено требуемое неравенство. $\square$

Поскольку неравенство (7.12) справедливо при любых $u \in G \setminus \{0\}$ и $v \in H$, то аналогичная оценка справедлива и для $\mu l(f)$.

Следствие 7.8. *Если группа гомоморфных трансляторов отображения $f \in H^G$ тривиальна, то*

$$\mu l(f) \leq \#G - \frac{d-1}{d} \cdot \frac{\#G}{\text{ih}(f)}, \quad (7.17)$$

где d — наименьший нетривиальный делитель числа $\#G/\text{ih}(f)$.

§8 Невырожденные булевы функции

Пусть $\mathbb{F}_2$ — поле Галуа из двух элементов. Рассмотрим множество групповых отображений

$$\mathcal{F}_n = \{f : G \rightarrow H\}, n \in \mathbb{N},$$

где $G = \mathbb{F}_2^n$, $H = \mathbb{F}_2$ — элементарные абелевы 2-группы. Групповую операцию для этих групп будем обозначать " $\oplus$ " — знак покомпонентного суммирования по модулю 2 наборов одинаковой длины. Исторически отображения из множества $\mathcal{F}_n$ называют булевыми функциями. В исследованиях свойств функций из $\mathcal{F}_n$ использовались различные их представления (нормальные формы).

Простейшим представлением булевой функции является ее табличное представление, используемое как в теоретических исследованиях (например, в теории кодирования), так и в технических описаниях разнообразных дискретных устройств. Эффективными (с точки зрения результатов исследований) показали себя конъюнктивная и дизъюнктивная нормальная формы ([Ябл 10]). В приложениях, связанных с обеспечением информационной безопасности, наибольшее распространение получили следующие представления:

- алгебраическая нормальная форма (АНФ - полиномы в кольце $R_n = \mathbb{F}_2[x_1, \dots, x_n] / (x_1^2 \oplus x_1, \dots, x_n^2 \oplus x_n)$, называемые также полиномами Жегалкина) ([ЛССЯ 15]);
- числовая нормальная форма (ЧНФ - полиномы в кольце $\mathbb{Z}[x_1, \dots, x_n]$ ([ЛССЯ 15]);
- спектральная форма (набор спектральных коэффициентов Фурье-Адамара, являющийся разложением функции по характерам элементарной абелевой 2-группы).

В данном параграфе для булевых функций будет рассмотрена еще одна полезная нормальная форма.

Будем рассматривать представление булевых функций в алгебраической нормальной форме (АНФ). Для любого $f \in \mathcal{F}_n$ через $\deg(f)$ обозначим алгебраическую степень функции f , равную максимальной длине мономов, входящих в ее АНФ. Производной булевой функции f по направлению $u \in \mathbb{F}_2^n$ называют булеву функцию $\frac{df}{du}$, определяемую равенством

$$\frac{df}{du}(x) = f(x \oplus u) \oplus f(x).$$

При взятии производной ее алгебраическая степень уменьшается (по сравнению с $\deg(f)$) по крайней мере на единицу (т.к. старшие однородные формы функций $f(x \oplus u)$ и $f(x)$ равны.) Если известны все 2^n производных функции f , то функция восстанавливается с точностью до константы с помощью следующего равенства:

$$f(u) = \frac{df}{du}(0^n) \oplus f(0^n),$$

где $0^n(1^n) \in \mathbb{F}_2^n$.

Алгебраическая степень функции f равна r тогда и только тогда, когда алгебраическая степень всех ее производных не превышает $r - 1$ и существует направление, по которому производная имеет алгебраическую степень $r - 1$.

Для функции $f \in \mathcal{F}_n$ определим совокупность множеств L_f^r , $0 \leq r \leq \deg(f) - 1$ равенством

$$L_f^r = \left\{ u \in \mathbb{F}_2^n : \deg\left(\frac{df}{du}\right) \leq r \right\}.$$

Для булева случая Все множества L_f^r являются не только группами, но и векторными подпространствами $\mathbb{F}_2^n$ (см. [ЛССЯ 15]), причем

$$L_f^0 \leq L_f^1 \leq \dots \leq L_f^{\deg(f)-1} = \mathbb{F}_2^n.$$

Очевидно, что $L_f^{r-1} = \mathbb{F}_2^n$ тогда и только тогда, когда $\deg(f) \leq r$. Ранее исследовалось только подпространство L_f^0 (оно называлось пространством (группой) линейных трансляторов) и его подпространство $L_f^- = \{u \in \mathbb{F}_2^n : f(x \oplus u) = f(x)\}$, которое называлось группой инерции функции f в группе сдвигов (группе Джевонса), а направления $u \in L_f^-$ называются несущественными ($\mathbb{F}_2^n \setminus L_f^-$ — существенные направления). При взятии производной размерность пространства ее несущественных направлений увеличивается по крайней мере на единицу.

Определение 8.1. *Невырожденной назовем булеву функцию $f \in \mathcal{F}_n$, для которой $L_f^{\deg(f)-2} = \{0^n\}$.*

Другими словами, невырожденными называются такие булевы функции, для которых взятие производной по любому ненулевому направлению уменьшает степень нелинейности ровно на единицу.

Пусть $\deg(f) = r$. Обозначим через $[f]_r$ однородную форму степени r функции f , а через $\left[\frac{df}{du}\right]_{r-1}$ — однородную форму степени $r-1$ функции $\frac{df}{du}$. Справедливо следующее утверждение.

Предложение 8.2. *Отображение*

$$\mathcal{D} : (f, u) \rightarrow \left[\frac{df}{du}\right]_{r-1}$$

для $u \in \mathbb{F}_2$ и $\deg(f) = r$ является билинейным.

Доказательство. Линейность по f отображения $\mathcal{D}$ очевидна. Непосредственно из определения производной вытекает справедливость следующей цепочки равенств

$$\begin{aligned} \frac{df}{d(u \oplus v)}(x) &= \frac{df}{du}(x) \oplus \frac{df}{dv}(x \oplus u) = \\ &= \frac{df}{du}(x) \oplus \frac{df}{dv}(x) \oplus \frac{d^2 f}{dudv}(x). \end{aligned} \tag{8.1}$$

Поскольку $\deg \left(\frac{d^2 f}{du dv} \right) \leq r - 2$, то имеем

$$\left[\frac{df}{d(u \oplus v)} \right]_{r-1} (x) = \left[\frac{df}{du} \right]_{r-1} (x) \oplus \left[\frac{df}{dv} \right]_{r-1} (x).$$

Из последнего равенства следует справедливость утверждения. $\square$

Невырожденность булевых функций связана с отображением $\mathcal{D}$ следующим образом: подпространство $L_f^{\deg(f)-2}$ — это в точности ядро линейного отображения $\mathcal{D}$ при фиксированном f .

$$L_f^{\deg(f)-2} = \left\{ u \in \mathbb{F}_2^n : \mathcal{D}(f, u) = \left[\frac{df}{du} \right]_{r-1} = 0 \right\}.$$

Невырожденными являются те и только те булевы функции f , для которых $\mathcal{D}(f, u) \neq 0$ при всех ненулевых $u \in \mathbb{F}_2^n$, т.е. линейное отображение $\mathcal{D}$ при фиксированной f является невырожденным. Полезно отметить следующее легко проверяемое свойство отображения $\mathcal{D}$.

Предложение 8.3. *Для любой функции g при условии $\deg(g) \leq \deg(f) - 1$ и любого направления $u \in \mathbb{F}_2^n$ выполнено*

$$\mathcal{D}(f \oplus g, u) = \mathcal{D}(f, u).$$

Из предложения 8.3, в частности, следует, что вместе с функцией f невырожденной является любая функция $f \oplus g$, если $\deg(g) \leq \deg(f) - 1$. Таким образом, невырожденность булевой функции — это свойство, которое определяется только старшей однородной формой функции. Более того, легко видеть, что если $\deg(f) = r$, то

$$L_f^{r-2} = L_{[f]_r}^{r-2}.$$

Пусть $f(x) = \bigoplus_{u \in \mathbb{F}_2^n} c^f(u) x^u$ — А.Н.Ф. булевой функции f , где $x^u = x_1^{u_1} \cdot \dots \cdot x_n^{u_n}$, $\deg(f) = r$. Весом вектора $u \in \mathbb{F}_2^n$ будем называть число $\text{wt}(u)$ его единичных координат, а весом $\text{wt}(f)$ функции $f \in \mathcal{F}_n$ — число единиц в табличном

представлении этой функции. Через $e^i = 0^{i-1}10^{n-i}$, $i = 1, 2, \dots, n$ обозначим векторы канонического базиса пространства $\mathbb{F}_2^n$. Определим для функции f двоичные наборы длины $\binom{n}{r-1}$ вида $b^{(i)} = \{b_u^{(i)} : u \in \mathbb{F}_2^n, \text{wt}(u) = r-1\}$, $i = 1, 2, \dots, n$, где

$$b_u^{(i)} = \begin{cases} 0, & \text{если } u \succcurlyeq e^i, \\ c_{(u \oplus e^i)}^f, & \text{в противном случае.} \end{cases}$$

Лемма 8.4. *Для любой функции f из $\mathcal{F}_n$, $\deg(f) = r$ выполняется равенство*

$$\dim L_f^{r-2} = n - \text{rank} \{b^{(1)}, \dots, b^{(n)}\}.$$

Доказательство. Непосредственной проверкой получаем

$$\frac{d[f]_r}{de^i}(x) = \bigoplus_{\substack{u \in \mathbb{F}_2^n \\ \text{wt}(u)=r-1}} b_u^{(i)} x^u.$$

Для фиксированной функции f образ $\mathbb{F}_2^n$ при отображении $\mathcal{D}$ совпадает с линейной оболочкой, натянутой на n однородных форм алгебраической степени $r-1$, задаваемых наборами $b^{(1)}, \dots, b^{(n)}$. Из известного соотношения, связывающего размерности ядра и образа линейного отображения, получаем утверждение леммы. $\square$

Для однородных форм выполняется следующее важное и полезное свойство

Предложение 8.5. *Пусть $f(x_1, \dots, x_n)$ — однородная форма, $\deg(f) = r$. Тогда либо x_i несущественная переменная, либо*

$$\deg\left(\frac{df}{de_i}\right) = r-1.$$

Доказательство. Получается непосредственной проверкой. $\square$

Невырожденную однородную форму алгебраической степени r от n переменных будем для краткости называть невырожденной (n, r) -формой или, если параметры n и r не нужны, невырожденной формой.

Теорема 8.6. Пусть $f \in \mathcal{F}_n$, $\deg(f) = r$, $\dim L_f^{r-2} = n - k$, $\mathbb{F}_2^n = U \dot{+} W$ (т.е. $\mathbb{F}_2^n$ является прямой суммой подпространств U и W), $L_f^{r-2} = U$. Тогда $k \geq r$ и при любом выборе базисов в U и W функция $f(u, w)$ может быть представлена в виде

$$f(u, w) = g(u, v) \oplus h(w),$$

где $h(w)$ — невырожденная (k, r) -форма, $\deg(g) \leq r - 1$, причем $L_f^m = L_g^m$ для всех $m \leq r - 2$.

Доказательство. Справедливость утверждения теоремы вытекает из леммы 8.4. □

В [ЛСЯ 98] введено понятие RM-эквивалентности булевых функций.

Определение 8.7. Две булевы функции $f, g \in \mathcal{F}_n$, $\deg(f) = \deg(g) = r$ называются RM-эквивалентными, если они могут быть получены одна из другой с помощью аффинной замены переменных и прибавления функции, алгебраическая степень которой не превышает $r - 1$.

Из теоремы 8.6 вытекает следующее утверждение.

Следствие 8.8. Любая булева функция RM-эквивалентна некоторой невырожденной форме.

В заключение настоящего параграфа рассмотрим некоторые аспекты, касающиеся однородных форм и возникающие в задачах классификации булевых функций, приведения к невырожденной нормальной форме, а также при расчете их комбинаторных и криптографических параметров.

Нам потребуются некоторые понятия и факты об ассоциированных представлениях группы $GL(n, 2)$. Для заданных матрицы $A \in GL(n, 2)$ и числа r , $1 \leq r < n$ через $C_r(A)$ обозначим r -ю ассоциированную матрицу размера $\binom{n}{r} \times \binom{n}{r}$, которая составлена из всех миноров порядка r матрицы A . Строки и столбцы матрицы $C_r(A)$ занумерованы всеми сочетаниями из n по r , расположенными в лексикографическом порядке. Для ассоциированных матриц известно много интересных свойств, с которыми можно ознакомиться, например, в [Бел 76], [МаМи 72], [ВоКу 84]. Отображение $A \rightarrow C_r(A)$ является гомоморфизмом группы $GL(n, 2)$ в группу $GL\left(\binom{n}{r}, 2\right)$, называемым r -м ассоциированным представлением группы $GL(n, 2)$.

Пусть группа $GL(n, 2)$ действует на множестве $\mathcal{F}_n$ обычным образом:

$$f(x) \rightarrow f(Ax), A \in GL(n, 2), f \in \mathcal{F}_n.$$

Как и ранее, булевы функции, в полиномиальном представлении которых содержатся только мономы одинаковой степени, будем называть однородными формами. Однородная форма $\varphi \in \mathcal{F}_n$ алгебраической степени r задается набором коэффициентов $c^\varphi = (c_u^\varphi)$ длины $\binom{n}{r}$:

$$\varphi(x) = \bigoplus_{u \in V_n, \text{wt}(u)=r} c_u^\varphi x^u,$$

где $\text{supp}(u) = \{i_1, \dots, i_r\}$ и $x^u = x_{i_1} x_{i_2} \dots x_{i_r}$. Между всеми сочетаниями из n по r и всеми векторами $u \in V_n$ такими, что $\text{wt}(u) = r$, установлено естественное взаимно однозначное соответствие. Будем считать, что в наборе c^φ компоненты c_u^φ расставлены в соответствии с лексикографическим порядком сочетаний $(i_1, i_2, \dots, i_r)$ из n по r .

Каждая булева функция $f \in \mathcal{F}_n$, $\deg(f) = r$ единственным образом (при фиксированном базисе пространства V_n) представляется в виде суммы однород-

ных форм:

$$f(x) = [f(x)]_r \oplus [f(x)]_{r-1} \oplus \dots \oplus [f(x)]_1 \oplus [f(x)]_0,$$

где $[f(x)]_j$ — сумма мономов степени j в полиномиальном представлении функции f . Для однородных форм можно ввести следующее действие группы $GL(n,2)$:

$$\varphi(x) \rightarrow [\varphi(Ax)]_r, A \in GL(n,2),$$

если $\varphi(x)$ — однородная форма степени r . Покажем, что это действие порождает на пространстве коэффициентов однородных форм степени r следующее отображение:

$$c^\varphi \rightarrow C_r(A)^\top c^\varphi, A \in GL(n,2).$$

Лемма 8.9. Пусть $\varphi(x)$ — однородная форма степени r из $\mathcal{F}_n$:

$$\varphi(x) = \bigoplus_{u \in V_n, \text{wt}(u)=r} c_u^\varphi x^u.$$

Тогда для любой матрицы $A \in GL(n,2)$ выполнено равенство

$$[\varphi(Ax)]_r = \bigoplus_{v \in V_r, \text{wt}(v)=r} \left(C_r(A)^\top c^\varphi \right)_v x^v.$$

Доказательство. Пусть

$$A = (a_{ij}), i, j = 1, 2, \dots, n$$

$$C_r(A) = (A_{uv}), u, v \in V_n, \text{wt}(u) = \text{wt}(v) = r.$$

Если $x^u = x_{i_1} \cdot \dots \cdot x_{i_r}$, то очевидно

$$\begin{aligned} [(Ax)^u]_r &= [(a_{i_1 1}x_1 \oplus \dots \oplus a_{i_1 n}x_n) \cdot \dots \cdot (a_{i_r 1}x_1 \oplus \dots \oplus a_{i_r n}x_n)]_r = \\ &= \bigoplus_{v \in V_n, \text{wt}(v)=r} A_{uv} x^v. \end{aligned}$$

Подставляя эти равенства в выражение для $\varphi(x)$, получаем, что

$$\begin{aligned} [\varphi(Ax)]_r &= \bigoplus_{u \in V_n, \text{wt}(u)=r} c_u^\varphi [(Ax)^u]_r = \\ &= \bigoplus_{u \in V_r, \text{wt}(u)=r} c_u^\varphi \left(\bigoplus_{v \in V_n, \text{wt}(v)=r} A_{uv} x^v \right) = \\ &= \bigoplus_{v \in V_r, \text{wt}(v)=r} \bigoplus_{u \in V_r, \text{wt}(u)=r} A_{uv} c_u^\varphi x^u = \\ &= \bigoplus_{v \in V_r, \text{wt}(v)=r} (C_r(A^\top) c^\varphi)_v x^v. \end{aligned}$$

□

Необходимо отметить, что подробнее информацию о некоторых свойствах ассоциированных представлений группы $\text{GL}(n, 2)$ можно найти в [ЛСЯ 00, 2].

§9 Пространства линейных трансляторов и пустые секции Фурье-кластеризации булевых функций

В данном параграфе будет рассмотрен еще один аспект сущностного содержания пространств (групп) линейных трансляторов (см §8). В работе [ЛФЯ 18, 1] рассмотрен вариант Фурье-кластеризации булевых функций на основе естественных геометрических представлений этих функций как точек на гиперсфере в евклидовом пространстве. В отличие от классификации булевых функций на основе некоторой групповой эквивалентности, кластеризация на

гиперсфере представляет собой процесс локализации данной булевой функции на области гиперсферы, определяемой ортантом, задаваемым знаками коэффициентов Уолша булевой функции.

Пусть f — булева функция из $\mathcal{F}_n$ и $m = 2^n$. Сепктр Уолша функции f обозначим через $W_f = \{W_f(u) \mid u \in V_n = \mathbb{F}_2^n\}$, где

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle u, x \rangle}. \quad (9.1)$$

Порядок расположения $W_f(u)$ в W_f соответствует лексикографическому порядку индексирующих векторов u из V_n . Ясно, что выражение (9.1) представляет преобразование Фурье экспоненты булевой функции f . Воспользовавшись равенством Парсеваля

$$\sum_{u \in V_n} W_f^2(u) = 2^{2^n}, \quad (9.2)$$

отобразим булеву функцию f в точку $(m - 1)$ -мерной сферы $S^{m-1} \subset \mathbb{R}^m$ с центром в 0^m :

$$f \longrightarrow x^f = W_f \in \mathbb{R}^m.$$

Функции, имеющие хотя бы один нулевой коэффициент Уолша, будем называть граничными функциями. Остальные функции назовем внутренними.

Пусть $g \in \mathcal{F}_n$ и $(-1)^g = \left((-1)^{g(u^0)}, (-1)^{g(u^1)}, \dots, (-1)^{g(u^{m-1})} \right)$ — таблица значений экспонент этой функции (порядок расположения $(-1)^{g(u)}$ в $(-1)^g$ соответствует лексикографическому порядку индексирующих векторов u из V_n .) Каждая функция g своей таблицей $(-1)^g$ однозначно задает один из 2^m ортантов пространства $\mathbb{R}^m$ — непересекающихся множеств, высекаемых в $\mathbb{R}^m$ ортогональными координатным осям гиперплоскостями $x_j = 0, 0 \leq j \leq m - 1$, или иначе говоря, являющихся пересечением m полупространств $\pm x_j > 0$. Заметим, что мы не включаем в ортант границу — часть гиперплоскостей, то есть считаем, что все координаты любой точки ортанта — ненулевые. Мы можем пронумеровать ортанты элементами множества $\mathcal{F}_n$ и ввести понятие секции с

номером g — "сферического" m -угольника (без границ) на S^{m-1} , получаемого пересечением сферы с соответствующим ортантом:

$$S(g) = S^{m-1} \cap \left\{ x \in \mathbb{R}^m \mid \text{sgn}(x_j) = (-1)^{g(u^j)}, 0 \leq j \leq m-1 \right\}, \quad (9.3)$$

где

$$\text{sgn}(r) = \begin{cases} 1, & \text{если } r > 0; \\ 0, & \text{если } r = 0; \\ -1, & \text{если } r < 0. \end{cases}$$

Элементы секции $S(g)$ будем называть ее внутренними точками, а ее границей — множество

$$BS(g) = \left(S^{m-1} \cap \left\{ x \in \mathbb{R}^m \mid \bigwedge_{j=0}^{m-1} (x_j \cdot (-1)^{g(u^j)} \geq 0) \right\} \right) \setminus S(g), \quad (9.4)$$

элементы которого назовем граничными точками секции.

В случае если внутренняя точка x из $S(g)$ представляет собой некоторую булеву функцию f (т.е. $x = x^f$), то

$$\text{sgn}(W_f(u^j)) = (-1)^{g(u^j)}, 0 \leq j \leq m-1.$$

Для множества булевых функций, отображаемых в секцию $S(g)$, введем обозначение

$$D(g) = \left\{ f \in \mathcal{F}_n \mid \text{sgn}(W_f(u^j)) = (-1)^{g(u^j)}, 0 \leq j \leq m-1 \right\}.$$

Целью кластеризации является исследование алгебраических, комбинаторных и криптографических свойств семейства $\{(S(g), D(g)), g \in \mathcal{F}_n\}$. В част-

ности, одним из важнейших элементов кластеризации является описание "пустых секций", т.е. секций $S(g)$, для которых не существует булевой функции $f \in \mathcal{F}_n$ такой, что

$$\operatorname{sgn}(W_f(u^j)) = (-1)^{g(u^j)}, 0 \leq j \leq m-1.$$

Справедливо следующее утверждение.

Теорема 9.1. *Если $g \in \mathcal{F}_n$ обладает линейным транслятором, то $D(g) = \emptyset$.*

Доказательство. Если выполнено условие теоремы, то для некоторых $u \neq 0^n$ и $\varepsilon_u \in \mathbb{F}_2$ выполнено условие

$$g(v \oplus u) = g(v) \oplus \varepsilon_u$$

для любых $v \in V_n$. Предположим противное, что $D(g) \neq \emptyset$ и $f \in D(g)$. Тогда для функции f выполнены условия: $W_f(v) \neq 0$ и $W_f(v) = (-1)^{g(v)} |W_f(v)|$ для всех $v \in V_n$.

Воспользуемся соотношением ортогональности для коэффициентов Уолша произвольной функции f из $\mathcal{F}_n$ ([ЛССЯ 15])

$$\sum_{v \in V_n} W_f(v) W_f(v \oplus u) = \begin{cases} 0, & \text{если } u \neq 0^n; \\ m^2, & \text{если } u = 0^n. \end{cases} \quad (9.5)$$

Преобразуем левую часть соотношения (9.5):

$$\begin{aligned} \sum_{v \in V_n} W_f(v) W_f(v \oplus u) &= \sum_{v \in V_n} (-1)^{g(v)} |W_f(v)| (-1)^{g(v) \oplus \varepsilon_u} |W_f(v \oplus u)| = \\ &= (-1)^{\varepsilon_u} \sum |W_f(v)| |W_f(v \oplus u)| \neq 0, \end{aligned}$$

так как все слагаемые в последней сумме положительны. Полученное противоречие с (9.5) доказывает теорему. $\square$

Известно (см., например, [ЛССЯ 15]), что любая квадратичная булева функция либо имеет линейный транслятор, либо является бент-функцией. Из этого факта и предыдущей теоремы вытекает следующее утверждение.

Лемма 9.2. *Пусть $g \in \mathcal{F}_n$ — квадратичная функция. Для четных n множество $D(g)$ непусто тогда и только тогда, когда g — бент-функция. Для нечетных n всегда $D(g) = \emptyset$.*

§10 Δ -эквивалентность и глобальные лавинные характеристики булевых функций

Взаимная корреляция и автокорреляция булевых функций являются одними из важнейших инструментов в исследовании алгебраических, комбинаторных и криптографических свойств булевых функций. С их помощью можно характеризовать различные свойства булевых функций и устанавливать между этими свойствами содержательные связи. В данном параграфе будут рассмотрены соотношения, связывающие глобальные лавинные характеристики пары булевых функций с их обобщенной глобальной лавинной характеристикой, а также показана неизменность обобщенной глобальной лавинной характеристики для любой пары булевых функций, взятых из двух фиксированных классов Δ -эквивалентности.

Напомним некоторые необходимые нам понятия и результаты.

Определение 10.1. *Функция взаимной корреляции булевых функций $f, g \in \mathcal{F}_n$ — это определенная на $\mathbb{F}_2^n$ целочисленная функция*

$$\Delta_{f,g}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus g(x \oplus u)}, u \in \mathbb{F}_2^n.$$

В случае $f = g$ рассматривают целочисленную функцию

$$\Delta_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus u)}, u \in \mathbb{F}_2^n,$$

называемую функцией автокорреляции.

Нам потребуется хорошо известное утверждение о взаимной корреляции (автокорреляции), описывающее связи между значениями функции взаимной корреляции булевых функций и их коэффициентами Уолша.

Теорема 10.2 ([ЛССЯ 15]). Пусть $f, g \in \mathcal{F}_n$. Тогда для любого $u \in \mathbb{F}_2^n$ выполняется соотношение

$$\sum_{v \in \mathbb{F}_2^n} \Delta_{f,g}(v) (-1)^{\langle u, v \rangle} = W_f(u) W_g(v).$$

Следствие 10.3. Для любой $f \in \mathcal{F}_n$ и любого $u \in \mathbb{F}_2^n$ выполняется соотношение

$$\sum_{v \in \mathbb{F}_2^n} \Delta_f(v) (-1)^{\langle u, v \rangle} = W_f^2(u).$$

Используя известное свойство матрицы Адамара типа Сильвестра, из теоремы 10.2 и следствия 10.3 нетрудно вывести следующее полезное утверждение.

Следствие 10.4. Пусть $f, g \in \mathcal{F}_n$. Для любого $u \in \mathbb{F}_2^n$ справедливы равенства

$$\sum_{u \in \mathbb{F}_2^n} \Delta_{f,g}^2(u) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} W_f^2(u) W_g^2(u) \text{ и } \sum_{u \in \mathbb{F}_2^n} \Delta_f^2(u) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} W_f^4(u).$$

На основе понятия автокорреляционной функции определяется криптографическая характеристика булевой функции $f \in \mathcal{F}_n$ ([ЛССЯ 15]):

$$\sigma_f = \sum_{u \in \mathbb{F}_2^n} \Delta_f^2(u),$$

называемая глобальной лавинной характеристикой. Существует также соответствующее понятие обобщенной глобальной лавинной характеристики, введенное

в [ZXX 10] для функции взаимной корреляции:

$$\sigma_{f,g} = \sum_{u \in \mathbb{F}_2^n} \Delta_{f,g}^2(u).$$

Как видим, следствие 10.4 дает выражение параметров σ_f и $\sigma_{f,g}$ через коэффициенты Уолша функций f и g .

Определение 10.5. Будем говорить, что функции $f, g \in \mathcal{F}_n$ — Δ - эквивалентны и писать $\triangleq$, если их функции автокорреляции совпадают: $\Delta_f = \Delta_g$.

Из следствия 10.3 вытекает, что условие $f \triangleq g$ равносильное равенству $|W_f| = |W_g|$ (как функций). Справедливо следующее утверждение.

Теорема 10.6. Для произвольных $f, g \in \mathcal{F}_n$ справедливо неравенство

$$\sigma_{f,g} \leq \sqrt{\sigma_f \cdot \sigma_g},$$

причем равенство здесь достигается тогда и только тогда, когда $f \triangleq g$.

Доказательство. Используем первое равенство из следствия 10.4, затем неравенство Гельдера, а потом второе равенство из следствия 10.4, чтобы получить требуемое неравенство:

$$\begin{aligned} 2^n \sum_{v \in \mathbb{F}_2^n} \Delta_{f,g}^2(v) &= \sum_{v \in \mathbb{F}_2^n} W_f^2(v) W_g^2(v) \leq \\ &\leq \sqrt{\sum_{v \in \mathbb{F}_2^n} W_f^4(v)} \cdot \sqrt{\sum_{v \in \mathbb{F}_2^n} W_g^4(v)} = \\ &= \sqrt{2^n \sum_{v \in \mathbb{F}_2^n} \Delta_f^2} \cdot \sqrt{2^n \sum_{v \in \mathbb{F}_2^n} \Delta_g^2}. \end{aligned}$$

Пусть в доказанном соотношении имеет место равенство. Известно, что в нашем случае равенство в соответствующем неравенстве Гельдера достигается

тогда и только тогда, когда

$$W_f^2(u) = C \cdot W_g^2(u),$$

где множитель C постоянен по всем $u \in \mathbb{F}_2^n$. Тогда из равенства Парсеваля для коэффициентов Уолша булевых функций следует, что $C = 1$. Таким образом, $|W_f| = |W_g|$ (как функции), что завершает доказательство. $\square$

Теперь докажем утверждение, описывающее влияние Δ -эквивалентности на обобщенную глобальную лавинную характеристику булевых функций. Справедливо следующее утверждение.

Теорема 10.7. Пусть $f_1, f_2, g_1, g_2 \in \mathcal{F}_n$ и $f_1 \triangle f_2, g_1 \triangle g_2$. Тогда

$$\sigma_{f_1, g_1} = \sigma_{f_2, g_2}.$$

Доказательство. Воспользовавшись следствием 10.4, имеем

$$2^n \sum_{u \in \mathbb{F}_2^n} \Delta_{f_1, g_1}^2(u) = \sum_{u \in \mathbb{F}_2^n} W_{f_1}^2(u) W_{g_1}^2(u),$$

$$2^n \sum_{u \in \mathbb{F}_2^n} \Delta_{f_2, g_2}^2(u) = \sum_{u \in \mathbb{F}_2^n} W_{f_2}^2(u) W_{g_2}^2(u).$$

Поскольку $f_1 \triangle f_2, g_1 \triangle g_2$, то $|W_{f_1}| = |W_{f_2}|, |W_{g_1}| = |W_{g_2}|$ как функции. Следовательно,

$$\sum_{u \in \mathbb{F}_2^n} W_{f_1}^2(u) W_{g_1}^2(u) = \sum_{u \in \mathbb{F}_2^n} W_{f_2}^2(u) W_{g_2}^2(u)$$

что завершает доказательство. $\square$

Глава 2. О связях алгебраических, комбинаторных и криптографических свойств булевых функций со свойствами их сужений

§11 Сужения булевых функций

В математических моделях, использующих групповые отображения, наиболее часто рассматриваются отображения, определенные на элементарных абелевых p -группах (p — простое). Среди таких отображений исторически первыми рассматривались булевы отображения (т.е. отображения элементарных абелевых 2-групп).

Учитывая также возможность двоичного кодирования произвольного отображения конечных абелевых групп, мы будем рассматривать сужения (ограничения) булевых функций и отображений (как систем булевых функций). Термин "ограничение" булевой функции также имеет достаточно широкое распространение (см., например [Бур 09], [Коло14]). Мы далее будем пользоваться термином "сужение" булевой функции.

Пусть $\mathcal{F}_n$ как и ранее - множество полностью определенных булевых функций от n переменных; $\mathcal{D}$ — область (подмножество) в $\mathbb{F}_2^n$ и $\mathcal{F}_n(\mathcal{D})$ — множество всех частичных булевых функций от n переменных, определенных на $\mathcal{D}$. Пусть f произвольная функция из $\mathcal{F}_n$. Сужением функции f на области $\mathcal{D} \subseteq \mathbb{F}_2^n$ называется частичная функция h из $\mathcal{F}_n(\mathcal{D})$ такая, что при всех $x \in \mathcal{D}$ справедливо равенство $f(x) = h(x)$. Сужение функции f на область $\mathcal{D}$ будем обозначать через $f_{\mathcal{D}}$. Очевидно, что при фиксированных f и $\mathcal{D}$ частичная функция $f_{\mathcal{D}}$ определяется однозначно.

Пусть $F : \mathcal{F}_n(\mathcal{D}) \rightarrow \mathcal{F}_n$ такое отображение, что для любой $g \in \mathcal{F}_n(\mathcal{D})$ справедливо равенство $(F(g))_{\mathcal{D}} = g$. Функцию $F(g)$ назовем продолжением функции g на $\mathbb{F}_2^n$ относительно отображения F .

Нетрудно видеть, что отображение F может быть определено неоднозначно. Приведем пример конкретного способа построения отображения F . Пусть $\mu : \mathcal{F}_n \rightarrow \mathbb{R}^+$ — произвольная вычислимая положительная функция, определенная на $\mathcal{F}_n$. Распространим μ на частичные булевы функции. Пусть $\mathcal{D} \subseteq \mathbb{F}_2^n$ и $g : \mathcal{D} \rightarrow \mathbb{F}_2$. Значение μ на g определим следующим образом:

$$\mu(g) = \min \{ \mu(f) : f \in \mathcal{F}_n, f_{\mathcal{D}} = g \}.$$

Линейно упорядочим все функции из $\mathcal{F}_n$. Сделать это можно разными способами, например, сравнивая вектора значений функций как целые числа, записанные в двоичной системе счисления. Каждой частичной функции $g : \mathcal{D} \rightarrow \mathbb{F}_2$ поставим в соответствие функцию f' из $\mathcal{F}_n$, являющуюся минимальной (относительно указанного линейного порядка) среди таких функций f , что $f_{\mathcal{D}} = g$ и $\mu(f) = \mu(g)$. Полагаем $F(g) = f'$. Построенное продолжение (функцию $F(g)$) называют минимальным продолжением функции g относительно функции μ .

Введенное понятие "продолжения" позволяет рассматривать частичные булевы функции как полностью определенные.

В различных разделах математики выделяются функциональные классы с целью исследования свойств их представителей. При этом сужения изучаемых функций играют важную роль, поскольку они в ряде случаев могут однозначно определять исходные функции. В качестве примера можно привести хорошо известный из анализа факт: любой вещественный многочлен алгебраической степени $d - 1$ однозначно определяется по своим значениям в d точках, не лежащих на кривой $(d - 2)$ степени (т.е. вся информация о полиноме содержится в конечном числе точек области определения отображения, задаваемого полиномом).

Для булевых функций нетрудно привести аналогичные примеры.

Произвольная (отличная от константы) аффинная булева функция от n переменных может быть восстановлена по значениям этой функции на множестве векторов мощности $n + 1$, порождающем все пространство $\mathbb{F}_2^n$.

Любая булева функция от n переменных алгебраической степени d , однозначно определяется по своим значениям в шаре радиуса d с центром в произвольном наборе из $\mathbb{F}_2^n$ (соотношения Мебиуса, см. [ЛССЯ 15]).

Произвольная булева функция, сложность которой удовлетворяет неравенству $L(f) \leq 2^{n-5}/n$, полностью определяется своими значениями на некоторых четырех областях $D_1, D_2, D_3, D_4 \subseteq \mathbb{F}_2^n$ (см. [Чаш 97])¹.

В ходе анализа математических моделей средств информационной безопасности важное значение имеют исследования сужений групповых функций, обладающих дополнительным свойством "аффинности", т.е. совпадением на некоторой области сужения исследуемой функции с сужением (на этой же области) подходящей аффинной функции. Области, обладающие данным свойством, называются локальными аффинностями булевых функций. Корректное определение этого понятия будет дано в §13. Имеется значительное число публикаций с результатами исследований локальных аффинностей основных криптографических классов булевых функций и отображений (см., например, [CDDL 06], [Бур 09], [Колю14], [Буг 15]).

Локальные аффинности играют значительную роль при построении эффективных алгоритмов обращения групповых функций. Одна из особенностей областей, для которых рассматриваются сужения функций, состоит в том, что они представляют собой плоскости пространства $\mathbb{F}_2^n$ (т.е. смежные классы по некоторым подпространствам).

¹Под сложностью $L(f)$ булевой функции f автор [Чаш 97] подразумевает сложность минимальной схемы, реализующей эту функцию в базисе $\{\&, \wedge, \neg\}$

§12 Наследование комбинаторных и спектральных свойств при сужении булевых функций. (H, u) -стабильность.

Разнообразные приложения в теории кодирования и криптологии получили некоторые свойства булевых функций, сохраняемые их сужениями. Например, концепция корреляционной иммунности (в одном из вариантов ее характеристики) определяется через сохранение доли значений функции при фиксации части переменных (подробнее см. [ЛССЯ 15]).

В общей постановке "наследование" некоторого свойства может быть определено следующим образом:

- фиксируется некоторое свойство $\mathcal{P}$ булевых функций;
- для данной булевой функции f из $\mathcal{F}_n$ и данного подпространства H пространства $\mathbb{F}_2^n$ рассматривается множество всех сужений булевой функции f на смежные классы $\mathbb{F}_2^n$ по H ;
- если сама функция f и все $2^{n-\dim H}$ ее сужений обладают свойством $\mathcal{P}$, то естественно говорить, что свойство $\mathcal{P}$ наследуется при данных сужениях функции f .

Если $u \in \mathbb{F}_2^n$ и M — подмножество $\mathbb{F}_2^n$, то будем использовать обозначение

$$u \oplus M = \{u \oplus x \mid x \in M\}.$$

Подпространством, натянутым на вектор $u \in \mathbb{F}_2^n$ и подпространство $H \subseteq \mathbb{F}_2^n$ будем называть минимальное (по включению) подпространство в $\mathbb{F}_2^n$, содержащее и вектор u , и подпространство H . Нам удобно будет отождествлять фактор-пространство $\mathbb{F}_2^n/H$ с некоторым фиксированным (полным) набором представителей смежных классов пространства $\mathbb{F}_2^n$ по подпространству H (трансверсалью $\mathbb{F}_2^n/H$). Таким образом, запись $u \in \mathbb{F}_2^n/H$ подразумевает, что $u \in \mathbb{F}_2^n$. Если H — некоторое подпространство в $\mathbb{F}_2^n$, то символом $H^\perp$ будем обозначать ортогональ-

ное к H подпространство

$$H^\perp = \{v \in \mathbb{F}_2^n \mid \langle v, x \rangle = 0 \text{ для всех } x \in H\},$$

где

$$\langle x, y \rangle = x_1 y_1 \oplus \dots \oplus x_n y_n$$

— скалярное произведение векторов x и y из $\mathbb{F}_2^n$. Для произвольного подпространства $H \subseteq \mathbb{F}_2^n$, $\dim H = t$ выполнено соотношение ортогональности для характеров

$$\sum_{x \in H} (-1)^{\langle u, x \rangle} = \begin{cases} 2^t, & \text{если } u \in H^\perp, \\ 0, & \text{если } u \notin H^\perp. \end{cases}$$

Пример 12.1. Булева функция f из $\mathcal{F}_n$ называется корреляционно-иммунной порядка t , $1 \leq t < n$, если при любой фиксации k , $k \leq t$ любых переменных для полученной подфункции f' от $n - k$ переменных выполнено равенство

$$\frac{\text{wt}(f')}{2^{n-k}} = \frac{\text{wt}(f)}{2^n}.$$

В данном случае свойство функции f быть корреляционно-иммунной порядка t задается наследованием свойства $\mathcal{P}_n$, состоящего в совпадении относительного веса функции f и относительных весов сужений этой функции на смежные классы относительно подпространств $\{H_{i_1 \dots i_k} \mid k \leq t, 1 \leq i_1 < \dots < i_k \leq n\}$, где

$$H_{i_1 \dots i_k} = \{x \in \mathbb{F}_2^n \mid x_{i_1} = \dots = x_{i_k} = 0\}.$$

В данном параграфе будет использовано понятие частичного преобразования Фурье (Уолша-Адамара) для экспонент булевых функций. В связи с этим

нам будет удобно перейти (в этом параграфе) на классическое обозначение (см. §2) для коэффициентов Уолша-Адамара экспонент булевых функций.

Тогда

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle u, x \rangle}, u \in \mathbb{F}_2^n$$

и

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in \mathbb{F}_2^n} W_f(u) (-1)^{\langle x, u \rangle}, x \in \mathbb{F}_2^n$$

преобразование Уолша-Адамара и обратное преобразование Уолша-Адамара функции f соответственно. Определим частичное преобразование Уолша-Адамара по области $\mathcal{D} \subseteq \mathbb{F}_2^n$ для булевой функции f соотношением

$$W_{f_{\mathcal{D}}}(u) = \sum_{x \in \mathcal{D}} (-1)^{f(x) \oplus \langle x, u \rangle}, u \in \mathbb{F}_2^n.$$

Ниже будет использовано соотношение, связывающее автокорреляционную функцию $\Delta_f(u)$ и коэффициенты Уолша-Адамара:

$$\begin{aligned} \Delta_f(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus u)} = \\ &= 2^{-n} \sum_{x \in \mathbb{F}_2^n} W_f^2(x) (-1)^{\langle u, x \rangle}. \end{aligned}$$

Определение 12.2. Булеву функцию f из $\mathcal{F}_n$ назовем (H, u) -стабильной, $H \subset \mathbb{F}_2^n$, $u \in \mathbb{F}_2^n$, если

$$\frac{W_{f_{x \oplus H}}(u)}{\#H} = \frac{W_f(u)}{2^n}$$

для любого $x \in \mathbb{F}_2^n$.

Для любой булевой функции f и вектора u из $\mathbb{F}_2^n$ определим семейство подпространств

$$\mathcal{H}_{f,u} = \{H \subset \mathbb{F}_2^n \mid f - (H, u)\text{-стабильная функция}\}.$$

Наибольший интерес представляют две задачи: проверка свойства (H, u) -стабильности и описание семейства $\mathcal{H}_{f,u}$. Заметим вначале, что можно ограничиться изучением случая $u = 0^n$, поскольку очевидно следующее утверждение.

Предложение 12.3. *Функция $f(x)$ является (H, u) -стабильной тогда и только тогда, когда $(H, 0^n)$ -стабильна функция $f(x) \oplus \langle u, x \rangle$.*

Непосредственно из определения $(H, 0^n)$ -стабильной функции вытекает следующее свойство.

Лемма 12.4. *Если булева функция $f(x)$ из $\mathcal{F}_n$ является $(H, 0^n)$ -стабильной, то*

$$W_f(0^n) \equiv 0 \pmod{2^{n-t+1}},$$

где $t = \dim H$.

Доказательство. Если функция $f(x)$ является (H, u) -стабильной, то для любого $x \in \mathbb{F}_2^n$

$$\sum_{y \in x \oplus H} (-1)^{f(y)} = W_f(0^n) / 2^{n-t}.$$

Поскольку

$$\sum_{y \in x \oplus H} (-1)^{f(y)} \equiv 0 \pmod{2},$$

справедливо сравнение

$$W_f(0^n) \equiv 0 \pmod{2^{n-t+1}}.$$

□

Пример 12.5. Пусть функция $f \in \mathcal{F}_n$ является $(H, 0^n)$ -стабильной, причем $\dim H = 1$, т.е. $H = \{0^n, v\}$, $0^n \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^n \setminus \{0^n\}$. По определению 12.2 это

равносильно тому, что для любого вектора $x \in \mathbb{F}_2^n$

$$(-1)^{f(x)} + (-1)^{f(x \oplus v)} = c,$$

где c — постоянная. Несложно видеть, что это возможно лишь в двух случаях, когда функция f является постоянной и когда вектор v является линейным транслятором функции f , то есть $f(x \oplus v) = f(x) \oplus 1$ для любого вектора $x \in \mathbb{F}_2^n$. Отметим, что если вектор v является линейным транслятором функции f , т.е. $f(x \oplus v) = f(x) \oplus \varepsilon$ для любого вектора $x \in \mathbb{F}_2^n$, $\varepsilon \in \{0,1\}$, то требуется, чтобы было выполнено более слабое условие $|(-1)^{f(x)} + (-1)^{f(x \oplus v)}| = c$, где c — постоянная.

Для получения критериев $(H, 0^n)$ -стабильности будут полезны два соотношения, связывающие некоторые суммы значений автокорреляционной функции, некоторые суммы квадратов коэффициентов Уолша-Адамара и некоторые суммы экспонент значений самой булевой функции. Эти соотношения представляют и самостоятельный интерес, поэтому сформулируем их в виде отдельной леммы.

Лемма 12.6. *Для любой булевой функции f из $\mathcal{F}_n$, любого подпространства $H \subset \mathbb{F}_2^n$, $\dim H = t$ и любого $v \in \mathbb{F}_2^n$ выполнены равенства*

$$\begin{aligned} \sum_{x \in H} \Delta_f(x) (-1)^{\langle x, v \rangle} &= \sum_{u \in \mathbb{F}_2^n / H} \left(\sum_{y \in u \oplus H} (-1)^{f(y) \oplus \langle y, v \rangle} \right)^2 = \\ &= 2^{-(n-t)} \sum_{z \in v \oplus H^\perp} W_f^2(z). \end{aligned}$$

Доказательство. Как известно,

$$\begin{aligned}
\Delta_f(v) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus v)} = \\
&= 2^{-n} \sum_{z \in \mathbb{F}_2^n} W_f^2(z) (-1)^{\langle z, v \rangle}.
\end{aligned} \tag{12.1}$$

Умножая обе части первого равенства в (12.1) на $(-1)^{\langle v, x \rangle}$ и суммируя по $x \in \mathbb{H}$, получаем, что

$$\begin{aligned}
\sum_{x \in \mathbb{H}} \Delta_f(x) (-1)^{\langle x, v \rangle} &= \sum_{x \in \mathbb{H}} \left(\sum_{z \in \mathbb{F}_2^n} (-1)^{f(z) \oplus f(z \oplus x)} \right) (-1)^{\langle x, v \rangle} = \\
&= \sum_{z \in \mathbb{F}_2^n} (-1)^{f(z)} \sum_{x \in \mathbb{H}} (-1)^{f(z \oplus x)} (-1)^{\langle x, v \rangle} = \\
&= \sum_{u \in \mathbb{F}_2^n / \mathbb{H}} \sum_{z \in u \oplus \mathbb{H}} (-1)^{f(z)} \sum_{x \in \mathbb{H}} (-1)^{f(z \oplus x)} (-1)^{\langle x, v \rangle} = \\
&= \sum_{u \in \mathbb{F}_2^n / \mathbb{H}} \sum_{z \in u \oplus \mathbb{H}} (-1)^{f(z) \oplus \langle z, v \rangle} \sum_{y \in z \oplus \mathbb{H}} (-1)^{f(y)} (-1)^{\langle y, v \rangle}.
\end{aligned}$$

Заметим, что если $z \in u \oplus \mathbb{H}$, то

$$\sum_{y \in z \oplus \mathbb{H}} (-1)^{f(y)} (-1)^{\langle y, v \rangle} = \sum_{y \in u \oplus \mathbb{H}} (-1)^{f(y) \oplus \langle y, v \rangle}.$$

Поэтому предыдущее равенство приводится к виду

$$\sum_{x \in \mathbb{H}} \Delta_f(x) (-1)^{\langle x, v \rangle} = \sum_{u \in \mathbb{F}_2^n / \mathbb{H}} \left(\sum_{y \in u \oplus \mathbb{H}} (-1)^{f(y) \oplus \langle y, v \rangle} \right)^2.$$

Умножая обе части второго равенства в (12.1) на $(-1)^{\langle v, x \rangle}$ и суммируя по $x \in \mathbb{H}$, находим, что

$$\begin{aligned}
\sum_{x \in \mathbb{H}} \Delta_f(x) (-1)^{\langle v, x \rangle} &= \sum_{x \in \mathbb{H}} \left(2^{-n} \sum_{z \in \mathbb{F}_2^n} W_f^2(z) (-1)^{\langle z, x \rangle} \right) (-1)^{\langle v, x \rangle} = \\
&= 2^{-n} \sum_{z \in \mathbb{F}_2^n} W_f^2(z) \sum_{x \in \mathbb{H}} (-1)^{\langle z \oplus v, x \rangle} = 2^{-(n-t)} \sum_{z \in v \oplus \mathbb{H}^\perp} W_f^2(z),
\end{aligned}$$

поскольку, как известно,

$$\sum_{x \in \mathbb{H}} (-1)^{\langle u, x \rangle} = \begin{cases} 2^t, & \text{если } u \in \mathbb{H}^\perp, \\ 0, & \text{если } u \notin \mathbb{H}^\perp. \end{cases}$$

□

Далее нам будет также полезно следующее теоретико-числовое утверждение.

Предложение 12.7. Пусть $\{a_1, \dots, a_N\} \subset \mathbb{R}$. Если

$$\sum_{i=1}^N a_i^2 = \frac{1}{N} \left(\sum_{i=1}^N a_i \right)^2,$$

то

$$a_i = \frac{1}{N} \sum_{j=1}^N a_j, \quad j = 1, \dots, N.$$

Доказательство. Положим

$$b_i = a_i - \frac{1}{N} \sum_{j=1}^N a_j.$$

Тогда

$$b_i^2 = a_i^2 - \frac{2a_i}{N} \sum_{j=1}^N a_j + \frac{1}{N^2} \left(\sum_{j=1}^N a_j \right)^2.$$

Суммируя по i , получаем

$$\begin{aligned}\sum_{i=1}^N b_i^2 &= \sum_{i=1}^N a_i^2 - \frac{2}{N} \sum_{i=1}^N a_i \sum_{j=1}^N a_j + \frac{1}{N} \left(\sum_{i=1}^N a_i \right)^2 = \\ &= \sum_{i=1}^N a_i^2 - \frac{1}{N} \left(\sum_{j=1}^N a_j \right)^2 = 0.\end{aligned}$$

Поскольку $b_i = 0$ для всех $i = 1, \dots, N$. □

Теорема 12.8. *Булева функция f из $\mathcal{F}_n$ является $(H, 0^n)$ -стабильной, $\dim H = t$, тогда и только тогда, когда выполнено любое из двух эквивалентных условий:*

$$\sum_{x \in H} \Delta_f(x) = 2^{-(n-t)} W_f^2(0^n);$$

$$W_f^2(u) = 0 \text{ для любого } u \in H^\perp \setminus \{0^n\}.$$

Доказательство. Если функция f из $\mathcal{F}_n$ является $(H, 0^n)$ -стабильной, то для любого $u \in \mathbb{F}_2^n$

$$\sum_{x \in u \oplus H} (-1)^{f(x)} = 2^{-(n-t)} W_f(0^n)$$

и поэтому

$$\sum_{u \in \mathbb{F}_2^n / H} \left(\sum_{x \in u \oplus H} (-1)^{f(x)} \right)^2 = 2^{-(n-t)} W_f^2(0^n).$$

Отсюда с учетом леммы 12.6 ($v = 0^n$) получаем оба условия теоремы.

Если выполнено одно из условий теоремы, то в силу леммы 12.6 выполнено и другое условие, а также равенство

$$\sum_{u \in \mathbb{F}_2^n / H} \left(\sum_{x \in u \oplus H} (-1)^{f(x)} \right)^2 = \frac{W_f^2(0^n)}{2^{n-t}} = \frac{1}{2^{n-t}} \left(\sum_{u \in \mathbb{F}_2^n / H} \left(\sum_{x \in u \oplus H} (-1)^{f(x)} \right) \right)^2.$$

Отсюда следует (см. предложение 12.7), что для любого $u \in \mathbb{F}_2^n$ выполнено равенство

$$\sum_{x \in u \oplus H} (-1)^{f(x)} = \frac{1}{2^{n-t}} \sum_{u \in \mathbb{F}_2^n / H} \left(\sum_{x \in u \oplus H} (-1)^{f(x)} \right) = \frac{1}{2^{n-t}} W_f(0^n),$$

то есть функция $f(x)$ — $(H, 0^n)$ -стабильная. $\square$

Второе условие теоремы 12.8 позволяет получить еще некоторые свойства коэффициентов Уолша-Адамара для $(H, 0^n)$ -стабильных функций. Вначале докажем вспомогательное утверждение.

Лемма 12.9. *Для булевой функции f из $\mathcal{F}_n$, любого подпространства $L < \mathbb{F}_2^n$ и любого $v \in \mathbb{F}_2^n \setminus L$ выполнено соотношение*

$$\sum_{u \in L} W_f(u) + \sum_{u \in v \oplus L} W_f(u) \equiv 0 \pmod{2^T},$$

где

$$T = \begin{cases} n, & \text{если } \dim L = n - 1, \\ \dim L + 2, & \text{если } \dim L < n. \end{cases}$$

Доказательство. Пусть M — подпространство, натянутое на L и v , $\dim L = s$. Для M справедливы следующие равенства

$$\begin{aligned} \sum_{u \in M} W_f(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} \sum_{u \in M} (-1)^{\langle u, x \rangle} = \\ &= 2^{s+1} \sum_{x \in M^\perp} (-1)^{f(x)}. \end{aligned}$$

По определению M имеем

$$\sum_{u \in M} W_f(u) = \sum_{u \in L} W_f(u) + \sum_{u \in v \oplus L} W_f(u).$$

Для завершения доказательства остается заметить, что

$$\sum_{x \in M^\perp} (-1)^{f(x)} \equiv \begin{cases} 1 \pmod{2}, & \text{если } \dim L = n - 1, \\ 0 \pmod{2}, & \text{если } \dim L < n - 1. \end{cases}$$

□

Следствие 12.10. Для любой булевой функции f из $\mathcal{F}_n$, любого подпространства $L < \mathbb{F}_2^n$ и любого $v \in \mathbb{F}_2^n \setminus L$ выполнено сравнение

$$\sum_{x \in L} W_f(x) (-1)^{\langle x, v \rangle} + \sum_{x \in v \oplus L} W_f(x) (-1)^{\langle x, v \rangle} \equiv 0 \pmod{2^T},$$

где

$$T = \begin{cases} n, & \text{если } \dim L = n - 1, \\ \dim L + 2, & \text{если } \dim L < n - 1. \end{cases}$$

Доказательство. Можно провести, повторяя доказательство леммы 12.9 для сумм вида

$$\sum_{x \in M} W_f(x) (-1)^{\langle x, v \rangle},$$

где v — произвольный вектор из $\mathbb{F}_2^n$.

□

Следствие 12.11. Пусть $f(x)$ — $(H, 0^n)$ -стабильная функция из $\mathcal{F}_n$. Тогда для любого $v \in \mathbb{F}_2^n$ выполнено сравнение

$$\sum_{x \in v \oplus H^\perp} W_f(x) (-1)^{\langle x, v \rangle} \equiv 0 \pmod{2^{n - \dim H + 1}}.$$

Доказательство. Легко проводится с использованием лемм 12.9, 12.4 и второго утверждения теоремы 12.8.

□

Теорема 12.8 кроме критерия $(H, 0^n)$ -стабильности булевой функции, дает также способ описания семейства $\mathcal{H}_{f, 0^n}$. Прежде всего заметим, что если $H \in \mathcal{H}_{f, 0^n}$, то и $H' \in \mathcal{H}_{f, 0^n}$ для любого $H' \supset H$. Поэтому семейство $\mathcal{H}_{f, 0^n}$ может

быть задано некоторым набором минимальных (по включению) подпространств $H_1, H_2, \dots, H_l$ таких, что

- f является $(H_i, 0^n)$ -стабильной для всех $i = 1, \dots, l$;
- для любого $H \in \mathcal{H}_{f, 0^n}$ найдется такое $i \in \{1, \dots, l\}$, что $H \supset H_i$;
- не существует такой пары $\{i, j\} \subset \{1, 2, \dots, l\}$, $i \neq j$, что $H_i \subset H_j$.

В соответствии с теоремой 12.8 имеем $W_f(u) = 0$ для всех $u \in H_i^\perp \setminus \{0^n\}$, $i = 1, 2, \dots, l$. Это условие позволяет сформулировать следующий алгоритм построения семейства $\mathcal{H}_{f, 0^n}$ для данной булевой функции f .

Алгоритм построения $\mathcal{H}_{f, 0^n}$.

1. Найти все коэффициенты Уолша-Адамара $W_f(u)$, $u \in \mathbb{F}_2^n$.
2. Определить множество нулей $Z_f = \{u \in \mathbb{F}_2^n \mid W_f(u) = 0\}$.
3. Найти все максимальные (по включению) подпространства L , которые входят в $Z_f \cup \{0^n\}$.
4. Набор всех дуальных к найденным в п.3 максимальным подпространствам задает семейство $\mathcal{H}_{f, 0^n}$.

Как видно из утверждения предложения 12.3, алгоритм построения семейства $\mathcal{H}_{f, v}$ для любого $v \in \mathbb{F}_2^n$ отличается от алгоритма построения $\mathcal{H}_{f, 0^n}$ заменой множества Z_f на множество $Z_f \oplus v$.

Замечание 12.12. Введенное выше множество Z_f произвольным быть не может. Так, например, несложно видеть, что множество Z_f заведомо не может быть объединением вида $Z_f = H_{v^1} \cup \dots \cup H_{v^t}$, где

$$H_{v^i} = \{x \in \mathbb{F}_2^n \mid \langle x, v^i \rangle = \varepsilon\},$$

$\varepsilon \in \mathbb{F}_2$, $i \in 1, \dots, t$ — некоторые гиперплоскости, в случае, когда векторы $v^1, \dots, v^t$ не образуют подпространство в $\mathbb{F}_2^n$. Это непосредственно вытекает из того, что все векторы $v \in \mathbb{F}_2^n$ такие, что $H_v \subseteq Z_f$ (и только они) являются линейными трансляторами функции f , а как известно, все линейные трансляторы образуют подпространство в $\mathbb{F}_2^n$.

Для иллюстрации введенных понятий и полученных результатов полезно рассмотреть пример класса $(H, 0^n)$ -стабильных булевых функций. Необходимо отметить, что приводимая конструкция используется для синтеза различных криптографических классов булевых функций (см. [ЛССЯ 15]).

Пример 12.13. Пусть базис в $\mathbb{F}_2^n$ выбран так, что $H = \{(0^{n-t}, y) \mid y \in \mathbb{F}_2^t\}$. Рассмотрим булеву функцию

$$f(x, y) = \langle \Phi(u), y \rangle = \varphi_1(u)y_1 \oplus \dots \oplus \varphi_t(u)y_t,$$

где $\Phi = (\varphi_1, \dots, \varphi_t) : \mathbb{F}_2^{n-t} \rightarrow \mathbb{F}_2^t$ — некоторое отображение, причем $\Phi(u) \neq 0^t$ для любого $u \in \mathbb{F}_2^{n-t}$. Тогда при любой фиксации переменной $u = u^0 \in \mathbb{F}_2^{n-t}$ функция $f(u^0, y)$ является линейной функцией, отличной от нулевой. Поэтому $W_{f(u, 0^t) \oplus H}(0^t) = W_f(0^n) = 0$ при всех $u \in \mathbb{F}_2^{n-t}$, то есть f — $(H, 0^n)$ -стабильная функция.

Пример 12.14. Пусть теперь $n = 2t$ и отображение $\Phi : \mathbb{F}_2^t \rightarrow \mathbb{F}_2^t$ удовлетворяет следующим условиям:

- $\Phi(u^1) = \Phi(u^2) = y^1 \neq 0^t$ при некоторых u^1, u^2 ($u^1 \neq u^2$), $y^1 \in \mathbb{F}_2^t$;
- $\Phi(u) \neq 0^t$ для любого $u \in \mathbb{F}_2^t$;
- отображение $\Phi' : \mathbb{F}_2^t \setminus \{u^1, u^2\} \rightarrow \mathbb{F}_2^t \setminus \{0^t, y^1\}$ взаимно однозначно, где $\Phi'(u) = \Phi(u)$ для любого $u \in \mathbb{F}_2^t \setminus \{u^1, u^2\}$.

Применим к функции $f(u, y)$ алгоритм построения $\mathcal{H}_{f, 0^n}$. Найдем все $W_f(a, b)$, $a, b \in \mathbb{F}_2^t$:

$$\begin{aligned} W_f(a, b) &= \sum_{u, y \in \mathbb{F}_2^t} (-1)^{f(u, y)} (-1)^{\langle a, u \rangle} (-1)^{\langle b, y \rangle} = \\ &= \sum_{u \in \mathbb{F}_2^t} (-1)^{\langle a, u \rangle} \sum_{y \in \mathbb{F}_2^t} (-1)^{\langle \Phi(u) \oplus b, y \rangle} = \\ &= 2^t \sum_{u \in \Phi^{-1}(b)} (-1)^{\langle a, u \rangle}. \end{aligned}$$

Отсюда находим, что

$$W_f(a, b) = \begin{cases} 2^t (-1)^{\langle a, \Phi^{-1}(b) \rangle}, & \text{если } b \neq 0^t, y^1, \\ 0, & \text{если } b = 0^t, \\ 2^t \left((-1)^{\langle a, u^1 \rangle} + (-1)^{\langle a, u^2 \rangle} \right), & \text{если } b = y^1. \end{cases}$$

Поэтому множество нулей Z_f имеет вид

$$Z_f = \{ (a, 0^t) \mid a \in \mathbb{F}_2^t \} \cup \{ (a, y^1) \mid a \in \mathbb{F}_2^t, \langle a, u^1 \oplus u^2 \rangle = 1 \}.$$

Мощность множества Z_f равна $2^t + 2^{t-1}$. Очевидно, что максимальное (по включению) подпространство, которое входит в Z_f — это подпространство $\{ (a, 0^t) \mid a \in \mathbb{F}_2^t \}$. Поэтому семейство $\mathcal{H}_{f, 0^n}$ — это все подпространства, содержащие подпространство $H = \{ (0^t, y) \mid y \in \mathbb{F}_2^t \}$.

Соотношение между свойствами $(H, 0^n)$ -стабильности и корреляционной иммунности достаточно ясно (см. пример 12.1). Сформулируем это соотношение в виде отдельного утверждения. По существу это утверждение является еще одной характеристикой (критерием) корреляционной иммунности наряду с теоретико-информационной, весовой и спектральной характеристиками ([ЛССЯ 15]).

Теорема 12.15. *Булева функция f из $\mathcal{F}_n$ является корреляционно-иммунной порядка t , $0 < t \leq n - 1$ тогда и только тогда, когда она является $(H, 0^n)$ -стабильной для всех $\binom{n}{m}$ подпространств, натянутых на какие-нибудь $n - t$ базисных векторов пространства $\mathbb{F}_2^n$.*

Доказательство. Вытекает из утверждения теоремы 12.8, определения корреляционной иммунности и структуры семейства $\mathcal{H}_{f, 0^n}$. □

§13 Аффинные сужения булевых функций и отображений.

Понятие локальной аффинности

Пусть Φ — произвольное отображение из $\mathcal{F}_{n,m}$ и $\mathcal{D}$ — некоторое произвольное подмножество (область) пространства $\mathbb{F}_2^n$.

Определение 13.1. Сужением отображения Φ на область $\mathcal{D} \subseteq \mathbb{F}_2^n$ будем называть отображение $\Phi_{\mathcal{D}}$ из $\mathcal{D}$ в $\mathbb{F}_2^m$ такое, что $\Phi_{\mathcal{D}}(x) = \Phi(x)$ для любого x из $\mathcal{D}$. В случае $m = 1$ будем говорить о сужении булевой функции (см. §7).

Определение 13.2. Сужение отображения $\Phi \in \mathcal{F}_{n,m}$ на область $\mathcal{D} \subseteq \mathbb{F}_2^n$ будем называть аффинным сужением, если существует $\Psi \in \mathcal{A}_{n,m}$ такое, что $\Phi_{\mathcal{D}} = \Psi_{\mathcal{D}}$. В случае $m = 1$ будем говорить об аффинном сужении функции. Область $\mathcal{D}$ соответственно назовем локальной аффинностью отображения Φ .

Вообще говоря, область $\mathcal{D}$ может быть выбрана произвольным образом. Однако, с точки зрения исследования алгебраических, комбинаторных, метрических и криптографических свойств булевых функций и отображений целесообразно выбирать область $\mathcal{D}$, имеющую достаточно простое (эффективное) описание. Наиболее удобными вариантами являются подмножества пространства $\mathbb{F}_2^n$, элементы которых являются решениями некоторой системы линейных уравнений, т.е., другими словами, смежными классами по подпространствам пространства $\mathbb{F}_2^n$. Для краткости будем называть такие подмножества плоскостями, как это принято в теории кодирования (см. [MWS 77]).

Пусть P_n — множество всех плоскостей пространства $\mathbb{F}_2^n$ (включая пустую плоскость — $\emptyset$). Для плоскости $\pi = L \oplus u$ ($u \in \mathbb{F}_2^n$, L — подпространство $\mathbb{F}_2^n$) будем считать, что $\dim \pi = \dim L$. При этом полагаем, что $\dim(\emptyset) = -1$.

Предложение 13.3. Для произвольного отображения $\Psi \in \mathcal{A}_{n,m}$ и произвольной плоскости $\pi \in P_n$ справедливо включение $\Psi(\pi) = \pi' \in P_m$.

Доказательство. Следует из свойств аффинного отображения. □

Определение 13.4. Пусть $\Phi \in \mathcal{F}_{n,m}$.

a) При $m \geq 2$ назовем плоскость $\pi \in P_n$ локальной аффинностью отображения Φ , если выполнено по крайней мере одно из условий:

$$1^\circ \Phi(\pi) = \pi' \in P_m;$$

2° Φ_π — аффинное сужение отображения Φ .

b) При $m = 1$, $\Phi = f \in \mathcal{F}_{n,1} = \mathcal{F}_n$, назовем плоскость $\pi \in P_n$ локальной аффинностью функции f , если f_π — аффинное сужение функции f .

Замечание 13.5. Пусть $m \geq 2$. Если локальная аффинность π удовлетворяет условию 2° определения 13.4а, то для него выполнено и условие 1° (см. предложение 13.3). Однако, для некоторых отображений $\Phi \in \mathcal{F}_{n,m}$, $m \geq 2$ существуют плоскости $\{\tau\}$ такие, что для них условие 1° определения 13.4а выполнено, а условие 2° не выполнено. Пример такой плоскости можно найти в приложении В.

Для взаимных однозначных отображений (S-боксов) с помощью их локальных аффинностей могут быть описаны почти совершенные нелинейные (almost perfect nonlinear - APN) отображения ([Hou 06], [CHM 04]). Локальные аффинности отображения тесно связаны с таким криптографическим параметром, как индекс линейности отображения, определяющим степень разветвления данного отображения аффинными отображениями ([ЛССЯ 15]). С помощью локальных аффинностей описаны нормальные (normal) и слабо нормальные (weakly normal) бент-функции ([CDDL 06]). Локальные аффинности играют также важную роль при синтезе конструкций, реализующих некоторые классы булевых функций. Примером может служить конструкция Майорана-МакФарланда, с помощью которой можно реализовать бент-функции и корреляционно-иммунные (устойчивые) функции ([Car 10,1], [WuD 00]). Другим примером могут служить мультиаффинные функции ([MWS 77], [ГоТа 09]).

Для отображения $\Phi \in \mathcal{F}_{n,m}$, $m \geq 2$ будем обозначать через $Q_{n,m}(\Phi)$ — множество всех локальных аффинностей (определение 13.4а 1°) отображения Φ , а через $P_{n,m}(\Phi)$ — множество локальных аффинностей отображения Φ , удовлетворяющих определению 13.4а 2°. Ясно, что $P_{n,m}(\Phi) \subseteq Q_{n,m}(\Phi)$.

Для булевой функции $f \in \mathcal{F}_n$ будем обозначать $Q_{n,1}(f) = P_{n,1}(f) = P_n(f)$ — множество всех локальных аффинностей функции f .

Пусть $d \in \{0, 1, \dots, n\}$ и $Q_{n,m}^d(\Phi)$, $P_{n,m}^d(\Phi)$ и $P_n^d(f)$ — множества локальных аффинностей размерности d из множеств $Q_{n,m}(\Phi)$, $P_{n,m}(\Phi)$ и $P_n(f)$ соответственно. Положим $q_{n,m}^d(\Phi) = \#Q_{n,m}^d(\Phi)$, $p_{n,m}^d(\Phi) = \#P_{n,m}^d(\Phi)$, $p_n^d(f) = \#P_n^d(f)$ и

$$\begin{aligned} q_{n,m}(\Phi) &= (q_{n,m}^0(\Phi), q_{n,m}^1(\Phi), \dots, q_{n,m}^n(\Phi)), \\ p_{n,m}(\Phi) &= (p_{n,m}^0(\Phi), p_{n,m}^1(\Phi), \dots, p_{n,m}^n(\Phi)), \\ p_n(f) &= (p_n^0(f), p_n^1(f), \dots, p_n^n(f)). \end{aligned} \quad (13.1)$$

Предложение 13.6. Пусть $\Phi_1, \Phi_2 \in \mathcal{F}_{n,m}$, $m \geq 2$ ($f_1, f_2 \in \mathcal{F}_n$) такие, что существует преобразование $\mathfrak{g} \in \mathbb{G} = \text{GA}(n, 2)$, удовлетворяющее условию $\Phi_1^{\mathfrak{g}} = \Phi_2$ ($f_1^{\mathfrak{g}} = f_2$). Тогда $q_{n,m}(\Phi_1) = q_{n,m}(\Phi_2)$, $p_{n,m}(\Phi_1) = p_{n,m}(\Phi_2)$ ($p_n(f_1) = p_n(f_2)$), то есть наборы (набор) $q_{n,m}(\Phi_1)$, $p_{n,m}(\Phi_1)$ ($p_n(f_1)$) являются (является) аффинными инвариантами (аффинным инвариантом) для соответствующих отображений (функций).

Доказательство. Следует из определения 13.4 и предложения 13.3. □

Существенную роль в исследованиях групповых отображений играют локальные аффинности, обладающие дополнительными свойствами.

Определение 13.7. Локальную аффинность π отображения Φ будем называть особенной, если выполнено следующее равенство: $\Phi^{-1}(\Phi(\pi)) = \pi$.

Результаты, использующие данное свойство, будут приведены далее.

Предложение 13.8. Пусть $\Phi \in \mathcal{F}_{n,m}$, $m \geq 2$ ($f \in \mathcal{F}_n$). Тогда выполнены следующие утверждения:

- 1° если плоскости $\pi_1 \in P_{n,m}(\Phi)$ ($\pi_1 \in P_n(f)$), $\pi_2 \in P_n$ и $\pi_1 \supset \pi_2$, то $\pi_2 \in P_{n,m}(\Phi)$ ($\pi_2 \in P_n(f)$);
- 2° если $\pi_1, \pi_2 \in P_{n,m}(\Phi)$ ($\pi_1, \pi_2 \in P_n(f)$) и $\pi_1 \cap \pi_2 \neq \emptyset$, то $\pi_1 \cap \pi_2 \in P_{n,m}(\Phi)$ ($\pi_1 \cap \pi_2 \in P_n(f)$).

Доказательство. Утверждение 1° следует из определения 13.4 и предложения 13.3.

Для доказательства утверждения 2° воспользуемся следующими соображениями. Элементы плоскости π_i , $i = 1, 2$ и только они являются решениями подходящей системы линейных уравнений $xA_i = u^i$. Следовательно, элементы множества $\pi_1 \cap \pi_2$ и только они являются решениями системы линейных уравнений $xA' = x[A_1 A_2] = (u^1, u^2)$. Утверждение 2° далее следует из утверждения 1°. $\square$

Пусть $\Phi \in \mathcal{F}_{n,m}$ ($f \in \mathcal{F}_n$). Будем говорить, что плоскость $\pi_1 \in P_{n,m}(\Phi)$ ($\pi_1 \in P_n(f)$) покрывает плоскость $\pi_2 \in P_{n,m}(\Phi)$ ($\pi_2 \in P_n(f)$), если $\pi_2 \subset \pi_1$ ($\pi_1 \neq \pi_2$) и не существует плоскости $\pi' \in P_{n,m}(\Phi)$ ($\pi' \in P_n(f)$), $\pi' \neq \pi_1$, $\pi' \neq \pi_2$ такой, что $\pi_2 \subset \pi' \subset \pi_1$.

Используя понятие покрытия, можно следующим образом получить графическое представление частично-упорядоченного (относительно теоретико-множественного включения) множества $P_{n,m}(\Phi)$ ($P_n(f)$). Изобразим каждый элемент множества $P_{n,m}(\Phi)$ ($P_n(f)$) в виде небольшого кружочка, располагая π_1 выше π_2 , если $\pi_2 \subset \pi_1$. Соединим π_1 и π_2 ребром, если π_1 покрывает π_2 . Полученная фигура называется диаграммой Хассе частично-упорядоченного множества $P_{n,m}(\Phi)$ ($P_n(f)$). Минимальными элементами этого множества являются одноэлементные множества $\{x\}$, $x \in \mathbb{F}_2^n$ (нижний ярус), представляющие собой плоскости размерности 0. Обозначим через $M_{n,m}(\Phi)$ ($M_n(f)$) множество макси-

мальных элементов частично-упорядоченного множества $P_{n,m}(\Phi) (M_n(f))$ (см. приложение **В**).

Предложение 13.9. Пусть $\Phi \in \mathcal{F}_{n,m}$, $m \geq 2$ ($f \in \mathcal{F}_n$). Тогда множество $M_{n,m}(\Phi) (M_n(f))$ однозначно определяет $P_{n,m}(\Phi) (P_n(f))$.

Доказательство. Вытекает из предложения **13.8**, поскольку $P_{n,m}(\Phi) (P_n(f))$ состоит из тех и только тех плоскостей, которые принадлежат хотя бы одной плоскости из $M_{n,m}(\Phi) (M_n(f))$. $\square$

Пример 13.10. Рассмотрим хорошо известный (см., например, [АЗКЧ 01]) потоковый шифр А5, применяемый для защиты телефонных переговоров в европейской системе мобильной связи GSM (Group Special Mobile).

Более конкретно, нас будет интересовать то нелинейное отображение, которое реализовано в этом шифре. Рассматриваемое отображение Φ является взаимно однозначным отображением пространства $\mathbb{F}_2^{64}$. Векторное пространство $\mathbb{F}_2^{64}$ представлено в виде декартового произведения $\mathbb{F}_2^{19}, \mathbb{F}_2^{22}, \mathbb{F}_2^{23}$, т.е. $\mathbb{F}_2^{64} = \mathbb{F}_2^{19} \times \mathbb{F}_2^{22} \times \mathbb{F}_2^{23}$. Соответственно, любой вектор x пространства $\mathbb{F}_2^{64}$ представим в виде

$$x = (x^1, x^2, x^3) = ((x_1^1 \dots x_{19}^1), (x_1^2 \dots x_{22}^2), (x_1^3 \dots x_{23}^3)),$$

где $x^1 \in \mathbb{F}_2^{19}$, $x^2 \in \mathbb{F}_2^{22}$, $x^3 \in \mathbb{F}_2^{23}$.

Пусть B_1 — линейное преобразование пространства $\mathbb{F}_2^{19}$, реализуемое линейным регистром сдвига с полиномом обратной связи $c_1(\lambda) = \lambda^{19} \oplus \lambda^5 \oplus \lambda^2 \oplus \lambda \oplus 1$; B_2 — линейное преобразование пространства $\mathbb{F}_2^{22}$, реализуемое линейным регистром сдвига с полиномом обратной связи $c_2(\lambda) = \lambda^{22} \oplus \lambda \oplus 1$; B_3 — линейное преобразование пространства $\mathbb{F}_2^{23}$, реализуемое регистром сдвига с полиномом обратной связи $c_3(\lambda) = \lambda^{23} \oplus \lambda^{15} \oplus \lambda^2 \oplus \lambda \oplus 1$. Разветвляющее пространство (см. §5) имеет размерность $k = 3$, а разветвляющее отображение l имеет вид $l(x) = (l_1(x), l_2(x), l_3(x)) = (x_{10}^1, x_{11}^2, x_{12}^3)$.

Разветвляемые отображения $A_u, u \in \mathbb{F}_2^3$ имеют вид

$$A_{000} = A_{111} = \begin{bmatrix} B_1 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & B_3 \end{bmatrix}, A_{001} = A_{110} = \begin{bmatrix} B_1 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & \text{Id}_{23} \end{bmatrix},$$

$$A_{010} = A_{101} = \begin{bmatrix} B_1 & 0 & 0 \\ 0 & \text{Id}_{22} & 0 \\ 0 & 0 & B_3 \end{bmatrix}, A_{100} = A_{011} = \begin{bmatrix} \text{Id}_{19} & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & \text{Id}_{23} \end{bmatrix}.$$

Следовательно, смежные классы (плоскости) по подпространству $L = \{x \in \mathbb{F}_2^{64} \mid x_{10}^1 = 0, x_{11}^2 = 0, x_{12}^3 = 0\}$ вида $\pi = L \oplus x^{(\alpha, \beta, \gamma)}$, где

$$u^{(\alpha, \beta, \gamma)} = (0^9 \alpha 0^9, 0^{10} \beta 0^{11}, 0^{11} \gamma 0^{11}), \alpha, \beta, \gamma \in \mathbb{F}_2,$$

являются локальными аффинностями отображения $\Phi \in \mathcal{F}_{64,64}$.

§14 Локальные аффинности булевых функций, связанные с фиксацией переменных

В данном параграфе мы рассмотрим некоторые параметры аффинных сужений булевых функций как для произвольных плоскостей пространства $\mathbb{F}_2^n$, так и для конкретных семейств плоскостей, описываемых фиксациями переменных. Представители указанного семейства плоскостей в качестве локальных аффинностей играют чрезвычайно важную роль в комбинаторных алгоритмах обращения дискретных функций, содержащих этапы перебора части описывающих функцию параметров.

Далее в этом параграфе мы будем рассматривать линеаризацию одного булева уравнения, используя аффинные сужения.

Относительно линеаризации системы булевых уравнений

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

следует напомнить следующее. Известно, что множество решений указанной выше системы уравнений совпадает с множеством решений уравнения

$$f(x_1, \dots, x_n) = \prod_{i=1}^m (f_i(x_1, \dots, x_n) \oplus 1) \oplus 1 = 0.$$

Пусть $f \in \mathcal{F}_n$ и $k \leq n$. Для наборов $1 \leq i_1 < \dots < i_k \leq n$, $(b_1, \dots, b_k) \in \mathbb{F}_2^n$ обозначим через $f_{i_1 \dots i_k}^{b_1 \dots b_k}$ булеву функцию из $\mathcal{F}_{n-k}$, полученную из f фиксацией переменных $x_{i_1} = b_1, \dots, x_{i_k} = b_k$ и называемую подфункцией функции f . При $k = 0$ соответствующая подфункция совпадает с самой функцией, а при $k = n$ подфункция есть просто значение данной функции на конкретном наборе значений переменных.

Поскольку фиксация переменных определяет плоскость

$$\pi = \pi_{i_1 \dots i_k}^{b_1 \dots b_k} = L \oplus b,$$

где

$$L = \{x \in \mathbb{F}_2^n \mid x_{i_1} = \dots = x_{i_k} = 0\}, \dim L = n - k,$$

$$b = (0 \dots 0 \underset{i_1}{b_1} 0 \dots 0 \underset{i_k}{b_k} 0 \dots 0),$$

$$\text{то } f_{i_1 \dots i_k}^{b_1 \dots b_k} = f_\pi.$$

Определение 14.1. а) Булева функция f из $\mathcal{F}_n$ называется k -аффинной, $0 \leq k \leq n-1$, если существуют наборы $1 \leq i_1 < \dots < i_k \leq n$ и $(b_1 \dots b_k) \in \mathbb{F}_2^k$ такие, что $\deg(f_{i_1 \dots i_k}^{b_1 \dots b_k}) \leq 1$.

б) Булева функция f из $\mathcal{F}$ называется сильно k -аффинной, $0 \leq k \leq n-1$, если существует набор $1 \leq i_1 < \dots < i_k \leq n$ такой, что для любого набора $(b_1 \dots b_k) \in \mathbb{F}_2^k$ выполнено $\deg(f_{i_1 \dots i_k}^{b_1 \dots b_k}) \leq 1$.

Замечание 14.2. Легко видеть, что любая функция из $\mathcal{F}_n$ является $(n-1)$ -аффинной и, более того, сильно $(n-1)$ -аффинной.

Замечание 14.3. Если функция f из $\mathcal{F}_n$ является сильно k -аффинной, то легко показать, что $\text{ill}(f) \leq k$.

Разнообразные конструкции на основе k -аффинных функций используются для синтеза криптографических булевых функций (например, бент-функций, корреляционно-иммунных и устойчивых функций). Мы приведем пример лишь одной такой конструкции.

Пример 14.4. Конструкция Майорана-МакФарланда (см. [Car 10,1]). Рассмотрим натуральное $n = k + r$ и $\mathbb{F}_2^n = \mathbb{F}_2^r \times \mathbb{F}_2^k$. Пусть $\Phi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^r$ — произвольное отображение из $\mathcal{F}_{k,r}$ и g — произвольная функция из $\mathcal{F}_k$. Определим булеву функцию из $\mathcal{F}_n$ вида

$$f_{\Phi,g}(x,y) = \langle x, \Phi(y) \rangle \oplus g(y),$$

где $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^k$. Очевидно, что функция $f_{\Phi,g}$ является сильно k -аффинной функцией, т.к. любая фиксация значений набора y превращает эту функцию в аффинную.

Пусть $n = 2k$, отображение $\Phi : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^k$ является взаимно однозначным и g — произвольная булева функция из $\mathcal{F}_k$. Тогда функция $f_{\Phi,g}$ является бент-функцией.

Пусть теперь для отображения $\Phi : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^r$ выполнено условие: для любого $u \in \Phi(\mathbb{F}_2^k)$ справедливо неравенство $\text{wt}(u) > s$. Тогда функция $f_{\Phi,g}$ — m -устойчивая при $m \geq s$.

Рассмотрим теперь некоторые числовые характеристики аффинных сужений, введенные в работах [ЛСЯ 04,2], [Бур 08], которые будут полезны нам далее.

Определение 14.5. а) Уровнем аффинности $la(f)$ булевой функции f из $\mathcal{F}_n$ называется минимальное натуральное число k , для которого f является k -аффинной.

б) Частичным уровнем аффинности $la^0(f)$ булевой функции f из $\mathcal{F}_n$ называется минимальное натуральное число k , для которого существует набор $1 \leq i_1 < \dots < i_k \leq n$ такой, что $\deg(f_{i_1 \dots i_k}^{0 \dots 0}) \leq 1$.

с) Обобщенным уровнем аффинности $\mathcal{L}a(f)$ булевой функции $f \in \mathcal{F}_n$ называется неотрицательное целое число

$$\mathcal{L}a(f) = n - \max_{\pi \in P_n(f)} \{\dim \pi\} = n - \max_{\pi \in M_n(f)} \{\dim \pi\}.$$

Непосредственно из определения 14.5 вытекает, что

$$\mathcal{L}a(f) \leq la(f) \leq la^0(f). \quad (14.1)$$

Подробному изучению свойств этих параметров и связи их с различными криптографическими свойствами булевых функций посвящены работы [БуЛо 05,1], [Лог 08], [Бур 08], [Лог 10]. В частности, в работе [БуЛо 05,1] полностью описан класс булевых функций, обладающих максимальным возможным значением уровня аффинности.

Теорема 14.6 ([БуЛо 05,1]). Для булевой функции f из $\mathcal{F}_n$ соотношение $la(f) = n - 1$ выполнено тогда и только тогда, когда

$$f(x_1, \dots, x_n) = \bigoplus_{i < j} x_i x_j \oplus l(x_1, \dots, x_n),$$

где l — произвольная аффинная функция из $\mathcal{A}_n$.

В работе [Лог 08] получена нижняя оценка уровня аффинности: для почти всех булевых функций при $n \rightarrow \infty$ уровень аффинности больше чем $n - 2 \log_2 n$.

В работе [Бур 08] получена более сильная оценка уровня аффинности (обобщенного уровня аффинности) для почти всех булевых функций.

Теорема 14.7 ([Бур 08]). Пусть $\alpha \in \mathbb{R}, \alpha > 1$, — произвольная фиксированная константа. Тогда асимптотически при $n \rightarrow \infty$ для почти всех функций из $\mathcal{F}_n$

$$\mathcal{L}a(f) \geq n - \alpha \log_2 n \quad (la(f) \geq n - \alpha \log_2 n).$$

Обозначим через $\mathcal{M}_{n,k}, 1 \leq k \leq n$, множество функций из $\mathcal{F}_n$, для которых выполнено неравенство $la(f) \leq k$, и $\overline{\mathcal{M}}_{n,k} = \mathcal{F}_n \setminus \mathcal{M}_{n,k}$. Соответствующую долю множества $\mathcal{M}_{n,k}$ в $\mathcal{F}_n$ обозначим $\delta_{n,k} = (\#\mathcal{M}_{n,k})/2^{2^n}$. Справедливо следующее утверждение.

Теорема 14.8. Асимптотически при $n \rightarrow \infty$ для почти всех булевых функций f из $\mathcal{F}_n$ справедливо неравенство

$$la(f) \leq n - \log_2 n + 1.$$

Доказательство. Пусть $f \in \mathcal{F}_n$ и $1 \leq k < n - 1$. Рассмотрим разложение f в сумму ее подфункций по переменным $x_1, \dots, x_k$ вида

$$f(x_1, \dots, x_n) = \bigoplus_{(u_1 \dots u_k) \in \mathbb{F}_2^k} (x_1 \oplus u_1 \oplus 1) \dots (x_k \oplus u_k \oplus 1) f_{1 \dots k}^{u_1 \dots u_k}(x_{k+1}, \dots, x_n). \quad (14.2)$$

Если $f \in \overline{\mathcal{M}}_{n,k}$, то необходимо, чтобы все подфункции $f_{1\dots k}^{u_1\dots u_k}$ из разложения (14.2) имели алгебраическую степень не менее 2, то есть не являлись бы аффинными функциями из $\mathcal{A}_{n-k}$. Следовательно,

$$\#\overline{\mathcal{M}}_{n,k} \leq \left(2^{2^{n-k}} - 2^{n-k+1}\right)^{2^k}$$

и

$$\#\mathcal{M}_{n,k} \geq 2^{2^n} - \left(2^{2^{n-k}} - 2^{n-k+1}\right)^{2^k}.$$

Тогда

$$\delta_{n,k} \geq 1 - \left(\frac{2^{2^{n-k}} - 2^{n-k+1}}{2^{2^{n-k}}}\right)^{2^k} = 1 - \alpha_{n,k}. \quad (14.3)$$

Положим $k = n - \log_2 n + 1$ и устремим $n \rightarrow \infty$. Для величины $\alpha_{n,n-\log_2 n+1}$ справедлива следующая цепочка равенств:

$$\begin{aligned} \alpha_{n,n-\log_2 n+1} &= \left(1 - \frac{2^{n-(n-\log_2 n+1)+1}}{2^{2^{n-(n-\log_2 n+1)}}}\right)^{2^{n-\log_2 n+1}} = \\ &= \left(1 - \frac{n}{2^{n/2}}\right)^{\frac{2^{n+1}}{n}} = \left(\left(1 + \frac{-1}{\frac{2^{n/2}}{n}}\right)^{\frac{2^{n/2}}{n}}\right)^{2^{n/2+1}}. \end{aligned} \quad (14.4)$$

Воспользовавшись известным соотношением

$$\lim_{t \rightarrow \infty} \left(1 + \frac{d}{t}\right)^t = e^d, \quad d \in \mathbb{R}, \quad (14.5)$$

совместно с (14.4), получаем

$$\lim_{n \rightarrow \infty} \alpha_{n,n-\log_2 n+1} = 0. \quad (14.6)$$

Следовательно, соотношения (14.3) и (14.6) дают

$$\lim_{n \rightarrow \infty} \delta_{n, n - \log_2 n + 1} = 1,$$

что и доказывает утверждение теоремы. $\square$

Следствие 14.9. *Асимптотически при $n \rightarrow \infty$ для почти всех булевых функций f из $\mathcal{F}_n$ справедливо неравенство $\mathcal{L}a(f) \leq n - \log_2 n + 1$.*

Доказательство. Непосредственно следует из утверждения теоремы 14.8 и неравенства (14.1). $\square$

Поскольку для любой функции f из $\mathcal{F}_n$ значения $la(f)$ и $\mathcal{L}a(f)$ являются неотрицательными целыми числами, то утверждения теорем 14.6, 14.7, 14.8 и следствия 14.9 могут быть объединены следующим образом.

Теорема 14.10. *Асимптотически при $n \rightarrow \infty$ для почти всех булевых функций f из $\mathcal{F}_n$ выполнены неравенства*

$$\begin{aligned} n - \lfloor \log_2 n \rfloor &\leq la(f) \leq n - \lceil \log_2 n \rceil + 1 \\ n - \lfloor \log_2 n \rfloor &\leq \mathcal{L}a(f) \leq n - \lceil \log_2 n \rceil + 1. \end{aligned} \tag{14.7}$$

Замечание 14.11. Легко видеть, что условия (14.7) выделяют два возможных случая $n = 2^b$ и $n \neq 2^b$, где b — натуральное число. В случае, когда $n = 2^b$, для почти всех булевых функций имеется два возможных значения уровня (обобщенного уровня) аффинности: $n - b$, $n - b + 1$. А в случае, когда n не является степенью 2, для почти всех функций из $\mathcal{F}_n$ имеется одно возможное значение для уровня (обобщенного уровня) аффинности:

$$n - \lfloor \log_2 n \rfloor = n - \lceil \log_2 n \rceil + 1.$$

Замечание 14.12. Воспользовавшись соотношениями (14.4) и (14.5) можно показать, что в случае $n = 2^b$ имеем

$$\lim_{b \rightarrow \infty} \delta_{n, n-b} \geq 1 - e^{-2}.$$

Определенный интерес представляет сравнение полученных результатов с результатами, связывающими значения уровня аффинности с параметрами булевых функций из известных классов. Рассмотрим эти сравнения на примере классов бент-функций и корреляционно-иммунных функций.

Пусть бент-функция f_n из $\mathcal{F}_n$ построена с использованием конструкции Майорана-Макфарланда ([Car 10,1]). При $n = 2m$, $\Phi = (\varphi_1, \dots, \varphi_m)$ — взаимно однозначном отображении $\mathbb{F}_2^m$ и h — произвольной функции из $\mathcal{F}_m$ бент-функция f_n имеет вид

$$f_n(z) = f(x, y) = \langle x, \Phi(y) \rangle \oplus h(y),$$

$z \in \mathbb{F}_2^n$, $x, y \in \mathbb{F}_2^m$. В работе [БуЛо 05,2] показано, что $la(f_n) = m$. Как следует из утверждения теоремы 14.10 при достаточно больших n для подавляющего большинства булевых функций из $\mathcal{F}_n$ уровень аффинности не менее $n - \lfloor \log_2 n \rfloor$.

Следовательно, при стремлении n к ∞ у функции f_n будут появляться значительно более мощные локальные аффинности, чем у случайной функции.

Кратко напомним, что булева функция $f_n \in \mathcal{F}_n$ называется корреляционно-иммунной порядка m , $1 \leq m \leq n$, если $\text{wt}(f_n \oplus l_{u,0}) = 2^{n-1}$ для любого $u \in \mathbb{F}_2^n$ такого, что $1 \leq \text{wt}(u) \leq m$. При этом

$$\text{cor}(f_n) = \max \{m \in \mathbb{N}_0 : f_n - \text{корр.-иммунна порядка } m\}$$

и $\deg f_n + \text{cor}(f_n) \leq n$ (неравенство Зигенталера).

В случае, если $\text{wt}(f_n) \neq 2^i$, $i = 0, 1, \dots, n-1$ известно (см. [БуЛо 05,2]), что $la(f_n) > \text{cor}(f_n)$. Следовательно, для данного класса функций при $n \rightarrow \infty$ увеличение порядка корреляционной иммунности m будет свидетельствовать

об отсутствии у этих функций мощных локальных аффинностей определенного вида (см. определение 14.5). Однако, следует отметить, что в этот класс входят лишь неуравновешенные функции (т.е. $\text{wt}(f_n) \neq 2^{n-1}$).

Уравновешенную корреляционно-иммунную булеву функцию порядка m обычно называют m -устойчивой. Рассмотрим рекурсивный класс устойчивых булевых функций, описанный в работе [Tap 02].

Пусть $(2n - 7)/3 \leq m \leq n - 2$. Тогда существует m -устойчивая булева функция $f_n \in \mathcal{F}_n$, для которой нелинейность достигает максимально возможного значения $nl(f_n) = 2^{n-1} - 2^{m+1}$. Доказательство этого утверждения конструктивно и проводится построение конкретной функции, обладающей необходимыми свойствами. Оказалось (см. [БуЛо 05,1]), что для таких функций выполнено неравенство

$$la(f_n) \leq \lfloor (m + 3)/2 \rfloor.$$

Из последнего неравенства, в частности, следует, что при достаточно больших n булева функция f_n имеет локальные аффинности (определяемые фиксацией переменных), размерность которых не менее $\lfloor n/2 \rfloor$.

§15 Аффинная нормальная форма булевой функции и ее свойства

Различные нормальные формы булевых функций (дизъюнктивная нормальная форма - ДНФ и конъюнктивная нормальная форма - КНФ [Ябл 10], [Чаш 12]; алгебраическая нормальная форма - АНФ и числовая нормальная форма - ЧНФ [Car 10,1], [ЛССЯ 15] и т.п.) использовались и используются в исследованиях разнообразных свойств булевых функций и отображений. Предпочтение той или иной нормальной форме отдается в зависимости от вида используемой в исследовании математической модели (математического аппарата) и характера решаемой в ходе исследования задачи. Каждая из нормальных форм

имеет свои особенности. Например, представление булевой функции с помощью ДНФ или КНФ не является однозначным, а представление с помощью АНФ (в соответствующем фактор-кольце) является однозначным.

В исследованиях, связанных с анализом информационной безопасности, активнее других используется АНФ. Однако, ряд задач обращения дискретных функций эффективно решаются с использованием локальных аффинностей соответствующих булевых функций и отображений.

В связи с этим актуальным является введение новой нормальной формы булевых функций и отображений на основе локальных аффинностей.

Пусть $\Phi \in \mathcal{F}_{n,m}$. Тогда

$$\mathbb{F}_2^n = \bigcup_{\pi \in P_{n,m}(\Phi)} \pi = \bigcup_{\pi \in M_{n,m}(\Phi)} \pi.$$

Определение 15.1. Совокупность $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ локальных аффинностей отображения Φ называется аффинным разбиением пространства $\mathbb{F}_2^n$ относительно отображения Φ , если выполнены условия

- а) $\bigcup_{i=1}^s \pi_i = \mathbb{F}_2^n$;
- б) $\pi_i \cap \pi_j = \emptyset$ при $i \neq j$.

Индикаторной (характеристической) функцией произвольного подмножества $\mathcal{D} \subset \mathbb{F}_2^n$, как обычно, будем называть функцию из $\mathcal{F}_n$ вида $I^{\mathcal{D}}(x) = \bigoplus_{u \in \mathcal{D}} \delta_u(x)$, где δ_u — функция Дирака, принимающая значение 1 лишь на наборе $u \in \mathbb{F}_2^n$.

В случае, когда $\mathcal{D} = \pi \in P_n$, $\dim \pi = r$, набор x из $\mathbb{F}_2^n$ принадлежит π тогда и только тогда, когда $xA \oplus b = 0^{n-r}$, где $A = (a_{ij})$ — некоторая $n \times (n-r)$ -матрица, $\text{rank } A = n-r$, $b \in \mathbb{F}_2^{n-r}$.

Тогда полином для характеристической функции плоскости π имеет вид

$$I^\pi(x) = \prod_{j=1}^{n-r} (x_1 a_{1j} \oplus \dots \oplus x_n a_{nj} \oplus b_j \oplus 1). \quad (15.1)$$

Рассмотрим аффинное разбиение $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ пространства $\mathbb{F}_2^n$ на локальные аффинности отображения $\Phi \in \mathcal{F}_{n,m}$, т.е. для любого $t = 1, 2, \dots, s$ существует аффинное отображение

$$G^t(x) = xC^t \oplus v^t,$$

где $C^t = (c_{ij}^t)$ - $n \times m$ матрица и $v^t \in \mathbb{F}_2^m$, такое, что $\Phi_{\pi_t} = G_{\pi_t}^t$. В случае $m = 1$ для булевой функции $f \in \mathcal{F}_n$ аналогично будем рассматривать аффинное разбиение $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ для этой функции, т.е. для любого $t = 1, 2, \dots, s$ существует аффинная функция

$$l^t(x) = \langle u^t, x \rangle \oplus \varepsilon^t,$$

где $u^t, x \in \mathbb{F}_2^n, \varepsilon^t \in \mathbb{F}_2$, такая, что $f_{\pi_t} = l^t$.

Определение 15.2. а) Пусть $\Phi \in \mathcal{F}_{n,m}, m \geq 2$. Аффинной нормальной формой (АффНФ) отображения Φ относительно аффинного разбиения $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ будем называть представление отображения Φ вида

$$\begin{aligned} \Phi(x) &= \bigoplus_{t=1}^s I^{\pi_t}(x) G^t(x) = \\ &= \bigoplus_{t=1}^s \prod_{j=1}^{n-\dim \pi_t} (x_1 a_{1j}^t \oplus \dots \oplus x_n a_{nj}^t \oplus b_j^t \oplus 1) [xG^t \oplus v^t]. \end{aligned} \quad (15.2)$$

б) Пусть $f \in \mathcal{F}_n$. Аффинной нормальной формой (АффНФ) булевой функции f относительно аффинного разбиения $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ будем

называть представление булевой функции f вида

$$\begin{aligned} f(x) &= \bigoplus_{t=1}^s \mathbb{I}^{\pi_t}(x) l^t(x) = \\ &= \bigoplus_{t=1}^s \prod_{j=1}^{n-\dim \pi_t} (x_1 a_{1j}^t \oplus \dots \oplus x_n a_{nj}^t \oplus b_j^t \oplus 1) l^t(x). \end{aligned} \quad (15.3)$$

Замечание 15.3. Очевидно, что булево отображение (функция) в виде аффинной нормальной формы представляется не однозначно. Имеется определенная свобода выбора аффинного разбиения пространства, зависящего от конечной цели такого представления.

Примеры аффинных нормальных форм некоторых криптографических отображений (функций) представлены в приложении Г.

Определение 15.4. *Длиной АффНФ отображения Φ (функции f) будем называть число плоскостей в аффинном разбиении пространства $\mathbb{F}_2^n$, задающем эту форму ((15.2), (15.3)).*

Следующая лемма будет полезна при исследовании преобразования Фурье-Адамара АффНФ булевых функций.

Лемма 15.5 ([ЛССЯ 15]). *Пусть $f \in \mathcal{F}_n$, $u, v \in \mathbb{F}_2^n$ и L — подпространство в $\mathbb{F}_2^n$. Тогда*

$$\sum_{x \in u \oplus L} (-1)^{f(x) \oplus \langle v, x \rangle} = 2^{\dim L - n} (-1)^{\langle u, v \rangle} \sum_{y \in v \oplus L^\perp} W_f(y) (-1)^{\langle u, y \rangle}. \quad (15.4)$$

Пусть $f \in \mathcal{F}_n$ и $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ — аффинное разбиение $\mathbb{F}_2^n$ относительно f . Предположим, что АффНФ функции f имеет вид

$$f(x) = \bigoplus_{t=1}^s \mathbb{I}^{\pi_t}(x) l^t(x), \quad (15.5)$$

где $l^t(x) = \langle u^t, x \rangle \oplus \varepsilon^t$, $u^t \in \mathbb{F}_2^n$, $\varepsilon^t \in \mathbb{F}_2$, $t = 1, 2, \dots, s$. Кроме того, пусть $\pi_t = b^t \oplus L_t$, где $b^t \in \mathbb{F}_2^n$ и L_t — подпространство $\mathbb{F}_2^n$, $t = 1, 2, \dots, s$. Справедливо следующее утверждение.

Теорема 15.6. *Для любого вектора $u \in \mathbb{F}_2^n$ справедливо равенство*

$$W_f(u) = \sum_{t=1}^s (-1)^{\langle u^t \oplus u, b^t \rangle \oplus \varepsilon^t} I_{L_t}^{\perp} (u^t \oplus u) 2^{\dim L_t}. \quad (15.6)$$

Доказательство. Следует из цепочки равенств, полученных с использованием утверждения леммы 15.5,

$$\begin{aligned} W_f(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle u, x \rangle} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\bigoplus_{t=1}^s I^{\pi_t}(x) [\langle u^t, x \rangle \oplus \varepsilon^t] \oplus \langle u, x \rangle} = \\ &= \sum_{x \in \pi_1} (-1)^{\langle u^1 \oplus u, x \rangle \oplus \varepsilon^1} + \dots + \sum_{x \in \pi_s} (-1)^{\langle u^s \oplus u, x \rangle \oplus \varepsilon^s} = \\ &= \sum_{y \in L_1} (-1)^{\langle u^1 \oplus u, y \oplus b^1 \rangle \oplus \varepsilon^1} + \dots + \sum_{y \in L_s} (-1)^{\langle u^s \oplus u, y \oplus b^s \rangle \oplus \varepsilon^s} = \\ &= \sum_{t=1}^s (-1)^{\langle u^t \oplus u, b^t \rangle \oplus \varepsilon^t} \sum_{y \in L_t} (-1)^{\langle u^t \oplus u, y \rangle} = \\ &= \sum_{t=1}^s (-1)^{\langle u^t \oplus u, b^t \rangle \oplus \varepsilon^t} I_{L_t}^{\perp} (u^t \oplus u) 2^{\dim L_t}. \end{aligned}$$

□

Следствие 15.7. *Пусть Π — аффинное разбиение пространства $\mathbb{F}_2^n$ относительно функции $f \in \mathcal{F}_n$ и $d = \min_{\pi \in \Pi} \dim \pi$. Тогда для любого $u \in \mathbb{F}_2^n$ коэффициент Уолша-Адамара $W_f(u)$ делится на 2^d .*

Доказательство. Вытекает непосредственно из утверждения теоремы 15.6. □

Теперь рассмотрим некоторые конструкции на основе аффинных разбиений, позволяющие строить криптографические функции из известных классов.

Напомним, что для четного n булева функция f из $\mathcal{F}_n$ называется бент-функцией, если $|W_f(u)| = 2^{n/2}$ для любого вектора $u \in \mathbb{F}_2^n$. Дуальной к бент-

функции f называют функцию $\tilde{f}$ из $\mathcal{F}_n$, задаваемую соотношениями $W_f(u) = 2^{n/2}(-1)^{\tilde{f}(u)}$ для любого $u \in \mathbb{F}_2^n$ (см. [ЛССЯ 15]).

Определение 15.8. Разбиения пространства $\mathbb{F}_2^n$ вида

$$\pi_1 = L_1 \oplus b^1, \pi_2 = L_2 \oplus b^2, \dots, \pi_s = L_s \oplus b^s \quad (15.7)$$

и

$$\pi'_1 = L_1^\perp \oplus a^1, \pi'_2 = L_2^\perp \oplus a^2, \dots, \pi'_s = L_s^\perp \oplus a^s, \quad (15.8)$$

где $L_1, \dots, L_s$ — подпространства $\mathbb{F}_2^n$, $a^1, \dots, a^s, b^1, \dots, b^s \in \mathbb{F}_2^n$, назовем дуальными. В случае $n = 2k$, $k \in \mathbb{N}$ дуальные разбиения (15.6), (15.7) будем называть центрально дуальными, если $\dim L_1 = \dim L_2 = \dots = \dim L_s = k$ и $s = 2^k$.

Теорема 15.9. Предположим, что $n = 2k, k \in \mathbb{N}$ и аффинные разбиения (15.7) и (15.8) для функции (15.5) центрально дуальны. Если векторы $u^1, \dots, u^{2^k}$ из $\mathbb{F}_2^n$ таковы, что $u^t \in \pi'_t = L_t^\perp \oplus a^t, t = 1, \dots, 2^k$ и $\varepsilon^1, \dots, \varepsilon^{2^k}$ из $\mathbb{F}_2$ — произвольные, то булева функция f , задаваемая АффНФ

$$f(x) = \bigoplus_{t=1}^{2^k} I^{\pi_t}(x) [\langle u^t, x \rangle \oplus \varepsilon^t]$$

является бент-функцией. Дуальная к f функция задается АффНФ вида

$$\tilde{f}(x) = \bigoplus_{t=1}^{2^k} I^{\pi'_t}(x) [\langle b^t, x \rangle \oplus \delta^t],$$

где $\delta^t = \varepsilon^t \oplus \langle u^t, b^t \rangle, t = 1, \dots, 2^k$.

Доказательство. Пусть $u \in \mathbb{F}_2^n$. Тогда, воспользовавшись утверждением теоремы 15.6, получаем

$$W_f(u) = 2^k \sum_{t=1}^{2^k} (-1)^{\langle u^t \oplus u, b^t \rangle \oplus \varepsilon^t} I_{L_t^\perp \oplus u^t}^\perp(u).$$

Так как наборы a^t и u^t принадлежат одной и той же плоскости $L_t^\perp \oplus u^t$, то мы имеем

$$L_t^\perp \oplus u^t = L_t^\perp \oplus a^t = \pi'_t.$$

Следовательно,

$$\begin{aligned} W_f(u) &= 2^k \sum_{t=1}^{2^k} (-1)^{\langle u^t \oplus u, b^t \rangle \oplus \varepsilon^t} I_{\pi'_t}^{\pi'_t}(u) = \\ &= 2^k (-1)^{\bigoplus_{t=1}^{2^k} I_{\pi'_t}^{\pi'_t}(u) [\langle u^t \oplus u, b^t \rangle \oplus \varepsilon^t]} = \\ &= 2^k (-1)^{\bigoplus_{t=1}^{2^k} I_{\pi'_t}^{\pi'_t}(u) [\langle u, b^t \rangle \oplus \delta^t]} = \\ &= 2^k (-1)^{\tilde{f}(u)}, \end{aligned}$$

где $\delta^t = \langle u^t, b^t \rangle \oplus \varepsilon^t$, $t = 1, \dots, 2^k$, а булева функция $\tilde{f}(u) = \bigoplus_{t=1}^{2^k} I_{\pi'_t}^{\pi'_t}(u) [\langle u, b^t \rangle \oplus \delta^t]$, определяющая знак коэффициента Уолша-Адамара функции f , является функцией, дуальной к функции f . $\square$

Следствие 15.10. *Предположим, что выполнены условия теоремы 15.9 и $L_1 = \dots = L_{2^k} = L$. Тогда бент-функция, определяемая этой теоремой, относится к классу бент-функций, доставляемому конструкцией Майорана - МакФарланда (см. пример 14.4).*

Доказательство. Непосредственно вытекает из утверждения теоремы 15.9. $\square$

Рассмотрим вопрос о максимальной возможной размерности локальной аффинности платовидной функции. Напомним, что булева функция f из $\mathcal{F}_n$ называется платовидной порядка $2r$, $0 \leq r \leq n$, если для любого набора $u \in \mathbb{F}_2^n$ выполнено включение $W_f^2(u) \in \{0, 2^{n-2r}\}$ (см. [ЛССЯ 15]). Легко видеть, что класс платовидных функций содержит в себе класс бент-функций, поскольку

любая бент-функция от n (n — четное) переменных является платовидной функцией порядка n .

Для доказательства оценки нам потребуется следующее утверждение.

Лемма 15.11 ([ЛССЯ 15]). Пусть $f \in \mathcal{F}_n$. Для любого d -размерного подпространства $L \subseteq \mathbb{F}_2^n$ и любого $u \in \mathbb{F}_2^n$ выполнено равенство

$$\sum_{t=1}^{2^{n-d}} \left(\sum_{x \in v^t \oplus L} (-1)^{f(x) \oplus \langle u, x \rangle} \right)^2 = 2^{-(n-d)} \sum_{y \in u \oplus L^\perp} W_f^2(y), \quad (15.9)$$

где $v^1 = 0^n, v^2, \dots, v^{2^{n-d}}$ — представители смежных классов $L \oplus v, v \in \mathbb{F}_2^n$.

Теорема 15.12. Пусть $f \in \mathcal{F}_n$ — платовидная булева функция порядка $2r$, $0 \leq r \leq n$. Тогда для любой локальной аффинности $\pi = v \oplus L$ из $P_n(f)$ выполняется неравенство $\dim \pi \leq n - r$.

Доказательство. Положим $d = \dim \pi = \dim L$. Выберем функцию $l(x) = \langle u, x \rangle \oplus \varepsilon$ ($u \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2^n$) такую, что $f_\pi = l_\pi$.

Рассмотрим слагаемое в левой части равенства (15.9), соответствующее индексу t такому, что $v^t \oplus L = v \oplus L = \pi$:

$$\left(\sum_{x \in v^t \oplus L} (-1)^{f(x) \oplus \langle u, x \rangle} \right)^2 = \left(\sum_{x \in v^t \oplus L} (-1)^\varepsilon \right)^2 = 2^{2d}.$$

Следовательно, имеем

$$2^{2d} \leq \sum_{t=1}^{2^k} \left(\sum_{x \in v^t \oplus L} (-1)^{f(x) \oplus \langle u, x \rangle} \right)^2. \quad (15.10)$$

Оценим сверху правую часть равенства (15.9) следующим образом:

$$\begin{aligned} 2^{-(n-d)} \sum_{y \in u \oplus L^\perp} W_f^2(y) &\leq 2^{-(n-d)} \# \{S_f \cap u \oplus L^\perp\} \cdot 2^{2n-2r} \leq \\ &\leq 2^{-(n-d)} \cdot 2^{n-d} \cdot 2^{2n-2r} = 2^{2n-2r}, \end{aligned} \quad (15.11)$$

где $S_f = \{v \in \mathbb{F}_2^n : W_f(v) = 2^{2n-2r}\}$. Из неравенств (15.10) и (15.11) следует, что $2^{2d} \leq 2^{2n-2r}$. Тогда

$$\dim \pi = d \leq n - r.$$

□

Утверждение теоремы 15.12 не только задает верхнюю границу для размерностей локальных аффинностей платовидных функций, но и совместно с утверждением теоремы ?? позволяет описать статистические свойства сужений таких функций относительно их локальных аффинностей. Эти статистические свойства используются при разработке методов анализа фильтрующих генераторов.

Замечание 15.13. В частности, из соотношения (15.9) следует, что если бент-функция $f \in \mathcal{F}_n$, $n = 2k$ удовлетворяет условию $f_\pi = c = \text{const}$, где π — плоскость имеет размерность $n/2 = k$, то f уравновешена на всех плоскостях вида $v \oplus \pi$, $v \in \mathbb{F}_2^n$ отличных от π . Кроме того, $\tilde{f}(0^n) = c$.

§16 Нелинейная аппроксимация булевых функций

Возможность аффинной (линейной) аппроксимации булевых функций с помощью множества функций $\{\langle u, x \rangle \oplus \varepsilon \mid u \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2^n\}$ определяются параметром — нелинейностью булевой функции (в криптоанализе) или радиусом покрытия кода Риды-Маллера первого порядка (в теории кодирования, см. [ЛССЯ 15]). Однако, в ходе решения задач обращения булевых отображений могут быть использованы нелинейные аппроксимации булевых функций.

Пусть $\{e_u(x), u \in \mathbb{F}_2^n\} \subset \mathcal{F}_n$. Систему из 2^n действительных функций $e_u(x), u, x \in \mathbb{F}_2^n$ будем называть биортогональным базисом, если выполнены условия

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{e_u(x)} (-1)^{e_v(x)} = 0, \text{ если } u \neq v, \quad (16.1)$$

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{e_u(x)} (-1)^{e_u(y)} = 0, \text{ если } x \neq y. \quad (16.2)$$

Это означает, что система функций $\{e_u(x)\}_{u \in \mathbb{F}_2^n}$ задает два ортогональных базиса в 2^n -мерном действительном векторном пространстве. Векторы первого базиса - это

$$\left((-1)^{e_u(x^1)}, \dots, (-1)^{e_u(x^{2^n})} \right), \text{ для всех } u \in \mathbb{F}_2^n,$$

векторы второго - это

$$\left((-1)^{e_{u^1}(x)}, \dots, (-1)^{e_{u^{2^n}}(x)} \right), \text{ для всех } x \in \mathbb{F}_2^n;$$

здесь $\{x^1, \dots, x^{2^n}\}, \{u^1, \dots, u^{2^n}\}$ — две произвольные фиксированные нумерации элементов пространства $\mathbb{F}_2^n$. На языке матриц условия (16.1), (16.2) означают, что матрица $[(-1)^{e_u(x)}]_{u, x \in \mathbb{F}_2^n}$ размера $2^n \times 2^n$ является матрицей Адамара по строкам (условие (16.1)) и по столбцам (условие (16.2)).

Известно, что любой вектор однозначно разлагается по ортогональному базису, причем коэффициенты разложения легко выражаются с помощью операции скалярного произведения. Применительно к интересующему нас случаю булевых функций это разложение и выражения для коэффициентов выглядят следующим образом

$$\check{f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{e_u(x)}, \text{ для всех } u \in \mathbb{F}_2^n, \quad (16.3)$$

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in \mathbb{F}_2^n} \check{f}(u) (-1)^{e_u(x)}, \text{ для всех } x \in \mathbb{F}_2^n. \quad (16.4)$$

Обозначение $\check{f}(u)$ и нормирующий коэффициент выбраны так, чтобы в случае $e_u(x) = \langle u, x \rangle$ получить $\check{f}(u) = W_f(u)$ и возвратиться к преобразованию Уолша-Адамара. Рассмотрим следующий важный класс биортогональных базисов.

Пример 16.1. Пусть $n = k + 2l$ и поэтому любой вектор $x \in \mathbb{F}_2^n$ можно представить в виде $x = (x^{(1)}, x^{(2)})$, где $x^{(1)} \in \mathbb{F}_2^k$, $x^{(2)} \in \mathbb{F}_2^{2l}$. Пусть $\varphi(x^{(2)})$ — некоторая бент-функция из $\mathcal{B}_{2l} \subset \mathcal{F}_{2l}$. Положим

$$\begin{aligned} e_u(x) &= e_{(u^{(1)}, u^{(2)})} (x^{(1)}, x^{(2)}) = \\ &= \langle u^{(1)}, x^{(1)} \rangle \oplus \varphi(x^{(2)} \oplus u^{(2)}). \end{aligned}$$

Тогда система функций $\{e_u(x)\}_{u \in \mathbb{F}_2^n}$ является биортогональным базисом. Условия (16.1), (16.2) легко проверяются с учетом того, что $\varphi(x^{(2)})$ — бент-функция:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{e_u(x)} (-1)^{e_v(x)} = \sum_{x^{(1)} \in \mathbb{F}_2^k} (-1)^{\langle u^{(1)} \oplus v^{(1)}, x^{(1)} \rangle} \sum_{x^{(2)} \in \mathbb{F}_2^{2l}} (-1)^{\varphi(x^{(2)} \oplus u^{(2)}) \oplus \varphi(x^{(2)} \oplus v^{(2)})} = 0,$$

если $(u^{(1)}, u^{(2)}) \neq (v^{(1)}, v^{(2)})$;

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{e_u(x)} (-1)^{e_u(y)} = \sum_{u^{(1)} \in \mathbb{F}_2^k} (-1)^{\langle u^{(1)}, x^{(1)} \oplus y^{(1)} \rangle} \sum_{u^{(2)} \in \mathbb{F}_2^{2l}} (-1)^{\varphi(x^{(2)} \oplus u^{(2)}) \oplus \varphi(y^{(2)} \oplus u^{(2)})} = 0,$$

если $(x^{(1)}, x^{(2)}) \neq (y^{(1)}, y^{(2)})$.

Заметим, что на языке теории кодирования из равенства (16.3) легко получить выражение для расстояния Хэмминга от вектора значений булевой функции $f(x)$ до вектора значений булевой функции $e_u(x)$:

$$\text{dist}(f(x), e_u(x)) = 2^{n-1} - \frac{1}{2} \check{f}(u). \quad (16.5)$$

Отсюда, в частности, следует, что ближе всего (в смысле расстояния Хэмминга) к функции $f(x)$ из системы функций $\{e_u(x)\}_{u \in \mathbb{F}_2^n}$ лежит функция $e_{u^0}(x)$ с тем индексом $u^0 \in \mathbb{F}_2^n$, для которого число $\check{f}(u^0)$ максимально среди всех $\check{f}(u)$. Таким образом, задача аппроксимации булевой функции элементами биортогонального базиса сведена к задаче нахождения $\max_{u \in \mathbb{F}_2^n} \check{f}(u)$.

Определение 16.2. *Обобщенным кодом Адамара $H(e_u(x))$ назовем множество строк, которые являются векторами значений булевых функций $e_u(x)$, $e_u(x) \oplus 1$, $u \in \mathbb{F}_2^n$, где $\{e_u(x)\}_{u \in \mathbb{F}_2^n}$ некоторый биортогональный базис.*

Обобщенный код Адамара, вообще говоря, нелинейный, кроме случая $e_u(x) = \langle u, x \rangle$, когда обобщенный код Адамара совпадает с кодом Рида-Маллера первого порядка. Справедливо следующее утверждение.

Теорема 16.3 ([ЛСЯ 04,3]). *Произвольный обобщенный код Адамара имеет следующие параметры:*

- а) длина — 2^n ;
- б) мощность — 2^{n+1} ;
- в) кодовое расстояние — 2^{n-1} ;
- г) радиус покрытия — $\leq 2^{n-1} - 2^{n/2-1}$.

Утверждение теоремы 16.3 показывает, что потенциальные возможности "нелинейной" аппроксимации не меньше, чем у "линейной". Ниже будет найден радиус покрытия для некоторых обобщенных кодов Адамара, построенных с помощью бент-функций (см. пример 16.1).

Теорема 16.4. *Пусть $n = 2m + 2l$ и $\varphi(z)$ — некоторая бент-функция из $\mathcal{B}_{2l} \subset \mathcal{F}_{2l}$. Тогда радиус покрытия обобщенного кода Адамара $H(e_u(x))$, где*

$$\begin{aligned} e_u(x) &= e_{(u^{(1)}, u^{(2)})} \left(x^{(1)}, x^{(2)} \right) = \\ &= \langle u^{(1)}, x^{(1)} \rangle \oplus \varphi \left(x^{(2)} \oplus u^{(2)} \right), \end{aligned}$$

$u^{(1)}, x^{(1)} \in \mathbb{F}_2^{2m}, u^{(2)}, x^{(2)} \in \mathbb{F}_2^{2l}$, равен $2^{n-1} - 2^{\frac{n}{2}-1}$.

Доказательство. С учетом утверждения теоремы 16.3 достаточно показать достижимость в нашем случае неравенства

$$\min_f \max_{u \in \mathbb{F}_2^n} |\check{f}(u)| \leq 2^{n/2}$$

для некоторой булевой функции f . Положим

$$f(x) = f(x^{(1)}, x^{(2)}) = \psi(x^{(1)}) \oplus \langle a, x^{(2)} \rangle,$$

где $x^{(1)} \in \mathbb{F}_2^{2m}$, $a, x^{(2)} \in \mathbb{F}_2^{2l}$, $\psi(x^{(1)})$ — некоторая бент-функция из $\mathcal{B}_{2m} \subset \mathcal{F}_{2m}$. В соответствии с (16.3) имеем

$$\begin{aligned} \check{f}(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{e_u(x)} = \\ &= \sum_{x^{(1)} \in \mathbb{F}_2^{2m}} (-1)^{\psi(x^{(1)})} (-1)^{\langle u^{(1)}, x^{(1)} \rangle} \sum_{x^{(2)} \in \mathbb{F}_2^{2l}} (-1)^{\varphi(x^{(2)} \oplus u^{(2)})} (-1)^{\langle a, x^{(2)} \rangle} = \\ &= (\pm 2^m) \cdot (\pm 2^l) = \pm 2^{n/2} \end{aligned}$$

для всех $u = (u^{(1)}, u^{(2)}) \in \mathbb{F}_2^n$, поскольку $\varphi(x^{(2)})$ и $\psi(x^{(1)})$ — бент-функции. $\square$

Сравним теперь возможности аппроксимаций — "линейной" (аффинными функциями $\langle u, x \rangle \oplus \varepsilon$) и "нелинейной" (функциями вида $\langle u^{(1)}, x^{(1)} \rangle \oplus \varphi(x^{(2)} \oplus u^{(2)}) \oplus \varepsilon$). В общем случае для выбора лучшего варианта аппроксимации достаточно сравнить два числа $\max_{u \in \mathbb{F}_2^n} |W_f(u)|$ и $\max_{u \in \mathbb{F}_2^n} |\check{f}(u)|$. Большее число укажет, элементами какого базиса данная функция приближается лучше. Реализация этого сравнения предполагает большой объем вычислений для нахождения $\max_{u \in \mathbb{F}_2^n} |W_f(u)|$ и $\max_{u \in \mathbb{F}_2^n} |\check{f}(u)|$. Некоторое сокращение объемов при вычислении величин $W_f(u)$ возможно за счет использования быстрого преобразования Адамара (Фурье). Однако, оказывается, что некоторые предварительные выво-

ды могут быть сделаны при наличии определенных соотношений между $W_f(u)$ и $\check{f}(u)$. Рассмотрим одно из таких соотношений.

Лемма 16.5. *Для любой булевой функции $f \in \mathcal{F}_n$, $n = k + 2l$ и для любой системы функций*

$$e_u(x) = e_{(u^{(1)}, u^{(2)})} \left(x^{(1)}, x^{(2)} \right) = \langle u^{(1)}, x^{(1)} \rangle \oplus \varphi \left(x^{(2)} \oplus u^{(2)} \right) \oplus \varepsilon$$

из примера 16.1 выполнено соотношение

$$\check{f}(u) = \frac{1}{2^l} \sum_{v^{(2)} \in \mathbb{F}_2^{2l}} (-1)^{\langle v^{(2)}, u^{(2)} \rangle} (-1)^{\tilde{\varphi}(v^{(2)})} W_f \left(u^{(1)}, v^{(2)} \right), \quad (16.6)$$

где $\tilde{\varphi}(v^{(2)})$ — дуальная бент-функция к функции $\varphi(x^{(2)})$.

Доказательство. Подставим выражения для обратных преобразования Уолша-Адамара

$$(-1)^{f(x)} = 2^{-n} \sum_{v \in \mathbb{F}_2^n} W_f(v) (-1)^{\langle v, x \rangle}$$

и

$$(-1)^{e_u(x)} = 2^{-n} \sum_{w \in \mathbb{F}_2^n} W_{e_u}(w) (-1)^{\langle w, x \rangle}$$

в выражение для $\check{f}(u)$ (16.3) и выполним необходимые преобразования

$$\begin{aligned} \check{f}(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{e_u(x)} = \\ &= \sum_{x \in \mathbb{F}_2^n} \left(2^{-n} \sum_{v \in \mathbb{F}_2^n} W_f(v) (-1)^{\langle v, x \rangle} \right) \left(2^{-n} \sum_{w \in \mathbb{F}_2^n} \hat{e}_u(w) (-1)^{\langle w, x \rangle} \right) = \\ &= 2^{-2n} \sum_{v, w \in \mathbb{F}_2^n} W_f(v)(w) \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{\langle v, x \rangle} (-1)^{\langle w, x \rangle} \right) = \\ &= 2^{-n} \sum_{v \in \mathbb{F}_2^n} W_f(v)(v). \end{aligned} \quad (16.7)$$

Выражение для $W_{e_u}(v)$ легко находится

$$\begin{aligned}
\hat{e}_u(v) &= \sum_{\substack{x^{(1)} \in \mathbb{F}_2^k \\ x^{(2)} \in \mathbb{F}_2^{2l}}} (-1)^{\langle u^{(1)}, x^{(1)} \rangle} (-1)^{\varphi(x^{(2)} \oplus u^{(2)})} (-1)^{\langle v^{(1)}, x^{(1)} \rangle} (-1)^{\langle v^{(2)}, x^{(2)} \rangle} = \\
&= \sum_{x^{(1)} \in \mathbb{F}_2^k} (-1)^{\langle u^{(1)} \oplus v^{(1)}, x^{(1)} \rangle} \sum_{x^{(2)} \in \mathbb{F}_2^{2l}} (-1)^{\varphi(x^{(2)} \oplus u^{(2)})} (-1)^{\langle v^{(2)}, x^{(2)} \rangle} = \\
&= \begin{cases} 0 & , \text{ если } u^{(1)} \neq v^{(1)}, \\ (-1)^{\langle u^{(2)}, v^{(2)} \rangle} (-1)^{\tilde{\varphi}(v^{(2)})} \cdot 2^{k+l} & , \text{ если } u^{(1)} = v^{(1)}. \end{cases}
\end{aligned}$$

Подставляя полученное выражение в (16.7), получим (16.5). □

Глава 3. Математические модели обращения дискретных функций

§17 Задача обращения дискретных функций в обеспечении информационной безопасности

Математические модели средств обеспечения информационной безопасности, как правило, представляют собой некоторые совокупности функций, имеющих дискретные области определения и значения. Типичными примерами таких областей являются подмножества строк конечной длины с компонентами, принадлежащими некоторому конечному или счетному алфавиту. Известно, что множество слов в таком алфавите перечислимо тогда и только тогда, когда перечислимо множество кодов этих слов. Таким образом, для задания любого перечислимого множества достаточно, по существу, алфавита $\{0,1\}$.

Например, в теории рекурсии (вычислимости, см. [Rog 67], [Мал 86]) принято в качестве основного алфавита использовать множество натуральных чисел. С другой стороны, в теории сложности вычислений (см. [ArBa 09]), а также в математической криптографии (см. [Gol 01], [Gol 04]) при формулировании основных понятий и результатов, проведении необходимых математических рассуждений используют основной алфавит $\{0,1\}$ (наряду с $\{0,1\}^*$). Вместе с тем, необходимо отметить также и то, что в ходе математических рассуждений имеют место погружения двоичного алфавита как в конечные поля характеристики 2, так и в комплексную (действительную) область.

Для описания вариантов задач обращения дискретных функций в данном параграфе мы будем использовать алфавит $\{0,1\}$.

К дискретным устройствам, реализующим такие функциональности, как шифрование (в том числе гомоморфное), хэширование, аутентификация, имитозащита, электронная подпись и т.п., предъявляется ряд жестких требований по

обеспечению защиты от различных атак. В соответствующих математических моделях должны использоваться дискретные функции с определенными свойствами. Одно из важнейших свойств качественно можно описать следующим образом.

При заданном значении аргумента значение функции на нем вычисляется эффективно, а при известном значении функции определение соответствующего этому значению прообраза является сложной математической задачей. Необходимо отметить, что эффективными вычислениями (в теории сложности вычислений) в настоящее время принято считать полиномиальные вычисления такие, в которых объем вычислений не превышает значения некоторого полинома от длины входных данных в подходящей кодировке (тезис Эдмондса — см. [ArBa 09]).

В теоретическом плане, в рамках теоретико-сложностного подхода, класс дискретных функций, обладающих описанным выше свойством, вводится на основе понятия "односторонняя" функция (см. [ArBa 09], [Gol 01]).

Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^*$ и для произвольного $y \in f(\{0,1\}^*)$ через $f^{-1}(y)$ обозначим его полный прообраз, т.е. $f^{-1}(y) = \{x \in \{0,1\}^* \mid f(x) = y\}$.

Определение 17.1 ([Gol 01]). *Функция*

$$f : \{0,1\}^* \rightarrow \{0,1\}^*$$

называется односторонней, если выполнены следующие два условия:

1. *Существует (детерминированный) полиномиальный алгоритм A такой, что для любого $x \in \{0,1\}^*$ алгоритм A вычисляет $f(x)$ (т.е. $A(x) = f(x)$).*
2. *Для любого вероятностного полиномиального алгоритма A' , любого положительного полинома $p(\cdot)$ и достаточно большого $n \in \mathbb{N}$*

$$\Pr [A'(f(U_n), 1^n) \in f^{-1}(f(U_n))] < 1/p(n),$$

где U_n — случайная величина, равномерно распределенная на $\{0,1\}^n$.

Рассмотрим подробнее некоторые аспекты понятия, вводимого определением 17.1.

Во-первых, область определения "односторонней функции" постулируется как бесконечное (счетное) множество. Во-вторых, основное соотношение (неравенство), описывающее для функции свойство "быть односторонней", имеет асимптотический характер. Следовательно, определить аналогичное понятие для "конечных" дискретных функций (с учетом двоичного кодирования) не представляется возможным.

В анализе конкретных средств обеспечения информационной безопасности их математические модели представляют собой некоторые композиции функций (отображений), определяемых на конечных множествах. Поэтому теоретико-сложностной подход, основанный на понятии "односторонней функции", к таким моделям неприменим.

Однако, в теоретико-сложностном подходе присутствуют некоторые варианты частичного обращения функций. Термин "частично" обозначает здесь восстановление (в процессе обращения) лишь некоторой информации о неизвестном прообразе, не позволяющей идентифицировать его однозначно. Один из таких подходов реализуется на основе понятия "трудный предикат" функции (см. [Gol 01], [ArBa 09]).

Определение 17.2 ([Gol 01]). Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^*$. Полиномиально вычислимый предикат

$$b : \{0,1\}^* \rightarrow \{0,1\}$$

называется трудным для функции f , если для любого вероятностного полиномиального алгоритма A' , любого положительного полинома $p(\cdot)$ и любого достаточно большого n выполнено

$$\Pr [A'(f(U_n)) = b(U_n)] < 1/2 + 1/p(n).$$

Таким образом, попытки эффективно вычислить значение трудного предиката $b(U_n)$ по существу не отличимы от выбора случайного бита, имеющего равномерное распределение.

Конкретный вид трудного предиката для функции доставляет следующее утверждение (см. [Gol 01]).

Теорема 17.3 ([Gol 01]). Пусть f — односторонняя функция и функция g определяется соотношением

$$g(x, r) = (f(x), r)$$

где x, r — строки одинаковой длины из $\{0, 1\}^*$.

Тогда предикат $b(x, r) = \langle x, r \rangle$ является трудным предикатом для функции g .

"Трудный предикат" в данном утверждении представляет собой некоторое линейное соотношение, выполненное для строки x . В частном случае, когда вес строки r равен единице, трудный предикат совпадает с некоторым битом строки x .

Как было отмечено ранее, к задаче оценки сложности обращения конкретной "конечной" дискретной функции неприменим математический аппарат, имеющийся в настоящее время в теории сложности вычислений.

Поэтому проводятся исследования по разработке алгоритмов и методов решения задачи обращения функции из данного конкретного класса с последующей оценкой их трудоемкости. Полученные результаты косвенным образом характеризуют сложность задачи обращения.

Перейдем теперь к формальному описанию интересующих нас классов задач обращения.

Пусть $n, m \in \mathbb{N}$ и $f : \{0, 1\}^* \rightarrow \{0, 1\}^m$. Рассмотрим пару подмножеств $S \subset \{0, 1\}^m$ и $D \subset f^{-1}(S) \cap \{0, 1\}^n$.

Под общей (S,D)-задачей обращения функции f будем понимать задачу поиска аналитических соотношений, которым удовлетворяют элементы подмножества D при известных f , S и n .

Функция f может задаваться разнообразными способами. Чаще всего она бывает представлена в виде композиции некоторого числа функций-компонент. Другим часто встречающимся способом представления f является система булевых функций (реализованных с использованием ДНФ, КНФ, АНФ и т.п.). Множества S и D также могут быть представлены различными способами.

Конкретные виды подмножеств S и D определяют частные виды задач обращения функции f . Говоря о задаче обращения, мы будем опускать пару (S,D), поскольку, как правило, из контекста всегда ясно, о каких подмножествах идет речь. Для удобства (если это возможно) будем говорить о задаче обращения функции $f' \in \mathcal{F}_{n,m}$, где $f_{\{0,1\}^n} = f'$.

Не претендуя на полноту, рассмотрим наиболее известные формулировки задач обращения дискретных функций.

Пример 17.4. а) Пусть $f \in \mathcal{F}_{n,m}$, $S = \{y\} \subset \{0,1\}^m$,

$$D = f^{-1}(S) = f^{-1}(\{y\}).$$

Описать (функционально, таблично и т.п.) полный прообраз элемента y из $\{0,1\}^m$. Данная задача эквивалентна задаче построения характеристической (индикаторной) функции $I_{f^{-1}(\{y\})}$.

б) Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^m$, $S = \{y\} \subset \{0,1\}^m$, $D = \{0,1\}^*$.

Найти (вычислить) какой-либо элемент из множества

$$f^{-1}(\{y\}) \subset D.$$

в) Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^m$, $S = \{y\} \subset \{0,1\}^m$, $D = \{0,1\}^*$.

Найти (вычислить) пару элементов $x, x' \in f^{-1}(\{y\}) \subset D$, $x \neq x'$.

г) Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^m$, $S = \{y\} \subset \{0,1\}^m$, $D = \{0,1\}^*$ и известно, что $f(x) = y$, $x \in \{0,1\}^*$.

Найти (вычислить) элемент $x' \in f^{-1}(\{y\})$, $x' \neq x$.

е) Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^m$, $S = \{y\} \subset \{0,1\}^m$, $D = \{0,1\}^*$.

Найти (вычислить) для некоторого неизвестного $x \in f^{-1}(\{y\})$,

$x \in \{0,1\}^n$ его какой-нибудь фрагмент $(x_{j_1}, x_{j_2}, \dots, x_{j_r})$, $1 \leq j_1 < \dots < j_r \leq n$, $r \leq n$.

ф) Пусть $f : \{0,1\}^* \rightarrow \{0,1\}^m$, $S = \{y\} \subset \{0,1\}^m$, $D = \{0,1\}^*$.

Найти отображение $\varphi : \{0,1\}^n \rightarrow \{0,1\}^r$ такое, что выполнено

$$f(x) = y \quad \Rightarrow \quad \varphi(x) = 0^r,$$

и последнее уравнение эффективно решается (например, φ — аффинное или треугольное отображение).

Важнейшим классом функций, возникающим в теории информационной безопасности, является класс ограниченно-детерминированных функций, то есть функций, реализуемых конечными автоматами. Рассмотрим некоторые примеры таких функций, связанных с генераторами псевдослучайных последовательностей.

Одним из важных требований к генераторам псевдослучайных последовательностей является сложность задачи нахождения начального состояния (ключа) генератора по известной выходной последовательности и известном строении генератора. В данном случае эта задача эквивалентна задаче обращения функции f из $\mathcal{F}_{n,m}$, $n < m$ с множествами $\mathcal{S} = \{y\} \subset \{0,1\}^m$ и $D = \{s\} \subset \{0,1\}^n$.

Основные свойства фильтрующего генератора определяются булевой функцией f , с помощью которой задается функция f_m . В научной литературе имеется значительное число публикаций, посвященных изучению свойств фильтрующих функций, а также разработке критериев выбора этих функций. С обширной библиографией по этому вопросу можно ознакомиться, например, по книгам [ЛССЯ 15], [CuSt 09], [Car 10,1], [Car 10,2]. Рассмотрим фильтру-

ющие функции из класса симметрических функций $\mathcal{S}_n$ ($\mathcal{S}_n \subset \mathcal{F}_n$) и из класса ротационно-симметрических функций — $\mathcal{RS}_n$ ($\mathcal{S}_n \subset \mathcal{RS}_n \subset \mathcal{F}_n$).

Пусть $G = \text{Sym}_n$ — симметрическая группа степени n (см. [Wiel 64]) и $\mathcal{S}_n$ ($\mathcal{S}_n \subset \mathcal{F}_n$) — класс симметрических функций от n переменных. Функция f из $\mathcal{F}_n$ принадлежит классу $\mathcal{S}_n$, если для любой перестановки $\sigma \in \text{Sym}_n$ выполнены соотношения

$$\begin{aligned} f^\sigma(x_1, x_2, \dots, x_n) &= f(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(n)}) = \\ &= f(x_1, x_2, \dots, x_n). \end{aligned}$$

Функция f называется ротационно-симметрической, если для полного цикла $\tau = (1, 2, \dots, n) \in \text{Sym}_n$ выполнено соотношение

$$f^\tau(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n).$$

Симметрические функции обладают рядом положительных свойств с точки зрения использования их при синтезе криптографических примитивов. Например, одним из таких свойств является возможность эффективной схемной реализации. В научной литературе опубликован ряд результатов исследований криптографических свойств симметрических булевых функций. Упомянем лишь некоторые из них. В работах [Goug 04], [CaVi 05], [MaSa 02], [Car 04] исследовалась нелинейность симметрических функций. Вопросы, связанные с корреляционной иммунностью симметрических булевых функций рассмотрены, например, в [GHS 93], [BGS 94], [Mit 90], [YaGu 95], [CaVi 05], [SaMa 07]. Алгебраическая иммунность симметрических функций изучалась в [QLF 07], [LiQi 06], [Br Pr 05], [LiuF 07]. Результаты аналогичных исследований для ротационно-симметрических функций можно найти в [FiFo 98], [SMC 04], [KMY 07], [LaVi 08].

Рассмотрим теперь содержательный пример, описывающий одну из задач обращения фильтрующего генератора.

Пример 17.5. Пусть $FG = \text{LFSR}(c(\lambda), f)$ — фильтрующий генератор (см. Приложение А в)), состоящий из регистра сдвига с линейными обратными связями $\text{LFSR}(n, c(\lambda))$ и фильтрующей функции $f \in \mathcal{F}_n$. Начальное заполнение регистра сдвига $s = (s_0, s_1, \dots, s_{n-1})$ является секретным ключом генератора. Конечная строка $s^{m+n-1} = (s_0, s_1, \dots, s_{m+n-2})$ представляет собой фрагмент линейной рекуррентной последовательности (ЛРП) с характеристическим полиномом $c(\lambda)$, вырабатываемой регистром $\text{LFSR}(n, c(\lambda))$. Выходные символы фильтрующего генератора FG определяются соотношениями

$$y_i = f(sB^i), i = 0, 1, \dots, m-1,$$

где B — сопровождающая матрица регистра $\text{LFSR}(n, c(\lambda))$, т.е. $y = f_m(s^{m+n-1})$, где $f_m: \{0,1\}^{m+n-1} \rightarrow \{0,1\}^m$, $f_m(s_0, \dots, s_{n-1}, s_n, \dots, s_{m+n-2}) = (f(s_0, \dots, s_{n-1}), f(s_1, \dots, s_n), \dots, f(s_m, \dots, s_{m+n-2}))$. Рассмотрим задачу определения начального состояния s генератора FG по выходной последовательности y .

Будем считать, что $f_m(s_0, s_1, \dots, s_{m+n-2}) \neq 0^m, 1^m$. Воспользовавшись этим предположением, найдем произвольный индекс i , $0 \leq i \leq m-2$ такой, что $y_i \oplus y_{i+1} = 1$ (т.е. соседние компоненты строки y не совпадают). Кратко это событие называют - "знакоперемена". Данные компоненты определяются соотношениями

$$\begin{aligned} y_i &= f(s_i, s_{i+1}, \dots, s_{i+n-1}), \\ y_{i+1} &= f(s_{i+1}, s_{i+2}, \dots, s_{i+n}). \end{aligned}$$

Поскольку $f \in S_n$, то выполнение соотношения $y_i \oplus y_{i+1} = 1$ свидетельствует о том, что

$$\text{wt}(s_i, s_{i+1}, \dots, s_{i+n-1}) \neq \text{wt}(s_{i+1}, s_{i+2}, \dots, s_{i+n}).$$

Легко видеть, что для разности весов этих векторов справедливо равенство

$$\left| \sum_{t=i}^{i+n-1} s_t - \sum_{r=i+1}^{i+n} s_r \right| = |s_i - s_{i+n}| = 1,$$

т.е. $s_i \oplus s_{i+n} = 1$. Напомним, что $(s_0, s_1, \dots, s_{m+n-2})$ является фрагментом линейной рекуррентной последовательности, вырабатываемой регистром $\text{LFSR}(n, c(\lambda))$. Следовательно, любая компонента строки s^{m+n-1} является суммой некоторых компонент начального заполнения $s = (s_0, s_1, \dots, s_{n-1})$ этого регистра.

Пусть $y_i = l^i(s) = \langle u^i, s \rangle$, где $l^i \in \mathcal{L}_n$, $u^i \in \{0,1\}^n$. Тогда соотношение $s_i \oplus s_{i+1} = 1$ задает линейное уравнение

$$\begin{aligned} s_i \oplus s_{i+1} &= l^i(s) \oplus l^{i+1}(s) = \langle u^i, s \rangle \oplus \langle u^{i+1}, s \rangle = \\ &= \langle u^i \oplus u^{i+1}, s \rangle = \langle v^i, s \rangle = 1 \end{aligned}$$

относительно неизвестного начального состояния s фильтрующего генератора. Если в строке y имеется m_0 , $m_0 < m$, (естественное предположение для хорошего генератора псевдослучайных чисел) знакоперемен и $\text{rank}\{v^i, i = 1, \dots, m_0\} = n$, то порожденная система линейных уравнений

$$\begin{cases} \langle v^1, s \rangle = 1 \\ \langle v^2, s \rangle = 1 \\ \vdots \\ \langle v^{m_0}, s \rangle = 1 \end{cases}$$

однозначно определяет начальное состояние s фильтрующего генератора $LFSR(f, c(\lambda))$. Таким образом, метод решения определенной выше задачи обращения для фильтрующего генератора состоит из трех этапов:

- выделение знакоперемен в строке y ;
- формирование линейной системы;
- решение линейной системы.

В работе [ЛоНа 07] получены полиномиальные (от n) оценки трудоемкости этапов этого метода, а также другие его параметры.

Необходимо отметить, что все рассуждения, приведенные выше для симметрических функций, остаются справедливыми и для ротационно-симметрических функций.

Приведенный пример показывает, что принципиальным (с точки зрения решения задачи обращения) может оказаться для функции не собственные ее "функциональные" свойства, а свойства, отображающие взаимодействие данной функции с различными элементами изучаемого дискретного устройства. Таким образом, актуальным является изучение алгоритмов и методов решения задач обращения для ограниченно-детерминированных (конечно-автоматных) функций.

§18 Теоретико-автоматная модель для задачи обращения

Вопросы восстановления информации о входных последовательностях конечных автоматов (как этапа решения задач обращения ограниченно-детерминированных функций) при соответствующих известных выходных последовательностях нашли свое отражение в классических монографиях по теории автоматов (см. [Ги 66], [Ги 74], [ТраБ 70], [ГеР 72], [КАП 85] и др.), так и в работах, посвященных специально данной тематике.

Задачи восстановления неизвестного входного слова конечного автомата исследовались ранее рядом авторов в различных аспектах: декодирование автоматного кодирования информации, эксперименты с автоматами и их диагностирование и т.п. При этом возможности восстановления существенно зависят от двух факторов: от известной информации о свойствах автомата и от точности, с которой необходимо восстановить входное слово. Сам автомат считается конечным, детерминированным и известным.

В [Ги 66], [Huf 59,1], [Huf 59,2] исследовались задачи однозначного восстановления входного слова по известным начальному состоянию, выходному слову и финальному состоянию автомата. В [Спе 71] рассматривалась задача однозначного восстановления входного слова по тем же данным, за исключением начального состояния. В [Спе 71], [Спе 72,1], [Кур 72], [Ев 65], [Тао 08] изучалась структура автоматов, для которых возможно частичное восстановление входного слова. В [Спе 72,2], [Dot 70] рассматривалась задача однозначного восстановления входного слова по известному выходному слову длины не большей, чем некоторое натуральное число, и известной информации о финальном состоянии автомата. Обратимость автоматов некоторого конкретного типа исследовалась в [Pre 66]. В [Сид 65] при некоторых ограничениях на структуру конечного автомата получено соотношение между энтропиями марковского источника и источника, полученного в результате подсоединения исходного марковского источника к конечному автомату. Необходимо также отметить [LiMa 95], где задача частичного обращения дискретных функций исследовалась методами символической динамики.

Вопросы частичного обращения дискретных функций нашли свое отражение и в теории сложности вычислений. В частности, в [GoLe 89] изучалась сложность восстановления отдельных битов аргумента дискретной функции по известному ее значению.

Нас будет интересовать задача частичного восстановления входного слова конечного автомата по известному выходному слову. Термин "частичное восста-

новление" означает восстановление фрагментов входной последовательности. Предлагаемая математическая модель частичного обращения конечного автомата представляет собой конечный автомат — так называемый частично-обратный автомат (ЧО-автомат).

Пусть $\mathcal{M} = (A, Q, B, \varphi, \psi)$ — абстрактный конечный автомат Мили, где A, Q, B — соответственно, входной, внутренний (состояния автомата) и выходной алфавиты, являющиеся конечными множествами, $\#A = u$, $\#Q = v$, $\#B = w$.

Отображения

$$\varphi : Q \times A \rightarrow Q \text{ и } \psi : Q \times A \rightarrow B —$$

функции переходов и выходов автомата $\mathcal{M}$ соответственно. Через $\varphi_a : Q \rightarrow Q$ и $\psi_q : A \rightarrow B$ ($a \in A$, $q \in Q$) будем обозначать соответственно частичную функцию переходов и частичную функцию выходов автомата $\mathcal{M}$:

$$\varphi_a(q) = \varphi(q, a), \psi_q(a) = \psi(q, a).$$

Через $\psi_q^{-1}(b)$ будем обозначать полный прообраз элемента $b \in B$ при отображении ψ_q . Функции переходов и выходов распространим на $Q \times A^*$ следующим образом: для $q \in Q$ и $\alpha = a_1 a_2 \dots a_k \in A^*$ положим

$$\varphi(q, \alpha) = q_1 q_2 \dots q_k \in Q^*, \quad (18.1)$$

где $q_1 = \varphi(q, a_1)$, $q_2 = \varphi(q_1, a_2)$, $\dots$, $q_k = \varphi(q_{k-1}, a_k)$, и $\varphi(q, \lambda) = q$;

$$\psi(q, \alpha) = b_1 b_2 \dots b_k \in B^*, \quad (18.2)$$

где $b_1 = \psi(q, a_1)$, $b_2 = \psi(q_1, a_2)$, $\dots$, $b_k = \psi(q_{k-1}, a_k)$, и для пустого слова λ имеем $\psi(q, \lambda) = \lambda$.

Зафиксируем какие-нибудь порядки на множествах A и Q . Тогда для произвольного натурального l на множестве $Q \times A^l$ возникает лексикографический

порядок. Рассмотрим теперь уравнение

$$\psi(q, \alpha) = \beta \quad (18.3)$$

при заданном $\beta \in B^l$ относительно неизвестных $(q, \alpha) \in Q \times A^l$. Все решения этого уравнения выпишем в лексикографическом порядке и получим таблицу из k строк и $l + 1$ столбцов

$$\begin{array}{cccc} q^{(1)}, & a_1^{(1)}, & \dots, & a_l^{(1)} \\ q^{(2)}, & a_1^{(2)}, & \dots, & a_l^{(2)} \\ \dots, & \dots, & \dots, & \dots \\ q^{(k)}, & a_1^{(k)}, & \dots, & a_l^{(k)} \end{array} . \quad (18.4)$$

Через $\text{Inv}_{\mathcal{M}}(\beta)$ обозначим совокупность входных слов автомата $\mathcal{M}$, полученную из таблицы (18.4) отбрасыванием первого столбца. Заметим, что некоторые входные слова могут повторяться в совокупности $\text{Inv}_{\mathcal{M}}(\beta)$. Если же слово β не может появиться на выходе автомата $\mathcal{M}$, то $k = 0$ и $\text{Inv}_{\mathcal{M}}(\beta) = \emptyset$.

Нашей целью является изучение совокупности $\text{Inv}_{\mathcal{M}}(\beta)$ и, в особенности, нахождение однозначно определяемых фрагментов слов из $\text{Inv}_{\mathcal{M}}(\beta)$.

§19 Частично обратный автомат

Исходя из сформулированных в §18 целей, опишем способ выделения однозначно определяемых координат совокупности входных слов $\text{Inv}_{\mathcal{M}}(\beta), \beta \in B^*$ с помощью частично обратного автомата (ЧО-автомата), ассоциированного с автоматом $\mathcal{M}$. Будем обозначать этот автомат $\mathcal{M}^{-1}$.

Определим $\mathcal{M}^{-1}$ как инициальный автомат Мили —

$$\mathcal{M}^{-1} = (B, S, A', \zeta, \eta, s_0) .$$

Входным алфавитом автомата $\mathcal{M}^{-1}$ является множество B , а его выходным алфавитом — $A' = A \cup \{*\}$, $*$ $\notin A$. Начальное состояние s_0 автомата $\mathcal{M}^{-1}$ совпадает с $Q \in 2^Q$. Множество состояний S автомата $\mathcal{M}^{-1}$ определено ниже.

Для любых $s \in 2^Q$ и $b \in B$ определим множества

$$\begin{aligned}\gamma(s, b) &= \{(q, x) \in s \times A : \psi(q, x) = b\}, \\ \omega(s, b) &= \{x \in A : \exists q \in s, \psi(q, x) = b\}.\end{aligned}$$

Зададим функции $\zeta : 2^Q \times B \rightarrow 2^Q$ и $\eta : 2^Q \times B \rightarrow A'$ следующими соотношениями:

$$\zeta(s, b) = \begin{cases} \{\varphi(q, x) : (q, x) \in \gamma(s, b)\}, & \text{если } s \neq \emptyset \text{ и } \gamma(s, b) \neq \emptyset, \\ \emptyset, & \text{если } s \neq \emptyset \text{ и } \gamma(s, b) = \emptyset, \\ \emptyset, & \text{если } s = \emptyset; \end{cases} \quad (19.1)$$

$$\eta(s, b) = \begin{cases} a, & \text{если } \gamma(s, b) \neq \emptyset \text{ и } \omega(s, b) = \{a\}, \\ *, & \text{если } \gamma(s, b) \neq \emptyset \text{ и } \#\omega(s, b) > 1, \\ *, & \text{если } \gamma(s, b) = \emptyset. \end{cases} \quad (19.2)$$

Множество состояний S автомата $\mathcal{M}^{-1}$ совпадает с совокупностью достижимых из Q подмножеств из 2^Q , т.е.

$$S = \{s \in 2^Q : \exists \beta \in B^*, \zeta(Q, \beta) = s\}.$$

Из соотношения (19.1) видно, что если $s = \emptyset \in S$, то это состояние является поглощающим. Кроме того, любое слово $\beta = b_1 b_2 \dots b_l \in B^*$, удовлетворяющее соотношению $\zeta(Q, \beta) = \emptyset$, является "запретным" для автомата $\mathcal{M}$, т.е. слово β не может появиться на выходе этого автомата. Если же $\emptyset \notin S$, то на

выходе автомата $\mathcal{M}$ может быть получено любое слово из V^* . Такие автоматы называют полными по выходу или автоматами без запретов.

Замечание 19.1. Еще одним возможным способом задания отображения $\text{Inv}_{\mathcal{M}}$ является построение диаграммы обращения автомата $\mathcal{M}$, обобщающей способ задания детерминированных функций с помощью деревьев (см. [Ябл 10], гл. 3). Однако для целей частичного обращения этот способ задания отображения $\text{Inv}_{\mathcal{M}}$ менее удобен.

Через $\Gamma_{\mathcal{M}^{-1}}$ будем обозначать граф автомата $\mathcal{M}^{-1}$, определяемый стандартным образом (см. [GeP 72]).

Возможность однозначного восстановления по выходному слову некоторых входных символов автомата $\mathcal{M}$ существенным образом зависит от строения графа $\Gamma_{\mathcal{M}^{-1}}$.

Лемма 19.2. Пусть $s, s' \in S$, т.е. при некоторых $\beta, \beta' \in V^*$

$$s = \zeta(Q, \beta), s' = \zeta(Q, \beta').$$

Тогда

$$\zeta(s, \beta') \subseteq s', \zeta(s', \beta) \subseteq s.$$

Доказательство. Из соотношения (19.1) легко видеть, что для функции $\zeta(s, b)$ выполняется следующее специфическое свойство монотонности: если $s \subseteq s'$, то для любого слова $\beta \in V^*$ выполнено включение

$$\zeta(s, \beta) \subseteq \zeta(s', \beta).$$

Используя это свойство и включения $s \subseteq Q, s' \subseteq Q$, легко показать справедливость утверждения леммы. $\square$

Если состояния $s \subseteq Q$ или $s' \subseteq Q$ в условиях леммы 19.2 имеют минимальную в S мощность (число входящих в s или в s' элементов q из Q), то

соответствующее включение (или оба) превращаются в равенство. Это соображение показывает особую роль множества всех состояний, мощность которых минимальна в S . Введем обозначения

$$d_{\mathcal{M}} = \min_{s \in S} \#s, 0 \leq d_{\mathcal{M}} \leq \#Q,$$

$$S^0 = \{s \in S : \#s = d_{\mathcal{M}}\}, 1 \leq \#S^0 \leq \binom{\#Q}{d_{\mathcal{M}}}.$$

Теорема 19.3. Пусть $s^0 \in S^0$ и для некоторого слова $\beta \in B^*$ выполнено $s^0 = \zeta(Q, \beta)$. Тогда для любого $s \in S$ выполнено $\zeta(s, \beta) = s^0$.

Доказательство. Очевидно, в силу приведенных выше соображений. $\square$

Таким образом, все слова $\beta \in B^*$, переводящие начальное состояние автомата $\mathcal{M}^{-1}$ в некоторое состояние $s^0 \in S^0$, являются синхронизирующими (см. определение 21.5) для автомата $\tilde{\mathcal{M}}^{-1} = (B, S, A', \zeta, \eta)$.

Следствие 19.4. Все состояния из S^0 достижимы друг из друга и поэтому S^0 целиком входит в некоторую компоненту сильной связности графа автомата $\mathcal{M}^{-1}$.

Доказательство. Непосредственно следует из утверждения теоремы 19.3. $\square$

Следствие 19.5. Граф автомата $\mathcal{M}^{-1}$ сильно связан тогда и только тогда, когда из некоторого состояния $s^0 \in S^0, \#s^0 > 0$ достижимо состояние $Q \in S$.

Доказательство. Непосредственно следует из утверждения теоремы 19.3. $\square$

Будем называть автомат $\mathcal{M}$ детерминированно обратимым автоматом (ДО-автоматом), если для любых $q \in Q$ и $b \in B$ выполнено неравенство $\#\psi_q^{-1}(b) \geq 1$. Очевидно, что для любого ДО-автомата выполнено неравенство $\#A \geq \#B$.

Будем говорить, что ДО-автомат $\mathcal{M}$ является автоматом со стабилизирующим обращением или СО-автоматом, если множество S^0 совпадает с некоторой компонентой сильной связности графа $\Gamma_{\mathcal{M}^{-1}}$. В этом случае в автомате $\mathcal{M}^{-1}$ естественным образом определен подавтомат с множеством состояний S^0 и теми же функцией переходов $\zeta(s,b)$ и функцией выходов $\psi(s,b)$. С учетом следствия 19.4 очевидно, что ДО-автомат $\mathcal{M}$ является СО-автоматом тогда и только тогда, когда для любого $s \in S^0$ и любого $\beta \in B^*$

$$\zeta(s,\beta) \in S^0.$$

Ясно, что это эквивалентно тому, что для любого $s \in S^0$ и любого $b \in B$

$$\zeta(s,b) \in S^0.$$

Последнее условие является локальным для функции переходов $\zeta(s,b)$, наиболее удобно для проверки, и его можно считать определением СО-автомата.

Будем говорить, что СО-автомат $\mathcal{M}$ является автоматом с единственным стабилизирующим обращением или ЕСО-автоматом, если для него $\#S^0 = 1$. Для ЕСО-автоматов множество S^0 состоит из единственного состояния, и это состояние является поглощающим (в стандартной терминологии цепей Маркова).

Можно легко описать два вырожденных случая СО-автоматов с $d_{\mathcal{M}} = 0$ и $d_{\mathcal{M}} = \#Q$. Они являются ЕСО-автоматами с $S^0 = \{\emptyset\}$ и $S^0 = \{Q\}$ соответственно. Справедливо следующее утверждение.

Лемма 19.6. *Равенство $d_{\mathcal{M}} = \#Q$ выполняется тогда и только тогда, когда для любых $q \in Q$ и $b \in B$ система из двух уравнений с двумя неизвестными $y \in Q, x \in A$*

$$\begin{cases} \varphi(y,x) = q \\ \psi(y,x) = b \end{cases}$$

имеет решение.

Доказательство. Вытекает из соотношений (19.1) и (19.2). $\square$

В условиях леммы 19.6 очевидно, что $S = S^0 = \{Q\}$. Важнейший невырожденный случай описывается следующим утверждением.

Теорема 19.7. Пусть $\mathcal{M}$ — ДО-автомат, $\#A = \#B$. Тогда автомат $\mathcal{M}$ является СО-автоматом и $d_{\mathcal{M}} \neq 0$.

Доказательство. Поскольку $\mathcal{M}$ — ДО-автомат, то $\#\psi_q^{-1}(b) \geq 1$ для любых $q \in Q$ и $b \in B$. Так как $\#A = \#B$, то для любых $q \in Q$ и $b \in B$ имеем $\#\psi_q^{-1}(b) = 1$, т.е. отображение $\psi_q : A \rightarrow B$ взаимно однозначно при всех $q \in Q$. Отсюда легко получить, что автомат $\mathcal{M}$ — полный по выходу, т.е. $d_{\mathcal{M}} \neq 0$.

Теперь заметим, что поскольку $\psi_q : A \rightarrow B$ взаимно однозначно при всех $q \in Q$, то при всех $s \in S$, $b \in B$ имеем

$$\#\zeta(s, b) \leq \#1.$$

Если это неравенство рассмотреть для состояний $s \in S^0$, мощность которых минимальна в S , то придем к выводу, что $\zeta(s, b) \in S^0$ для всех $s \in S^0$, $b \in B$. А это и означает, что $\mathcal{M}$ — СО-автомат. $\square$

Пусть $\beta = b_1 \dots b_{l-1} b_l = \beta' b_l \in B^*$ и $\zeta(Q, \beta') = s = \{q_1, \dots, q_{d_{\mathcal{M}}}\} \in S^0$. При подаче на вход автомата $\mathcal{M}^{-1}$, находящегося в состоянии s , символа b_l имеем $\zeta(s, b_l) = s' \in S^0$, где $s' = \{\varphi(q_1, a_1), \dots, \varphi(q_{d_{\mathcal{M}}}, a_{d_{\mathcal{M}}})\}$, $a_i = \psi_q^{-1}(b_l)$, $i = 1, \dots, d_{\mathcal{M}}$. С точки зрения восстановления по β неизвестного входного слова α автомата $\mathcal{M}$ это означает следующее. После попадания автомата $\mathcal{M}^{-1}$ в состояние из множества S^0 , каждый оставшийся символ входной последовательности может быть восстановлен не более чем в $d_{\mathcal{M}}$ вариантах.

Суммируя полученные результаты о строении графа автомата $\mathcal{M}^{-1}$, видим, что наиболее законченный вид они имеют для автоматов $\mathcal{M}$, удовлетворяющих условиям теоремы 19.7 или, другими словами, автоматов, для которых

$\#A = \#B$ и отображение $\psi_q : A \rightarrow B$ взаимно однозначно при всех $q \in Q$. Такие автоматы называют автоматами без потери информации (БПИ-автоматы, см. [КАП 85]).

§20 Асимптотическое поведение характеристик частичного обращения для БПИ-автоматов

Как было показано ранее (см. §19), большое значение для возможности восстановления фрагментов входного слова имеет параметр d_M . Приведем два утверждения, характеризующие этот параметр.

Будем говорить, что два различных состояния $q, q' \in Q$ автомата M слипаются, если найдутся два таких слова $\alpha, \alpha' \in A^*$, что

$$\begin{aligned}\psi(q, \alpha) &= \psi(q', \alpha'), \\ \varphi(q, \alpha) &= \varphi(q', \alpha').\end{aligned}$$

Лемма 20.1. *Величина d_M для БПИ-автомата M равна максимальному числу попарно неслипающихся состояний из Q .*

Доказательство. Ясно, что если некоторое подмножество состояний $Q^0 \subseteq Q$ состоит только из попарно неслипающихся состояний, то при всех $\beta \in B^*$ имеем

$$\#\zeta(Q_0, \beta) = \#Q_0.$$

Остается понять, какие из этих подмножеств достижимы из Q в графе автомата M^{-1} , т.е. входят в S . Ясно, что достижимы только множества с максимальным числом попарно неслипающихся состояний. □

Рассмотрим теперь алгебраическое описание параметра $d_{\mathcal{M}}$. Введем при любом $b \in B$ следующее преобразование $\theta_b : Q \rightarrow Q$:

$$\theta_b(q) = \varphi(q, \psi_q^{-1}(b)) .$$

Через $\mathcal{T} = \langle \theta_b, b \in B \rangle$ обозначим полугруппу преобразований, порожденную образующими θ_b . Напомним (см. [Лал 85]), что рангом $\text{rank} \tau$ преобразования $\tau : Q \rightarrow Q$ называется мощность его образа $\# \tau(Q)$, а минимальным рангом $\text{rank} \mathcal{T}$ полугруппы $\mathcal{T}$ число $\min_{\tau \in \mathcal{T}} \text{rank} \tau$.

Лемма 20.2. *Величина $d_{\mathcal{M}}$ для БПИ-автомата $\mathcal{M}$ равна минимальному рангу полугруппы $\mathcal{T} = \langle \theta_b, b \in B \rangle$: $d_{\mathcal{M}} = \text{rank} \mathcal{T}$.*

Доказательство. Из определений функции переходов $\zeta(s, b)$ и отображения θ_b легко получить, что

$$\zeta(s, b) = \bigcup_{q \in s} \theta_b(q) .$$

Отсюда для любого слова $\beta = b_1 b_2 \dots b_l \in B^*$ по индукции получаем

$$\zeta(Q, \beta) = \bigcup_{q \in Q} \theta_{b_l} \theta_{b_{l-1}} \dots \theta_{b_1}(q) .$$

Последнее соотношение доказывает утверждение леммы. □

Отметим, что в алгебраической теории полугрупп нахождение минимального ранга полугруппы преобразований связано с описанием минимальных идеалов данной полугруппы, и этим задачам посвящено значительное количество работ (подробнее см. [Лал 85]).

Вернемся к первоначальной постановке задачи частичного восстановления входного слова автомата $\mathcal{M}$. С учетом введенных выше частично обратных автоматов решение этой задачи на теоретико-автоматном уровне можно представить схемой, изображенной на рис. 20.1.

$$\boxed{\mathbf{I}} \xrightarrow{\alpha} \boxed{\mathcal{M}} \xrightarrow{\beta} \boxed{\mathcal{M}^{-1}} \xrightarrow{\eta(Q,\beta)}$$

Рисунок 20.1

Здесь $\mathbf{I}$ — некоторый источник (генератор) входных слов $\alpha \in A^*$ для автомата $\mathcal{M}$, автомат $\mathcal{M}^{-1}$ описан в параграфе 19. Все символы слова $\eta(Q, \beta)$ на рис.20.1, отличные от $*$, являются однозначно восстановленными по β символами неизвестного входного слова $\alpha \in A^*$.

Естественной характеристикой частичного обращения в этом случае является доля однозначно восстанавливаемых символов входного слова.

В исходной постановке задачи известным является только слово β . Поэтому неизвестные входные слова и неизвестные состояния естественно считать случайными, распределенными по какому-нибудь известному закону, и тем самым прийти к соответствующей вероятностной постановке задачи: изучить в этой ситуации характеристики частичного обращения автомата $\mathcal{M}$.

Пусть $\mathcal{D}(W)$ — произвольный вероятностный закон распределения на конечном непустом множестве W . Пусть $\tilde{w} \in_{\mathcal{D}} W$ — случайная величина (элемент), распределенная в соответствии с законом $\mathcal{D}$ на множестве W . В частности, $\mathcal{U}(W)$ — равномерное распределение на множестве W .

Предположим, что $(q, \tilde{\alpha}) \in_{\mathcal{D}} Q \times A^l, l \in \mathbb{N}$. Естественным образом функции переходов $(\varphi(q, a))$ и выходов $(\psi(q, a))$ автомата $\mathcal{M}$ индуцируют распределение $\mathcal{D}'(B^l)$, а функция переходов $(\zeta(s, b))$ автомата $\mathcal{M}^{-1}$ в свою очередь индуцирует цепь Маркова $S^{\mathcal{M}^{-1}}$ с множеством состояний S . Начальное распределение цепи $S^{\mathcal{M}^{-1}}$ сосредоточено в состоянии $s = Q$, поскольку $\mathcal{M}^{-1}$ — инициальный автомат. Компоненты случайной строки $\tilde{\beta} = (\tilde{b}_1 \tilde{b}_2 \dots \tilde{b}_l) \in_{\mathcal{D}'} B^l$ имеют распределения

$$\tilde{b}_i \in \mathcal{D}'_i(B), i = 1, 2, \dots, l,$$

индуцированные распределением $\mathcal{D}'(B^l)$. Матрица переходных вероятностей цепи $S^{\mathcal{M}^{-1}}$ на i -ом шагу имеет вид

$$P^{\mathcal{M}^{-1}}(i) = [P_{s,s'}(i)], i = 1, 2, \dots, l, \quad (20.1)$$

где $P_{s,s'}(i) = \sum_{b: \zeta(s,b)=s'} \Pr[\tilde{b}_i = b]$. В общем случае цепь $S^{\mathcal{M}^{-1}}$ не является однородной. Если же распределение $\mathcal{D}(Q \times A^l)$ таково, что $\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_l$ — независимые, одинаково распределенные величины, то цепь Маркова $S^{\mathcal{M}^{-1}}$ — однородная. Для БПИ-автоматов справедливо следующее утверждение.

Предположим, что источник I (см. рис.15.1) является источником без памяти, порождающим в дискретные моменты времени символы из алфавита A в соответствии с распределениями $\mathcal{U}(A^l)$, $l = 1, 2, \dots$, а начальное состояние автомата $\mathcal{M}$ выбирается независимо в соответствии с распределением $\mathcal{U}(Q)$. Это равносильно тому, что $(q, \tilde{\alpha}) \in_{\mathcal{U}} Q \times A^l$.

Лемма 20.3. Пусть $\mathcal{M}$ — БПИ-автомат, $(q, \tilde{\alpha}) \in_{\mathcal{U}} Q \times A^l$, $l = 1, 2, \dots$. Тогда цепь $S^{\mathcal{M}^{-1}}$ однородная и множество S^0 — класс эргодических состояний.

Доказательство. Равномерное распределение на $Q \times A^l$ и автомат $\mathcal{M}$ индуцируют распределение $P_i^{\mathcal{M}}(\beta) = \Pr[\psi(q, \tilde{\alpha}) = \beta]$ на множестве B^l :

$$P_i^{\mathcal{M}}(\beta) = \#Q^{-1} \cdot (\#A)^{-1} \cdot \#\{(q, \alpha) \in Q \times A^l, \psi(q, \alpha) = \beta\}.$$

Поскольку $\mathcal{M}$ — БПИ-автомат, то для любого $\beta \in B^l$ получаем $P_i^{\mathcal{M}}(\beta) = (\#A)^{-l} = (\#B)^{-l}$, т.е. случайная величина $\tilde{\beta} = \psi(q, \tilde{\alpha})$ равномерно распределена на B^l . Тогда компоненты случайной строки $\tilde{\beta} = (\tilde{b}_1 \tilde{b}_2 \dots \tilde{b}_l)$ являются независимыми равномерно распределенными на B случайными величинами. Следовательно, согласно (20.1), цепь Маркова $S^{\mathcal{M}^{-1}}$ — однородная.

Пусть $s, s' (s \neq s')$ — произвольные состояния автомата $\mathcal{M}^{-1}$ из множества S^0 . Тогда согласно утверждению теоремы 19.3 существуют $l \in \mathbb{N}$ и $\beta \in B^l$ такие,

что $\zeta(s, \beta) = s'$. Поэтому при $\tilde{\beta} \in_{\mathcal{U}} B^l$ имеем

$$\Pr \left[\zeta \left(s, \tilde{\beta} \right) = s' \right] \geq (\#A)^{-l} > 0.$$

Поскольку $\mathcal{M}$ — БПИ-автомат, то $\#\zeta(s, \beta) \leq \#s$ для любых $s \in S$ и $\beta \in B^l$, $l = 1, 2, \dots$, то цепь $C^{\mathcal{M}^{-1}}$ не может выйти из множества S^0 , то есть S^0 — эргодический класс состояний. $\square$

В условиях леммы 20.3 введем в рассмотрение следующие величины. Обозначим через $r_l^{\mathcal{M}}(\beta)$ — число символов выходного слова $\eta(Q, \beta)$ автомата $\mathcal{M}^{-1}$, отличных от $*$; $\rho_l^{\mathcal{M}}$ — математическое ожидание случайной величины $l^{-1}r_l^{\mathcal{M}}$, или содержательно, среднюю долю однозначно восстановленных на длине l входных символов автомата $\mathcal{M}$:

$$\rho_l^{\mathcal{M}} = (\#B)^{-l} l^{-1} \sum_{\beta \in B^l} r_l^{\mathcal{M}}(\beta);$$

$\rho^{\mathcal{M}} = \lim_{l \rightarrow \infty} \rho_l^{\mathcal{M}}$, если он существует. Ясно, что наиболее важной характеристикой частичного обращения является величина $\rho^{\mathcal{M}}$. Рассмотрим некоторые утверждения о величине $\rho^{\mathcal{M}}$.

Теорема 20.4. Пусть для БПИ-автомата $\mathcal{M}$ выполнено равенство $d_{\mathcal{M}} = 1$. Тогда $\rho^{\mathcal{M}} = 1$.

Доказательство. Обозначим через P_l вероятность того, что конечная марковская цепь через l шагов окажется в эргодическом состоянии. Согласно утверждению теоремы 3.1.1 ([KeC 70], стр.62), независимо от того, где начался процесс, вероятность P_l стремится к 1 при $l \rightarrow \infty$. В нашем случае P_l определяется следующим выражением:

$$P_l = \sum_{\substack{\beta \in B^l \\ \#\zeta(Q, \beta)=1}} P_l^{\mathcal{M}}(\beta) = \sum_{\substack{\beta \in B^l \\ \#\zeta(Q, \beta)=1}} (\#B)^{-l},$$

поскольку в соответствии с утверждениями теоремы 19.7, леммы 20.3 и условием $d_{\mathcal{M}} = 1$ состояния $s \in S^0 \subseteq S$ мощности единица являются эргодическими. Кроме того, для слов $\beta = (b_1 b_2 \dots b_l) \in B^l$, таких, что $\#\zeta(Q, (b_1 \dots b_{l_0})) = 1, l_0 < l$, выполнено $r_l^{\mathcal{M}}(\beta) \geq l - l_0$.

Пусть $\varepsilon > 0$. Тогда существует $l_0 = l_0(\varepsilon)$ такое, что при всех $l \geq l_0$ выполнено неравенство $P_l \geq 1 - \varepsilon$. Предположим, что $l \geq l_0$. Тогда

$$\begin{aligned} \rho_l^{\mathcal{M}} &= (\#B)^{-l} l^{-1} \sum_{\beta \in B^l} r_l^{\mathcal{M}}(\beta) \geq \\ &\geq (\#B)^{-l} l^{-1} \sum_{\substack{\beta \in B^l \\ \#\zeta(Q, (b_1 \dots b_{l_0}))=1}} r_l^{\mathcal{M}}(\beta) \geq \\ &\geq (\#B)^{-l} l^{-1} \sum_{\substack{\beta \in B^l \\ \#\zeta(Q, (b_1 \dots b_{l_0}))=1}} (l - l_0) = \\ &= \frac{l - l_0}{l} P_{l_0} \geq \frac{l - l_0}{l} (1 - \varepsilon). \end{aligned}$$

Правая часть последнего неравенства, поскольку ε произвольно, сколь угодно близка к 1 при $l \rightarrow \infty$, что и доказывает теорему. $\square$

Теорема 20.5. Пусть для БПИ-автомата $\mathcal{M}$ выполнено равенство $d_{\mathcal{M}} = \#Q$. Тогда $\rho^{\mathcal{M}} = \frac{r}{\#B}$, где $r = \#\{b \in B : r_1^{\mathcal{M}}(b) = 1\}$, $0 \leq r \leq \#B$.

Доказательство. В соответствии с утверждением леммы 19.6 частично обратный автомат $\mathcal{M}^{-1}$ в рассматриваемом случае имеет всего одно состояние, т.е. $S = \{Q\}$. Поэтому для любого $\beta = (b_1 b_2 \dots b_l) \in B^l$

$$\eta(Q, \beta) = \eta(Q, b_1) \eta(Q, b_2) \dots \eta(Q, b_l),$$

причем каждый символ $\eta(Q, b_i)$ независимо от других может принимать значение, отличное от $*$, r раз. Напомним, что по определению условие $r_1^{\mathcal{M}}(b) = 1$ эквивалентно условию $\eta(Q, b) \neq *$. Поэтому $\rho_l^{\mathcal{M}} = r/\#B$ при любом l , что и доказывает теорему. $\square$

Теорема 20.6. Пусть $\mathcal{M} = (A, Q, B, \varphi, \psi)$ — БПИ-автомат, $\mathcal{M}' = (A, Q', B, \varphi, \psi)$ — его некоторый подавтомат и $Q' \subseteq Q$. Тогда $\rho^{\mathcal{M}'} \geq \rho^{\mathcal{M}}$, если они существуют.

Доказательство. Ясно, что $\mathcal{M}'$ является БПИ-автоматом. Из определений $r_l^{\mathcal{M}}(\beta)$ и $r_l^{\mathcal{M}'}(\beta)$ очевидно, что для любого $\beta \in B^l$ выполнено неравенство $r_l^{\mathcal{M}}(\beta) \leq r_l^{\mathcal{M}'}(\beta)$. Теперь из определения получаем, что

$$\rho_l^{\mathcal{M}} = (\#B)^l l^{-1} \sum_{\beta \in B^l} r_l^{\mathcal{M}}(\beta) \leq (\#B)^l l^{-1} \sum_{\beta \in B^l} r_l^{\mathcal{M}'}(\beta) = \rho_l^{\mathcal{M}'}.$$

Поскольку по условию пределы при $l \rightarrow \infty$ величин, стоящих в правой и левой частях неравенства, существуют, это и доказывает теорему. $\square$

§21 Локальное обращение БПИ-автоматов

Рассмотренное в §§18,19,20 частичное обращение дискретных ограниченно-детерминированных функций имеет характерную особенность. Локализация (т.е. положение) однозначно восстанавливаемых фрагментов прообраза не может быть задана детерминированно и имеет характер случайного процесса, параметры которого определяются свойствами частично обратного автомата. Однако для автоматов без потери информации может быть рассмотрен вариант частичного обращения, для которого позиция однозначно восстанавливаемого фрагмента в прообразе точно определяется появлением в выходном слове автомата специальных подслов-индикаторов. Этот вариант частичного обращения в [Лог 07] был назван локальным обращением.

Пусть, как и ранее, A — конечное множество (алфавит), A^* — множество слов конечной длины в этом алфавите (включая пустое слово λ), A^∞ — множество бесконечных вправо последовательностей в алфавите A .

Для последовательности из A^∞ определим оператор редуцирования.
Пусть $i, j \in \mathbb{N}$ ($\mathbb{N} = \{1, \dots, n, \dots\}$), $1 \leq i \leq j$. Тогда для любой последовательности $x \in A^\infty$ положим

$$x_{[i,j]} = x_i x_{i+1} \dots x_j$$

и

$$x_{[i,j)} = x_i x_{i+1} \dots x_{j-1}.$$

Если $i = j$, то $x_{[i,i]} = x_{[i]} = x_i$.

Кроме того, положим

$$x_{[i,\infty)} = x_i x_{i+1} \dots$$

Аналогично операторы редуцирования определим для элементов множества A^* .

Пусть

$$\mathcal{M} = (A, Q, B, \varphi, \psi) —$$

конечный автомат Мили, где конечные множества A и B — входной и выходной алфавит соответственно, Q — конечное множество состояний автомата, $\varphi : Q \times A \rightarrow Q$ — функция переходов автомата, $\psi : Q \times A \rightarrow B$ — функция выходов автомата.

Естественным образом (см. §18) распространим действие функций φ и ψ на $Q \times A^*$. Пусть $x = x_1 x_2 \dots x_k \in A^*$, $q \in Q$. Если

$$q_1 = \varphi(q, x_1), q_2 = \varphi(q_1, x_2), \dots, q_k = \varphi(q_{k-1}, x_k)$$

и

$$y_1 = \psi(q, x_1), y_2 = \psi(q_1, x_2), \dots, y_k = \psi(q_{k-1}, x_k),$$

где $q_1, \dots, q_k \in Q$, $y_1, \dots, y_k \in B$, то будем полагать

$$\varphi(q, x) = q_k, \psi(q, x) = y_1 y_2 \dots y_k.$$

Кроме того, для любого q из Q будем полагать $\varphi(q, \lambda) = q$, $\psi(q, \lambda) = \lambda$.

Аналогичным образом распространим действие функций на множестве $Q \times A^\infty$.

Определение 21.1. Состояния q^1 и q^2 автомата $\mathcal{M}$ называются эквивалентными, если при любых $x \in A^*$ выполнено $\psi(q^1, x) = \psi(q^2, x)$. Автомат $\mathcal{M}$ называется приведенным, если у него нет эквивалентных состояний.

Определение 21.2. Автомат Мили $\mathcal{M} = (A, Q, B, \varphi, \psi)$ называется автоматом без потери информации (БПИ-автоматом), если $\#A = \#B$ ($\#A$ — мощность конечного множества A) и для любого состояния q из Q отображение $\psi_q = \psi(q, \cdot) : A \rightarrow B$ является взаимно однозначным.

Замечание 21.3. Очевидно, что любая последовательность из A^∞ может быть получена на выходе БПИ-автомата $\mathcal{M}$. Более того, при этом в качестве начального состояния может быть выбрано произвольное состояние из Q . Следовательно, для любой выходной последовательности (слова) автомата $\mathcal{M}$ существует ровно $\#Q$ различных пар начальное состояние - входная последовательность (входное слово), перерабатываемых автоматом $\mathcal{M}$ в данную выходную последовательность (слово).

Пусть $\mathcal{M} = (A, Q, B, \varphi, \psi)$ — конечный автомат Мили, удовлетворяющий условию $\#A = \#B$. Для удобства (не теряя общности) будем считать, что $A = B$. Вместе с тем, для рассматриваемых далее конструкций нам важно различать входные и выходные слова (последовательности) автомата $\mathcal{M}$. Будем обозначать входные слова (последовательности) этого автомата $x = x_1x_2 \dots x_r, a = a_1a_2 \dots a_r \in A^r, r \in \mathbb{N}$ ($x = x_1x_2 \dots, a = a_1a_2 \dots \in A^\infty$), а его выходные слова (последовательности) — $y = y_1y_2 \dots y_s, b = b_1b_2 \dots b_s \in A^s$ ($y = y_1y_2 \dots, b = b_1b_2 \dots \in A^\infty$).

Кроме того, если для пары последовательностей $x, y \in A^\infty$ и состояния $q \in Q$ равенство $\psi(q, x_{[1,j]}) = y_{[1,j]}$ выполняется для всех $j \geq 1$, то будем писать $\psi(q, x) = y$.

Будем обозначать через $\mathcal{B} = (A, Q, \delta)$ — конечный автомат без выхода, где A — входной алфавит, Q — множество состояний, а $\delta : Q \times A \rightarrow Q$ — функция переходов. Естественным образом (как ранее для автомата Мили) распространим действие функции δ на множества $Q \times A^k, k \in \mathbb{N}$ и $Q \times A^\infty$. Если $S \subseteq Q$ и $y \in A^*$, то будем полагать

$$\delta(S, y) = \bigcup_{q \in S} \{\delta(q, y)\}.$$

Определение 21.4. Автомат Мили $\mathcal{M} = (A, Q, B, \varphi, \psi)$ без потери информации обладает свойством локальной обратимости, если существует слово $u \in B^l, l \in \mathbb{N}$, для которого выполнено следующее условие: для любых $x^1, x^2 \in A^\infty, q^1, q^2 \in Q, i \in \mathbb{N}$ таких, что

$$\psi(q^1, x^1) = \psi(q^2, x^2) \text{ и } \psi(q^1, x^1)_{[i, i+l-1]} = \psi(q^2, x^2)_{[i, i+l-1]} = u,$$

справедливо равенство

$$x^1_{[i+l, \infty]} = x^2_{[i+l, \infty]}.$$

Слово u будем называть индикатором локального обращения для автомата $\mathcal{M}$.

В теории автоматов уделяется значительное внимание изучению понятия "синхронизируемость автомата", имеющего важные практические приложения. Впервые это понятие было формализовано в работе Я. Черны [Cer 64], хотя ранее неявно оно использовалось в научных исследованиях по крайней мере с 1956г. Поскольку статья Я. Черны была опубликована на словацком языке, то она длительное время оставалась неизвестной (см., например, [LaRu 69], [Клю 88], [Рыс 94]).

Необходимо также отметить тесную связь этого понятия с теорией автоматов без потери информации конечного порядка, теорией префиксных кодов и символической динамикой.

Определение 21.5. Конечный автомат без выхода $\mathcal{B} = (A, Q, \delta)$ называется синхронизируемым, если существует такое слово $y \in A^*$, что

$$\#\delta(Q, y) = 1.$$

Слово y называют синхронизирующим для автомата без выхода $\mathcal{B}$.

Замечание 21.6 (Гипотеза Черны). Пусть $r \in \mathbb{N}$ и $C(r)$ — максимальная длина кратчайших синхронизирующих слов синхронизируемых автоматов с r состояниями (функция Черны). Для этой функции справедливы следующие оценки (см. [Cer 64], [Pin 83])

$$(r - 1)^2 \leq C(r) \leq \frac{n^3 - n}{6}.$$

В частности, в [Cer 64] построена серия автоматов с кратчайшими синхронизирующими словами длины $(r - 1)^2$. Под гипотезой Я. Черны понимают его предположение о том, что описанная в [Cer 64] серия автоматов реализует наилучший в смысле скорости синхронизации случай, т.е. любой синхронизируемый автомат с r состояниями обладает синхронизирующим словом длины не более $(r - 1)^2$ (подробнее см. [Vol 08]).

Имеет место следующий критерий синхронизируемости.

Лемма 21.7. Автомат без выхода $\mathcal{B} = (A, Q, \delta)$ является синхронизируемым тогда и только тогда, когда для любой пары состояний $q, q' \in Q$ существует слово $y = y(q, q') \in A^*$ такое, что $\delta(q, y) = \delta(q', y)$.

Доказательство. Пусть автомат без выхода $\mathcal{B}$ синхронизируемый. Тогда существует слово $y \in A^*$, что $\#\delta(Q, y) = 1$. Следовательно, необходимость условия леммы очевидна.

Докажем достаточность. Предположим, что условие леммы выполнено. Пусть $q, \tilde{q} \in Q$, $q \neq \tilde{q}$. Тогда существует слово $y^1 \in A^*$ такое, что $\delta(q, y^1) =$

$\delta(\tilde{q}, y^1)$, и для множества $S^1 = \delta(Q, y^1)$ выполнено неравенство $\#S^1 \leq \#Q - 1$. Если $\#S^1 \geq 2$, то выберем из S^1 пару состояний $q^1, \tilde{q}^1, q^1 \neq \tilde{q}^1$. По условию леммы для этих состояний существует слово $y^2 \in A^*$ такое, что $\delta(q^1, y^2) = \delta(\tilde{q}^1, y^2)$. Следовательно, для множества состояний $S^2 = \delta(S^1, y^2)$ выполнено неравенство $\#S^2 \leq \#Q - 2$. Если $\#S^2 \geq 2$, то, продолжив аналогичные рассуждения, определим конечную последовательность множеств состояний $S^3, S^4, \dots$. Для них выполнены неравенства $\#S^i \leq \#Q - i, i = 3, 4, \dots$. Поскольку Q — конечное множество, найдется $t \leq \#Q - 1$ такое, что $\#S^t = 1$. Тогда для слова $y = y^1 y^2 \dots y^t \in A^*$ выполнено условие $\#\delta(Q, y) = 1$, т.е. автомат без выхода $\mathcal{B}$ — синхронизируемый. ■

Для дальнейшего изучения свойства локальной обратимости нам потребуется понятие "автомата без выхода, ассоциированного с автоматом без потери информации."

Определение 21.8. Пусть $\mathcal{M} = (A, Q, A, \varphi, \psi)$ — произвольный конечный автомат без потери информации. Будем называть автоматом без выхода, ассоциированным с $\mathcal{M}$, автомат $\mathcal{B}(\mathcal{M})$, задаваемый следующим образом:

- A — входной алфавит автомата $\mathcal{B}(\mathcal{M})$;
- Q — множество состояний автомата $\mathcal{B}(\mathcal{M})$;
- δ — функция переходов автомата $\mathcal{B}(\mathcal{M})$, определяемая соотношением

$$\delta(q, b) = \varphi(q, \psi_q^{-1}(b)) \quad (21.1)$$

для любых $q \in Q, b \in A$.

Теперь мы можем сформулировать утверждение, связывающее свойство локальной обратимости автомата $\mathcal{M}$ с синхронизируемостью автомата $\mathcal{B}(\mathcal{M})$.

Замечание 21.9. В ходе доказательства данного утверждения мы будем пользоваться хорошо известным свойством автоматов без потери информации. При

произвольном фиксированном состоянии $q \in Q$ и любом $r \in \mathbb{N}$ отображение из A^r в A^r вида $\psi_q : z \rightarrow \psi_q(z) = \psi(q, z)$, $z \in A^r$ является взаимно однозначным.

Теорема 21.10. *Приведенный автомат без потери информации $\mathcal{M} = (A, Q, A, \varphi, \psi)$ обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат без выхода $\mathcal{B}(\mathcal{M})$ синхронизируем.*

Доказательство. Предположим, что автомат $\mathcal{B}(\mathcal{M})$ синхронизируем. Тогда существует синхронизирующее слово $u = u_1 u_2 \dots u_l$ и состояние $q^0 \in Q$ такие, что $\delta(q, u) = q^0$ для любого состояния $q \in Q$.

Пусть $x^1, x^2 \in A^\infty$, $q^1, q^2 \in Q$, $i \in \mathbb{N}$ такие, что

$$\psi(q^1, x^1) = \psi(q^2, x^2) = y \in A^\infty, y_{[i, i+l-1]} = u. \quad (21.2)$$

Покажем, что

$$\varphi(q^1, x^1_{[1, i+l-1]}) = \varphi(q^2, x^2_{[1, i+l-1]}) = q^0. \quad (21.3)$$

Действительно, если

$$q' = \varphi(q^1, x^1_{[1, i-1]}), q'' = \varphi(q^2, x^2_{[1, i-1]}),$$

то, воспользовавшись соотношением 21.2 и тем, что u — синхронизирующее слово для $\mathcal{B}(\mathcal{M})$, получаем

$$\varphi(q', x^1_{[i, i+l-1]}) = \delta(q', y_{[i, i+l-1]}) = \delta(q', u) = q^0,$$

$$\varphi(q'', x^2_{[i, i+l-1]}) = \delta(q'', y_{[i, i+l-1]}) = \delta(q'', u) = q^0.$$

Поскольку в соответствии с (21.2)

$$\psi \left(q^0, x_{[i+l, \infty)}^1 \right) = \psi \left(q^0, x_{[i+l, \infty)}^2 \right) = y_{[i+l, \infty)}$$

и частичная функция выходов (при фиксированном q) $\psi_q(\cdot) = \psi(q, \cdot)$ является перестановкой элементов A , то $x_{[i+l, \infty)}^1 = x_{[i+l, \infty)}^2$. Следовательно, БПИ-автомат $\mathcal{M}$ обладает свойством локальной обратимости и слово u — индикатор.

Обратно. Пусть приведенный БПИ-автомат $\mathcal{M}$ обладает свойством локальной обратимости. Тогда существует слово-индикатор $u \in A^l$, для которого выполняется условие: для любых $x^1, x^2 \in A^\infty, q^1, q^2 \in Q, i \in \mathbb{N}$ таких, что $\psi(q^1, x^1) = \psi(q^2, x^2)$ и $\psi(q^1, x^1)_{[i, i+l-1]} = \psi(q^2, x^2)_{[i, i+l-1]} = u$, выполнено равенство $x_{[i+l, \infty)}^1 = x_{[i+l, \infty)}^2$.

Будем доказывать от противного. Предположим, что автомат $\mathcal{B}(\mathcal{M})$ не является синхронизируемым. Тогда существует пара состояний $q', q'' \in Q, q' \neq q''$, для которых выполнено $\delta(q', z) \neq \delta(q'', z)$ при любом слове $z \in A^*$. Следовательно, и для слова-индикатора u выполнено $\delta(q', u) \neq \delta(q'', u)$.

Так как $\mathcal{M}$ — БПИ-автомат, то для пар (q', u) и (q'', u) однозначно определяются слова этого автомата v' и v'' соответственно такие, что

$$\psi(q', v') = \psi(q'', v'') = u \quad (21.4)$$

и

$$\varphi(q', v') = \delta(q', u) \neq \delta(q'', u) = \varphi(q'', v''). \quad (21.5)$$

Пусть y — произвольная последовательность из A^∞ . Тогда для состояний $\varphi(q', v')$ и $\varphi(q'', v'')$ однозначно определяются последовательности $x', x'' \in A^\infty$ такие, что

$$\psi(\varphi(q', v'), x') = \psi(\varphi(q'', v''), x'') = y \quad (21.6)$$

и

$$\psi(q', v' x') = \psi(q'', v'' x'') = uy. \quad (21.7)$$

Так как БПИ-автомат $\mathcal{M}$ обладает свойством локальной обратимости и u — индикатор, то из соотношений (21.6), (21.7) вытекает равенство $x' = x'' = x$. Следовательно, для любой последовательности $y \in A^\infty$ существует $x \in A^\infty$ такая, что

$$\psi(\varphi(q', v'), x) = \psi(\varphi(q'', v''), x) = y. \quad (21.8)$$

Для произвольного $r \in \mathbb{N}$ рассмотрим семейство из $t = (\#A)^r$ последовательностей $y^1, y^2, \dots, y^t$ из A^∞ таких, что

$$\{y_{[1,r]}^i : i = 1, \dots, t\} = A^r. \quad (21.9)$$

Для соответствующих (см. 21.8) входных последовательностей $x^1, x^2, \dots, x^t$ из A^∞ имеем

$$\begin{aligned} \psi(\varphi(q', v'), x^i) &= \psi(\varphi(q'', v''), x^i) = y^i, \\ i &= 1, 2, \dots, t. \end{aligned}$$

Поскольку $\mathcal{M}$ — БПИ-автомат и выполнено (21.9), то (см. замечание 21.9)

$$\{x_{[1,r]}^i : i = 1, \dots, t\} = A^r$$

и

$$\psi(\varphi(q', v'), x_{[1,r]}^i) = \psi(\varphi(q'', v''), x_{[1,r]}^i) = y_{[1,r]}^i, \quad (21.10)$$

$i = 1, 2, \dots, t$.

Так как соотношения (21.10) выполняются при любом $r \in \mathbb{N}$, то состояния $\varphi(q', v')$ и $\varphi(q'', v'')$ эквивалентные. Это противоречит приведенности автомата $\mathcal{M}$. Следовательно, автомат $\mathcal{B}(\mathcal{M})$ синхронизируем. $\square$

§22 Локальное обращение неавтономных регистров сдвига с фильтрующими функциями

Рассмотрим теперь вопрос о локальном обращении для одного частного вида БПИ-автоматов. Интересующий нас класс автоматов — неавтономные регистры сдвига с фильтрующими функциями (см. приложение A.d). Они используются, в частности, при синтезе генераторов псевдослучайных последовательностей. Свойство "без потери информации" в данном случае означает, что фильтрующая функция линейна по последней переменной.

В приложении A.d автомат $\text{SR}(n, f)$ представлен как автомат Мура. Для наших целей БПИ-автомат $\text{SR}(n, f)$ удобно представить как автомат Мили вида $\mathcal{M}_n(f) = (\mathbb{F}_2, \mathbb{F}_2^n, \mathbb{F}_2, \varphi_n, \psi_n)$, $f \in \mathcal{F}_n$, где

$$\begin{aligned}\varphi_n((x_1, \dots, x_n), x_{n+1}) &= (x_2, \dots, x_n, x_{n+1}) \\ \psi_n((x_1, \dots, x_n), x_{n+1}) &= f(x_1, \dots, x_n) \oplus x_{n+1}.\end{aligned}\tag{22.1}$$

Предложение 22.1. Автомат, ассоциированный с $\mathcal{M}_n(f)$ (см. определение 21.8) имеет вид

$$\mathcal{B}(\mathcal{M}_n(f)) = (\mathbb{F}_2^n, \mathbb{F}_2, \delta_n^f),$$

где

$$\delta_n^f((s_1, \dots, s_n), y) = (s_2, \dots, s_n, f(s_1, \dots, s_n) \oplus y).$$

Доказательство. Проводится непосредственной проверкой выполнения условия определения 21.8. $\square$

Замечание 22.2. Автомат $\mathcal{B}(\mathcal{M}_n(f))$ в работах по теории кодирования и криптологии иногда называют неавтономным регистром сдвига длины n с нелинейной обратной связью — $\text{NFSR}(f)$, $\deg(f) > 1$ (см. приложение А.с).

Формулировку аналога теоремы 21.10 для данного класса автоматов необходимо предварить некоторым вспомогательным утверждением.

Предложение 22.3. *Существуют функции $f \in \mathcal{F}_n$ такие, что автомат $\mathcal{M}_n(f)$ не является приведенным.*

Доказательство. Пусть для функции $f \in \mathcal{F}_n$ выполняется условие: существует фиксированный набор $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ такой, что

$$f(x_1 \oplus 1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n).$$

Тогда, очевидно, что состояния $x = (x_1, x_2, \dots, x_n)$ и $x' = (x_1 \oplus 1, x_2, \dots, x_n)$ будут эквивалентными для автомата $\mathcal{M}_n(f)$. $\square$

Следовательно, для класса автоматов $\mathcal{M}_n(f)$ не выполняется условие теоремы 21.10. Вместе с тем, утверждение этой теоремы для любого автомата $\mathcal{M}_n(f)$ и ассоциированного с ним автомата без выхода $\text{NFSR}(f)$ справедливо.

Кроме того, особенности этого класса автоматов таковы, что параметры локальной обратимости для них отличны от приведенных в определении 21.2.

Определение 22.4. Автомат $\mathcal{M}_n(f) = (\mathbb{F}_2, \mathbb{F}_2^n, \mathbb{F}_2, \varphi_n, \psi_n)$ обладает свойством локальной обратимости, если существует слово $y \in \mathbb{F}_2^l, l \geq n$ такое, что для любых последовательностей $x^1, x^2 \in \mathbb{F}_2^\infty$, состояний $s^1, s^2 \in \mathbb{F}_2^n$ и $i \in \mathbb{N}$ таких, что

$$\psi_n(s^1, x^1) = \psi_n(s^2, x^2)$$

и

$$\psi_n(s^1, x^1)_{[i, i+l-1]} = \psi_n(s^2, x^2)_{[i, i+l-1]} = y$$

справедливо равенство

$$x_{[i+l-n,\infty)}^1 = x_{[i+l-n,\infty)}^2.$$

Слово y будем называть индикатором локального обращения для автомата $\mathcal{M}_n(f)$.

Замечание 22.5. Очевидно, что свойство локальной обратимости автомата $\mathcal{M}_n(f)$ остается содержательным и в случае, когда мы рассматриваем конечные входные (выходные) наборы, содержащие подслово-индикатор y .

Теорема 22.6. Автомат $\mathcal{M}_n(f)$ обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат без выхода $\text{NFSR}(f)$ синхронизируем.

Доказательство. Необходимость. Предположим, что автомат $\mathcal{M}_n(f)$ обладает свойством локальной обратимости. Тогда существует индикаторное слово $y \in \mathbb{F}_2^l$, $l \geq n$ такое, что для любых слов $x^1, x^2 \in \mathbb{F}_2^l$ и состояний $s^1, s^2 \in \mathbb{F}_2^n$ таких, что

$$\psi_n(s^1, x^1) = \psi_n(s^2, x^2) = y, \quad (22.2)$$

выполняется равенство

$$x_{[l-n+1,l]}^1 = x_{[l-n+1,l]}^2. \quad (22.3)$$

Рассмотрим систему уравнений (22.2) подробнее

$$\left\{ \begin{array}{lcl} y_1 & = & f(s_1^1, \dots, s_n^1) \oplus x_1^1 = f(s_1^2, \dots, s_n^2) \oplus x_1^2 \\ \vdots & & \\ y_{l-n} & = & f(\dots, x_{l-n-1}^1) \oplus x_{l-n}^1 = f(\dots, x_{l-n-1}^2) \oplus x_{l-n}^2 \\ y_{l-n+1} & = & f(\dots, x_{l-n}^1) \oplus x_{l-n+1}^1 = f(\dots, x_{l-n}^2) \oplus x_{l-n+1}^2 \\ \vdots & & \\ y_l & = & f(x_{l-n}^1, \dots, x_{l-1}^1) \oplus x_l^1 = f(x_{l-n}^2, \dots, x_{l-1}^2) \oplus x_l^2. \end{array} \right. \quad (22.4)$$

Преобразуем систему уравнений (22.4) в систему уравнений функционирования автомата

$$\mathcal{B}(\mathcal{M}_n(f)) = \text{NFSR}(f).$$

Пусть мы имеем два экземпляра этого автомата с начальными состояниями s^1 и s^2 соответственно. На их входы подается одна и та же последовательность y . Тогда получаем

$$\left\{ \begin{array}{lcl} \delta_n^f((s_1^1, \dots, s_n^1), y_1) & = & (s_2^1, \dots, s_n^1, x_1^1) \\ \delta_n^f((s_2^1, \dots, x_1^1), y_2) & = & (s_3^1, \dots, x_1^1, x_2^1) \\ & \vdots & \\ \delta_n^f((\dots, x_{l-n-1}^1), y_{l-n}) & = & (\dots, x_{l-n-1}^1, x_{l-n}^1) \\ \delta_n^f((\dots, x_{l-n}^1), y_{l-n+1}) & = & (\dots, x_{l-n}^1, x_{l-n+1}^1) \\ & \vdots & \\ \delta_n^f((\dots, x_{l-1}^1), y_l) & = & (x_{l-n+1}^1 \dots, x_l^1) \end{array} \right. \quad (22.5)$$

$$\left\{ \begin{array}{lcl} \delta_n^f((s_1^2, \dots, s_n^2), y_1) & = & (s_2^2, \dots, s_n^2, x_1^2) \\ \delta_n^f((s_2^2, \dots, x_1^2), y_2) & = & (s_3^2, \dots, x_1^2, x_2^2) \\ & \vdots & \\ \delta_n^f((\dots, x_{l-n-1}^2), y_{l-n}) & = & (\dots, x_{l-n-1}^2, x_{l-n}^2) \\ \delta_n^f((\dots, x_{l-n}^2), y_{l-n+1}) & = & (\dots, x_{l-n}^2, x_{l-n+1}^2) \\ & \vdots & \\ \delta_n^f((\dots, x_{l-1}^2), y_l) & = & (x_{l-n+1}^2 \dots, x_l^2) \end{array} \right.$$

Поскольку выполнено (22.3), то

$$\delta_n^f(s^1, y) = \delta_n^f(s^2, y). \quad (22.6)$$

Так как $\mathcal{M}_n(f)$ — БПИ-автомат, то для любого состояния $s \in \mathbb{F}_2^n$ существует единственное входное слово $x \in \mathbb{F}_2^l$, что $\psi_n(s, x) = y$. Следовательно,

существует всего 2^n таких пар

$$\begin{aligned} (s^1, x^1), (s^2, x^2), \dots, (s^{2^n}, x^{2^n}), \\ \psi_n(s^i, x^i) = y, i = 1, 2, \dots, 2^n. \end{aligned} \quad (22.7)$$

При этом $\{s^1, s^2, \dots, s^{2^n}\} = \mathbb{F}_2^n$ — пространство внутренних состояний автомата $\mathcal{M}_n(f)$. Соотношения (22.2), (22.3), (22.4), (22.5), (22.6) и (22.7) показывают, что

$$\delta_n^f(s^1, y) = \delta_n^f(s^2, y) = \dots = \delta_n^f(s^{2^n}, y),$$

т.е. входное слово y является синхронизирующим для автомата $\text{NFSR}(f)$.

Достаточность. Предположим, что $y \in \mathbb{F}_2^l, l \geq n$ является синхронизирующим словом для автомата $\mathcal{B}(\mathcal{M}_n(f)) = \text{NFSR}(f)$. Тогда существует состояние $s^\circ \in \mathbb{F}_2^n$ автомата $\text{NFSR}(f)$ такое, что выполнены 2^n соотношений вида

$$\delta_n^f(s^1, y) = \delta_n^f(s^2, y) = \dots = \delta_n^f(s^{2^n}, y) = s^\circ. \quad (22.8)$$

Заметим, что соответствующие (22.8) системы булевых уравнений можно преобразовать в системы функционирования автомата $\mathcal{M}_n(f)$ (см. (22.3), (22.4), (22.5) в обратном порядке). Тогда получаем

$$\psi_n(s^1, x^1) = \psi_n(s^2, x^2) = \dots = \psi_n(s^{2^n}, x^{2^n}) = y$$

и

$$\varphi_n(s^1, x^1) = \varphi_n(s^2, x^2) = \dots = \varphi_n(s^{2^n}, x^{2^n}) = s^\circ.$$

Напомним, что $\mathcal{M}_n(f)$ — БПИ-автомат, и для любого $s^i \in \mathbb{F}_2^n$ входное слово x^i определяется однозначно. Кроме того, для любого x^i имеем $x_{[l-n+1, l]}^i = s^\circ$.

Таким образом, если в выходном слове автомата $\mathcal{M}_n(f)$ встретилось подслово y , то, начиная с такта, в котором на выход автомата поступает символ

y_{l-n+1} , входные символы определяются однозначно. Следовательно, автомат $\mathcal{M}_n(f)$ обладает свойством локальной обратимости. $\square$

Рассмотрим теперь подробнее параметры и характеристики функций f из $\mathcal{F}_n$, влияющие на наличие (или отсутствие) у автомата $\text{NFSR}(f)$ свойства синхронизируемости. Для краткости будем говорить, что функция $f \in \mathcal{F}_n$ обладает (не обладает) свойством синхронизируемости, если автомат $\text{NFSR}(f)$ синхронизируем (не синхронизируем).

Пример 22.7. Пусть $f \in \mathcal{F}_n$ — самодвойственная функция, т.е.

$$f(x \oplus 1^n) \oplus 1 = f(x). \quad (22.9)$$

Для произвольного слова $y \in \mathbb{F}_2^l$ и пары состояний $s \in \mathbb{F}_2^n$ и $s' = s \oplus 1^n$ с учетом свойства (22.9) для автомата $\text{NFSR}(f)$ имеем:

$$\begin{aligned} \delta_n^f(s, y_1) &= (s_2, \dots, s_n, f(s_1, \dots, s_n) \oplus y_1), \\ \delta_n^f(s \oplus 1^n, y_1) &= (s_2 \oplus 1, \dots, s_n \oplus 1, f(s_1 \oplus 1, \dots, s_n \oplus 1) \oplus y_1) = \\ &= (s_2 \oplus 1, \dots, s_n \oplus 1, f(s_1, \dots, s_n) \oplus 1 \oplus y_1), \end{aligned}$$

то есть после первого такта

$$\delta_n^f(s, y_1) \oplus \delta_n^f(s \oplus 1^n, y_1) = 1^n. \quad (22.10)$$

Аналогично после тактов $i = 2, 3, \dots, l$ получаем

$$\begin{aligned} \delta_n^f(s, y_1 y_2) \oplus \delta_n^f(s \oplus 1^n, y_1 y_2) &= 1^n \\ &\vdots \\ \delta_n^f(s, y_1 \dots y_i) \oplus \delta_n^f(s \oplus 1^n, y_1 \dots y_i) &= 1^n \\ &\vdots \\ \delta_n^f(s, y) \oplus \delta_n^f(s \oplus 1^n, y) &= 1^n. \end{aligned} \quad (22.11)$$

Соотношения (22.10) и (22.11) показывают, что состояния s и $s \oplus 1^n$ не могут быть переведены автоматом $\text{NFSR}(f)$ в одно и то же состояние под действием произвольного входного слова y . Следовательно, функция f не обладает свойством синхронизируемости.

Пример 22.8. Пусть $n \in \mathbb{N}$. Приведем результаты для представителей класса монотонных функций [Ябл 10], а именно так называемые функции "голосования".

1° Если n — нечетное, то функция

$$f(x_1, \dots, x_n) = \begin{cases} 0, & \text{при } \sum_{i=1}^n x_i \leq n/2; \\ 1, & \text{при } \sum_{i=1}^n x_i > n/2 \end{cases}$$

обладает свойством синхронизируемости.

2° Если n — нечетное, то функция

$$g(x_1, \dots, x_n) = \begin{cases} 0, & \text{при } \sum_{i=1}^n x_i \leq (n+1)/2; \\ 1, & \text{при } \sum_{i=1}^n x_i > (n+1)/2 \end{cases}$$

не обладает свойством синхронизируемости.

Пример 22.9. Рассмотрим представителей так называемого класса бесповторных функций, т.е. функций, существенно зависящих от всех своих переменных, у которых каждая переменная входит только один раз в АНФ.

1° Функция $f(x_1, \dots, x_n) = x_1 \oplus x_2 \cdot \dots \cdot x_n$ не обладает свойством синхронизируемости.

2° Функция $f(x_1, \dots, x_n) = x_1 x_2 \oplus \dots \oplus x_{n-1} x_n$, где n — четное, обладает свойством синхронизируемости. Необходимо отметить, что данная функция является бент-функцией.

Пример 22.10. Пусть $f \in \mathcal{F}_n$ и $f(x \oplus e^1) \oplus f(x) = 1$, ($x = (x_1, \dots, x_n)$, $e^1 = (1, 0, \dots, 0)$) т.е. функция f линейна по переменной x_1 . Тогда отображение

$\delta_n^f(\cdot, \varepsilon) : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ является взаимно однозначным и, следовательно, функция f не обладает свойством синхронизируемости.

Рассмотрим ряд утверждений, описывающих свойства классов функций относительно наличия или отсутствия свойства синхронизируемости.

Теорема 22.11. *Пусть функция $f \in \mathcal{F}_n$, существенно зависящая от всех переменных, удовлетворяет следующему условию: АНФ этой функции содержит лишь мономы алгебраической степени 2 вида $x_i x_{i+1}$ для некоторого $i \in \{1, 2, \dots, n-1\}$. Тогда функция f обладает свойством синхронизируемости.*

Доказательство. Предположим, что $s, s' \in \mathbb{F}_2^n$, $s \neq s'$ — произвольная пара несовпадающих состояний автомата $\text{NFSR}(f)$. Тогда существует входное слово $y^1 \in \mathbb{F}_2^n$ этого автомата, что

$$\begin{aligned}\delta_n^f(s, y^1) &= (*, 0, *, 0, \dots), \\ \delta_n^f(s', y^1) &= (0, *, 0, *, \dots).\end{aligned}\tag{22.12}$$

Звездочкой в (22.12) помечены компоненты векторов, конкретные значения которых в данном доказательстве не важны. Существование слова y^1 вытекает из линейной зависимости очередного состояния $\text{NFSR}(f)$ от входного символа. Нетрудно заметить, что для наборов вида $(*, 0, *, 0, \dots) \in \mathbb{F}_2^n$ или $(0, *, 0, *, \dots) \in \mathbb{F}_2^n$ значения функции f равны 0. Наконец, выбрав $y^2 = 0^n$, получаем

$$\delta_n^f((*, 0, *, 0, \dots), 0^n) = \delta_n^f((0, *, 0, *, \dots), 0^n) = 0^n.$$

В результате для входного слова $y = y^1 y^2 \in \mathbb{F}_2^{2n}$ имеем

$$\delta_n^f(s, y) = \delta_n^f(s', y) = 0.$$

Легко видеть (см. лемму [21.7](#)), что доказанное свойство равносильно существованию для $\text{NFSR}(f)$ синхронизирующей последовательности. Следовательно, функция f обладает свойством синхронизируемости. $\square$

Определение 22.12. Множество булевых функций из $\mathcal{F}_n$, обладающих синхронизирующим свойством, для которых выполнены соотношения

$$f(x \oplus e^1) \oplus f(x) \neq 0, f(x \oplus e^n) \oplus f(x) \neq 0,$$

будем обозначать $\mathcal{F}_n^{\text{sync}}$.

Обозначим через $\delta_{n,\varepsilon}^f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ — частичную функцию переходов автомата $\text{NFSR}(f)$:

$$\delta_{n,\varepsilon}^f(x) = \delta_n^f(x, \varepsilon)$$

для любых $x \in \mathbb{F}_2^n$ и $\varepsilon \in \mathbb{F}_2^n$. Полугруппу, порожденную отображениями $\delta_{n,0}^f$ и $\delta_{n,1}^f$ называют (см. [\[КАП 85\]](#)) полугруппой автомата $\text{NFSR}(f)$: $\text{Sem}(\text{NFSR}(f)) = \langle \delta_{n,0}^f, \delta_{n,1}^f \rangle$. Справедливо следующее утверждение.

Предложение 22.13. Функция f из $\mathcal{F}_n$ обладает свойством синхронизируемости ($f \in \mathcal{F}_n^{\text{sync}}$) тогда и только тогда, когда в полугруппе $\text{Sem}(\text{NFSR}(f))$ имеется постоянное отображение (константа).

Доказательство. Непосредственно вытекает из определения [21.5](#). $\square$

На сегодняшний день множество $\mathcal{F}_n^{\text{sync}}$ не описано полностью. Найдены лишь некоторые классы булевых функций, лежащие в $\mathcal{F}_n^{\text{sync}}$. Кроме того, отсутствует описание группы преобразований (в симметрической группе степени 2^n), действующих на $\mathcal{F}_n$ и оставляющих синхронизирующее свойство инвариантным.

Необходимо отметить также, что $\mathcal{F}_n \setminus \mathcal{F}_n^{\text{sync}} \neq \emptyset$ (см. примеры [22.9.1°](#) и [22.10](#)).

Рассмотрим вспомогательное утверждение, полезное при изучении синхронизирующих свойств булевых функций.

Лемма 22.14. *Следующие условия эквивалентны:*

1. $f(x) \in \mathcal{F}_n^{sync}$;
2. $g(x) = 1 \oplus f(x) \in \mathcal{F}_n^{sync}$;
3. $h(x) = f(x \oplus 1^n) \oplus 1 \in \mathcal{F}_n^{sync}$;
4. $h'(x) = f(x \oplus 1^n) \in \mathcal{F}_n^{sync}$.

Доказательство. 1. — 2. Пусть функция f из $\mathcal{F}_n$ обладает свойством синхронизируемости. Тогда для автомата $\text{NFSR}(f)$ существует синхронизирующее слово $y = (y_1, y_2, \dots, y_l) \in \mathbb{F}_2^l$. Следовательно, для любого $s \in \mathbb{F}_2^n$ выполнено

$$\delta_n^f(s, y) = s^\circ = (s_1^\circ, \dots, s_n^\circ), \quad (22.13)$$

где s° — некоторое фиксированное состояние автомата $\text{NFSR}(f)$. Рассмотрим подробнее соотношение (22.13):

$$\begin{aligned} \delta_n^f((s_1, \dots, s_n), y_1) &= (s_2, \dots, s_{n+1}), s_{n+1} = f(s_1, \dots, s_n) \oplus y_1, \\ \delta_n^f((s_2, \dots, s_{n+1}), y_2) &= (s_3, \dots, s_{n+2}), s_{n+2} = f(s_2, \dots, s_{n+1}) \oplus y_2, \\ &\vdots \\ \delta_n^f((s_i, \dots, s_{i+n-1}), y_i) &= (s_{i+1}, \dots, s_{i+n}), s_{i+n} = f(s_i, \dots, s_{i+n-1}) \oplus y_i, \\ &\vdots \\ \delta_n^f((s_l, \dots, s_{l+n-1}), y_l) &= (s_{l+1}, \dots, s_{l+n}), s_{l+n} = f(s_l, \dots, s_{l+n-1}) \oplus y_l, \\ & \\ (s_{l+1}, \dots, s_{l+n}) &= (s_1^\circ, \dots, s_n^\circ). \end{aligned} \quad (22.14)$$

Нетрудно заметить, что i -ое уравнение системы (22.14) можно представить в виде

$$\begin{aligned}
& \delta_n^f((s_i, \dots, s_{i+n-1}), y_i) = \\
& = (s_{i+1}, \dots, s_{i+n-1}, f(s_i, \dots, s_{i+n-1}) \oplus y_i) = \\
& = (s_{i+1}, \dots, s_{i+n-1}, f(s_i, \dots, s_{i+n-1}) \oplus 1 \oplus (y_i \oplus 1)) = \\
& = \delta_n^{1 \oplus f}((s_i, \dots, s_{i+n-1}), y_i \oplus 1) = \delta_n^g((s_i, \dots, s_{i+n-1}), y_i \oplus 1).
\end{aligned} \tag{22.15}$$

Соотношения (22.15) для $i = 1, 2, \dots, l$ показывают, что для любого $s \in \mathbb{F}_2^n$ выполнено

$$\delta_n^g(s, y \oplus 1^l) = s^\circ,$$

т.е. $g(x) = 1 \oplus f(x) \in \mathcal{F}_n^{sync}$. Получаем: из условия 1 следует условие 2. Обратное утверждение доказывается аналогичными рассуждениями из предположения, что $g(x) = 1 \oplus f(x) \in \mathcal{F}_n^{sync}$.

1. — 3. Пусть функция f из $\mathcal{F}_n^{sync}$. Тогда для автомата $\text{NFSR}(f)$ существует синхронизирующее слово $y = (y_1, \dots, y_l) \in \mathbb{F}_2^l$ и выполнено соотношение (22.13). Рассмотрим отображение $\delta_n^h(\cdot, y)$, реализуемое автоматом $\text{NFSR}(h)$, взяв в качестве начального состояния $s' = s \oplus 1^n$, где s — произвольное из $\mathbb{F}_2^n$. Выпишем систему уравнений для $\delta_n^h(s \oplus 1^n, y)$:

$$\begin{aligned}
& \delta_n^h((s_1 \oplus 1, \dots, s_n \oplus 1), y_1) = (s_2 \oplus 1, \dots, s_{n+1} \oplus 1), \\
& \quad \vdots \\
& \delta_n^h((s_i \oplus 1, \dots, s_{i+n-1} \oplus 1), y_i) = (s_{i+1} \oplus 1, \dots, s_{i+n} \oplus 1), \\
& \quad \vdots \\
& \delta_n^h((s_l \oplus 1, \dots, s_{l+n-1} \oplus 1), y_l) = (s_{l+1} \oplus 1, \dots, s_{l+n} \oplus 1),
\end{aligned}$$

где $s_i, i = 1, \dots, l+n$ те же, что и в (22.14). Следовательно, $\delta_n^h(s \oplus 1^n, y) = s^\circ \oplus 1^n$ для любых $s \in \mathbb{F}_2^n$. Очевидно, что тогда $\delta_n^h(s, y) = s^\circ \oplus 1^n$, т.е. $h(x) \in \mathcal{F}_n^{sync}$.

Обратное утверждение очевидно, т.к.

$$h(x \oplus 1^n) \oplus 1 = f(x).$$

1. — 4. Очевидно, т.к. функция $h'(x)$ получается из $f(x)$ комбинацией преобразований, описанных в условиях 2 и 3 леммы 22.14. $\square$

Исследуем некоторые особенности "монотонности" функций, обладающих свойствами синхронизируемости.

Для двух векторов $x = (x_1, \dots, x_n)$ и $y = (y_1, \dots, y_n)$ из $\mathbb{F}_2^n$ выполнено отношение предшествования $x \preceq y$ (см. [Ябл 10]), если

$$x_1 \leq y_1, \dots, x_n \leq y_n.$$

В случае, когда $x \preceq y$ и $x \neq y$, используем обозначение $x \prec y$. Если $x \preceq y$ и $y \preceq z$, то $x \preceq z$. Не все пары находятся в отношении предшествования. Таким образом, пространство $\mathbb{F}_2^n$ с отношением предшествования $\preceq$ является частично упорядоченным множеством.

Определение 22.15. Функция $f \in \mathcal{F}_n$ называется *неубывающей* (в [Ябл 10] — *монотонной*), если для любых двух векторов x и y таких, что $x \preceq y$, имеет место неравенство

$$f(x) \leq f(y).$$

Будем обозначать через $\mathcal{FM}_n^+$ класс неубывающих функций из $\mathcal{F}_n$.

Функция f из $\mathcal{F}_n$ называется *невозрастающей*, если для любых двух векторов x и y таких, что $x \preceq y$, имеет место неравенство

$$f(x) \geq f(y).$$

Будем обозначать через $\mathcal{FM}_n^-$ класс невозрастающих функций из $\mathcal{F}_n$.

Объединение этих классов функций будем обозначать

$$\mathcal{FM}_n = \mathcal{FM}_n^+ \cup \mathcal{FM}_n^- \subset \mathcal{F}_n.$$

Нетрудно заметить, что если $f \in \mathcal{FM}_n^+$, то функции $f'(x) = f(x) \oplus 1$ и $f''(x) = f(x \oplus 1^n)$ принадлежат $\mathcal{FM}_n^-$. С другой стороны, если $g \in \mathcal{FM}_n^-$, то функции $g'(x) = g(x) \oplus 1$ и $g''(x) = g(x \oplus 1^n)$ принадлежат $\mathcal{FM}_n^+$.

Пусть $f \in \mathcal{F}_n$, $\text{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$ и $\overline{\text{supp}(f)} = \mathbb{F}_2^n \setminus \text{supp}(f)$. Докажем утверждения, выделяющие из класса $\mathcal{FM}_n^- \cup \mathcal{FM}_n^+ \subset \mathcal{F}_n$ некоторые подклассы, состоящие из функций, обладающих свойством синхронизируемости.

Теорема 22.16. *Пусть n — четное.*

1. *Если $f \in \mathcal{FM}_n^+$ и для любого $x \in \text{supp}(f)$ выполнено $\text{wt}(x) > n/2$ (либо для любого $x \in \overline{\text{supp}(f)}$ выполнено $\text{wt}(x) < n/2$), то функция f обладает свойством синхронизируемости.*
2. *Если $f \in \mathcal{FM}_n^-$ и для любого $x \in \text{supp}(f)$ выполнено $\text{wt}(x) < n/2$ (либо для любого $x \in \overline{\text{supp}(f)}$ выполнено $\text{wt}(x) > n/2$), то функция f обладает свойством синхронизируемости.*

Доказательство. 1. Пусть $f \in \mathcal{FM}_n^+$ и для любого $x \in \text{supp}(f)$ выполнено $\text{wt}(x) > n/2$. Рассмотрим произвольную пару состояний s^1 и s^2 , $s^1 \neq s^2$ автомата $\text{NFSR}(f)$. Как и ранее в теореме 22.6 воспользуемся линейной зависимостью очередного состояния $\text{NFSR}(f)$ от входного символа. Тогда существует входное слово $y^1 \in \mathbb{F}_2^n$, что $\delta_n^f(s^1, y^1) = 0^n$ и $\delta_n^f(s^2, y^1) = (u_1, \dots, u_n) = u$ — некоторое фиксированное состояние. Подберем теперь такое входное слово $y^2 \in \mathbb{F}_2^{n/2}$, что

$$\begin{aligned}
\delta_n^f(0^n, y^2) &= (\underbrace{0, \dots, 0}_{n/2}, v_1, \dots, v_{n/2}), \\
\delta_n^f(u, y^2) &= (u_{n/2+1}, \dots, u_n, \underbrace{0, \dots, 0}_{n/2}),
\end{aligned} \tag{22.16}$$

где $(v_1, \dots, v_{n/2}) \in \mathbb{F}^{n/2}$ — некоторый фиксированный набор. Поскольку для состояний из (22.16) выполнено

$$\begin{aligned}
\text{wt}((\underbrace{0, \dots, 0}_{n/2}, v_1, \dots, v_{n/2})) &\leq n/2, \\
\text{wt}((u_{n/2+1}, \dots, u_n, \underbrace{0, \dots, 0}_{n/2})) &\leq n/2,
\end{aligned} \tag{22.17}$$

то

$$f((\underbrace{0, \dots, 0}_{n/2}, v_1, \dots, v_{n/2})) = f((u_{n/2+1}, \dots, u_n, \underbrace{0, \dots, 0}_{n/2})) = 0. \tag{22.18}$$

Для состояний (22.16) подберем входное слово $y^3 \in \mathbb{F}_2^n$ такое, что

$$\begin{aligned}
\delta_n^f((\underbrace{0, \dots, 0}_{n/2}, v_1, \dots, v_{n/2}), y^3) &= 0^n, \\
\delta_n^f((u_{n/2+1}, \dots, u_n, \underbrace{0, \dots, 0}_{n/2}), y^3) &= 0^n.
\end{aligned}$$

Это возможно, поскольку, учитывая (22.17) и (22.18), в каждом из n тактов мы выбираем входной символ автомата так, чтобы веса получаемых состояний не увеличивались.

В итоге получаем для входного слова $y = y^1 y^2 y^3$

$$\delta_n^f(s^1, y) = \delta_n^f(s^2, y) = 0^n,$$

т.е. любые два состояния автомата $\text{NFSR}(f)$ подходящим входным словом y переводятся в состояние 0^n . Следовательно (см. лемму 21.7), для данного автомата существует синхронизирующее слово и f обладает свойством синхронизируемости.

Предположим теперь, что $f \in \mathcal{FM}_n^+$ и для любого $x \in \overline{\text{supp}(f)}$ выполнено $\text{wt}(x) < n/2$. Доказательство соответствующего утверждения теоремы проводится аналогично рассмотренному выше с заменой состояния 0^n на состояние 1^n .

2. Доказательство второго утверждения данной теоремы проводится аналогично доказательству первого утверждения. $\square$

Теорема 22.17. Пусть n — нечетное.

1. Если $f \in \mathcal{FM}_n^+$ и для любого $x \in \text{supp}$ выполнено $\text{wt}(x) > \frac{n+1}{2}$ (либо для любого $x \in \overline{\text{supp}(f)}$ выполнено $\text{wt}(x) < \frac{n-1}{2}$), то функция f обладает свойством синхронизируемости.
2. Если $f \in \mathcal{FM}_n^-$ и для любого $x \in \text{supp}(f)$ выполнено $\text{wt}(x) > \frac{n+1}{2}$ (либо для любого $x \in \overline{\text{supp}(f)}$ выполнено $\text{wt}(x) < \frac{n-1}{2}$), то функция f обладает свойством синхронизируемости.

Доказательство. Проводится аналогично доказательству теоремы 22.16. Его особенностью является использование в рассуждениях в качестве подходящей границы (в теореме 22.16 это $\frac{n}{2}$) либо $\frac{n+1}{2}$, либо $\frac{n-1}{2}$. $\square$

§23 Локальные аффинности в задачах обращения дискретных функций

Способы использования сужений дискретных функций в задачах их обращения исторически восходят к классу переборных методов решения систем уравнений над конечными алгебраическими системами (поля Галуа, конечные

кольца, абелевы группы и т. п.). Способы заданий таких систем уравнений должны обладать свойством "эффективности", т.е. дискретные функции, моделируемые данными системами уравнений, должны эффективно вычисляться.

В булевом случае дискретная функция задается системой уравнений в алгебраической нормальной форме (полиномы Жегалкина), либо с помощью табличного представления (или суперпозиции табличных представлений). Размеры таблиц, задающих дискретную функцию, как правило, таковы, что позволяют достаточно легко восстановить алгебраическую нормальную форму соответствующих координатных булевых функций.

Пусть имеется система булевых уравнений, представляющая некоторую дискретную функцию в задаче обращения,

$$\begin{cases} f_1(x_1, x_2, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) = 0, \end{cases} \quad (23.1)$$

$m, n \in \mathbb{N}$ и $m > n$. В задачах обращения преимущественно рассматривают совместные системы (23.1), а в ряде случаев эти системы имеют единственное неизвестное решение.

Достаточно широкий класс методов решения систем вида (23.1) содержит "переборный" этап, заключающийся в опробовании всех возможных значений части неизвестных системы уравнений (см. §10) и выделении соответствующих систем-следствий от меньшего числа переменных.

Этап решения систем-следствий может быть реализован, например, методом линеаризации в модели "случайных систем линейных уравнений" (см. [Мел 11]), использующим критерий мономиальной совместимости. Ясно, что в этом случае размерности получаемых линейных систем уравнений будут примерно равны значениям некоторого положительного полинома $p(\lambda)$ степени большей 1 (степень $p(\lambda)$ зависит от алгебраических степеней уравнений системы (22.1)). При достаточно большом числе переменных - n ($n \approx 128, 256, 1024$ и т. п.) раз-

мерность получаемой линейной системы уравнений $p(n - s)$ (s — число опробуемых переменных) бывает слишком велико для практической реализации алгоритмов их решений.

Целью использования семейств локальных аффинностей функций $f_1, f_2, \dots, f_m$ из (23.1) является: уменьшить размерность линейных задач на этапе решения систем-следствий.

Рассмотрим общую схему использования локальных аффинностей булевых функций для решения систем полиномиальных булевых уравнений.

Пусть $\pi(f_1, \dots, f_m) = \{\pi^r \mid r = 1, 2, \dots, m\}$ — семейство разбиений пространства $\mathbb{F}_2^n$ на локальные аффинности функций $f_1, f_2, \dots, f_m$ из (23.1). Каждое разбиение $\pi^r = \{\pi^{r,1}, \dots, \pi^{r,t_r}\}$ удовлетворяет следующим условиям:

1. $\pi^{r,1}, \dots, \pi^{r,t_r}$ — локальные аффинности функции f_r , $\pi^{r,i} = L^{r,i} \oplus u^{r,i}$ ($L^{r,i}$ — подпространство $\mathbb{F}_2^n$, $u^{r,i} \in \mathbb{F}_2^n$) и $\dim \pi^{r,i} = \dim L^{r,i} = d^{r,i}$, $1 \leq i \leq t_r$;
2. $\pi^{r,1} \cup \dots \cup \pi^{r,t_r} = \mathbb{F}_2^n$;
3. $\pi^{r,i_1} \cap \pi^{r,i_2} = \emptyset$, если $i_1 \neq i_2$;
4. существуют аффинные функции $l^{r,1}, \dots, l^{r,t_r}$ из $\mathcal{A}_n$ такие, что $(f_r)_{\pi^{r,i}} = l^{r,i}|_{\pi^{r,i}}$, $i = 1, \dots, t_r$.

Пусть вектор u из $\mathbb{F}_2^n$ является решением системы уравнений (23.1). Тогда существует набор натуральных чисел $\{\tau_1, \tau_2, \dots, \tau_m\}$, $1 \leq \tau_r \leq t_r$, $1 \leq r \leq m$, удовлетворяющий условию: $u \in \pi^{r,\tau_r}$, $r = 1, 2, \dots, m$.

Векторы из $\mathbb{F}_2^n$, лежащие в плоскости $\pi^{r,i}$, являются решениями системы линейных уравнений (см. [MWS 77])

$$A^{r,i}x = b^{r,i}, \quad (23.2)$$

где $A^{r,i} — $(n - d^{r,i}) \times n$ -матрица, $\text{rank} A^{r,i} = n - d^{r,i}$, $b^{r,i} \in \mathbb{F}_2^{n-d^{r,i}}$.$

Следовательно, для вектора-решения u системы (23.1) выполнено

$$\begin{aligned} l^{r,\tau_r}(u) \oplus l^{r,\tau_r}(0^n) &= l^{r,\tau_r}(0^n), \\ A^{r,\tau_r}u &= b^{r,\tau_r}, \end{aligned} \quad (23.3)$$

$r = 1, 2, \dots, m$. Для произвольного набора натуральных чисел $\{i_1, i_2, \dots, i_m\}$, удовлетворяющих условию $1 \leq i_j \leq t_j$ $j = 1, 2, \dots, m$, соответствующую ему совокупность локальных аффинностей $\{\pi^{1,i_1}, \pi^{2,i_2}, \dots, \pi^{m,i_m}\}$ будем называть траекторией. Каждой траектории, учитывая (23.2) и (23.3), можно поставить в соответствие систему линейных уравнений вида:

$$\left\{ \begin{array}{lcl} l^{1,i_1}(x) \oplus l^{1,i_1}(0^n) & = & l^{1,i_1}(0^n) \\ A^{1,i_1}x & = & b^{1,i_1} \\ l^{2,i_2}(x) \oplus l^{2,i_2}(0^n) & = & l^{2,i_2}(0^n) \\ A^{2,i_2}x & = & b^{2,i_2} \\ \vdots & & \\ l^{m,i_m}(x) \oplus l^{m,i_m}(0^n) & = & l^{m,i_m}(0^n) \\ A^{m,i_m}x & = & b^{m,i_m}. \end{array} \right. \quad (23.4)$$

Система (23.4) состоит из $m(n+1) - \sum_{r=1}^m d^{r,i_r}$ линейных уравнений от n переменных.

Траекторию, соответствующую набору $\{\tau_1, \tau_2, \dots, \tau_m\}$ будем называть траекторией решения системы (23.1). Очевидно, что число траекторий решений не более числа решений системы (23.1).

В случае, когда система (23.1) имеет единственное решение, ему соответствует единственная траектория решения $\{\pi^{1,\tau_1}, \pi^{2,\tau_2}, \dots, \pi^{m,\tau_m}\}$.

Приведем краткое описание метода решения систем булевых полиномиальных уравнений, использующего локальные аффинности уравнений (ЛАФ-метод).

ЛАФ-метод.

1. Предварительный этап.

Построение разбиений пространства $\mathbb{F}_2^n$ на локальные аффинности для булевых функций $f_1, f_2, \dots, f_m$, задающих систему (23.1):

$$\pi(f_1, f_2, \dots, f_m) = \{\pi^r \mid r = 1, 2, \dots, m\}.$$

2. Основной этап.

Перебор траекторий $\{\pi^{1,i_1}, \pi^{2,i_2}, \dots, \pi^{m,i_m}\}$, $1 \leq i_1 \leq t_1$, $1 \leq i_2 \leq t_2, \dots, 1 \leq i_m \leq t_m$, с последующим решением системы линейных уравнений (23.4). Перебор траекторий осуществляется до момента выделения решения системы (23.1).

Число перебираемых траекторий в ходе реализации ЛАФ-метода не превосходит $\prod_{r=1}^m t_r$. Трудоемкость решения системы линейных уравнений (23.4) для траектории $\{\pi^{1,i_1}, \pi^{2,i_2}, \dots, \pi^{r,i_r}\}$ методом Гаусса составляет $O\left(\left[m(n+1) - \sum_{r=1}^m d^{r,i_r}\right] n^2\right)$ двоичных операций. Тогда общая трудоемкость метода не превосходит

$$O\left(\prod_{r=1}^m t_r \left[m(n+1) - \sum_{r=1}^m d^{r,i_r}\right] n^2\right)$$

двоичных операций.

Пример 23.1. Системы квадратичных булевых уравнений. Известно, что задача поиска решения произвольной нелинейной системы булевых уравнений не менее сложна, чем задача распознавания совместности такой системы, принадлежащая классу $\mathcal{NP}$ и являющейся $\mathcal{NP}$ -полной. Поэтому поиск эффективных методов решения систем квадратичных булевых уравнений является актуальной теоретической задачей. Кроме того, эта задача актуальна в свете имеющихся попыток построения криптосистем с открытым ключом на основе сложности решения систем квадратичных уравнений (см. [Bar 09], [GoTa 17]).

Пусть для системы (23.1) выполнено $\deg(f_1) = \deg(f_2) = \dots = \deg(f_m) = 2$ и $m \leq n^k, k \leq 2$. Нас будет интересовать трудоемкость первого этапа ЛАФ-метода в данном случае, поскольку основной этап этого метода сводится к перебору линейных систем уравнений и их решению.

Реализация первого этапа ЛАФ-метода связана с теоремой Диксона.

Теорема 23.2 ([MWS 77]). Пусть

$$f(x) = xQ_fx^\top \oplus \langle a_f, x \rangle \oplus c \quad -$$

квадратичная функция из $\mathcal{F}_n$, где

$$Q_f = \begin{bmatrix} 0 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ddots & a_{n-1n} \\ 0 & 0 & \cdots & 0 \end{bmatrix}, a_f = (a_1, \dots, a_n) \in \mathbb{F}_2^n, c \in \mathbb{F}_2^n.$$

Тогда существует такой элемент $\mathfrak{g} \in \mathfrak{GA}(n)$, что $f^\mathfrak{g}$ имеет один из перечисленных ниже видов:

- a) если $\text{rank}(Q_f \oplus Q_f^\top) = 0$, то либо $f^\mathfrak{g}(x) = \varepsilon, \varepsilon \in \mathbb{F}_2$, либо $f^\mathfrak{g}(x) = x_1$;
- b) если $\text{rank}(Q_f \oplus Q_f^\top) = 2s, s \geq 1$, то либо

$$f^\mathfrak{g} = \bigoplus_{j=1}^s x_{2j-1}x_{2j} \oplus \varepsilon, \varepsilon \in \mathbb{F}_2,$$

либо

$$f^\mathfrak{g}(x) = \bigoplus_{j=1}^s x_{2j-1}x_{2j} \oplus x_{2s+1}.$$

Если $\text{rank}(Q_f \oplus Q_f^\top) = 2s$, то первоначально выполняем s следующих шагов. Без нарушения общности считаем, что моном x_1x_2 содержится в АНФ

функции f . Тогда f представляется в виде

$$f(x) = x_1 x_2 \oplus x_1 l^1(x_3, \dots, x_n) \oplus x_2 l^2(x_3, \dots, x_n) \oplus h(x_3, \dots, x_n),$$

где $\deg(l^1) \leq 1$, $\deg(l^2) \leq 1$, $\deg(h) \leq 2$. Сделаем аффинную замену переменных $x_1 \leftarrow x_1 \oplus l^2(x_3, \dots, x_n)$, $x_2 \leftarrow x_2 \oplus l^1(x_3, \dots, x_n)$. Тогда функция $f(x)$ перейдет в функцию $f^1(x) = x_1 x_2 \oplus h^1(x_3, \dots, x_n)$, где $\deg(h^1) \leq 2$. Проведя еще $s - 1$ раз аффинную замену переменных, мы получим функцию

$$f^s(x) = x_1 x_2 \oplus \dots \oplus x_{2s-1} x_{2s} \oplus l(x_{2s+1}, \dots, x_n), \quad (23.5)$$

где $\deg(l) \leq 1$.

Очевидно, что трудоемкость T_i приведения к виду (23.5) совпадает с общей трудоемкостью совокупности описанных выше аффинных замен переменных, т.е. $T_i \leq n^{c_i}$ (дв. оп.), где c_i — некоторая положительная константа. Тогда для трудоемкости T приведения функций $f_1, \dots, f_m$ к виду (23.5) справедливо неравенство

$$T = \sum_{i=1}^m T_i \leq \sum_{i=1}^m n^{c_i}. \quad (23.6)$$

Вид АНФ функции f^s позволяет задать разбиение пространства $\mathbb{F}_2^n$ на локальные аффинности этой функции различными способами. Рассмотрим один из возможных вариантов.

Пусть $b = (b_1 \dots b_s) \in \mathbb{F}_2^s$. Обозначим через $\pi_{1,3,\dots,2s-1}^b$ плоскость в пространстве $\mathbb{F}_2^n$, задаваемую системой уравнений

$$\left\{ \begin{array}{lcl} x_1 & = & b_1 \\ x_3 & = & b_2 \\ \vdots & & \\ x_{2s-1} & = & b_s. \end{array} \right. \quad (23.7)$$

Из (23.5) очевидно, что плоскость $\pi_{1,3,\dots,2s-1}^b$ является локальной аффинностью функции f^s . При этом f^s совпадает на плоскости $\pi_{1,3,\dots,2s-1}^b$ с аффинной функцией

$$l_{1,3,\dots,2s-1}^{s,b}(x) = b_1x_2 \oplus \dots \oplus b_sx_{2s} \oplus l(x_{2s+1}, \dots, x_n). \quad (23.8)$$

Тогда $\pi^*(f) = \{\pi_{1,3,\dots,2s-1}^b \mid b \in \mathbb{F}_2^s\}$ является разбиением пространства $\mathbb{F}_2^n$ на локальные аффинности функции f^s , а семейство аффинных функций $\{l_{1,3,\dots,2s-1}^{s,b} \mid b \in \mathbb{F}_2^s\}$ являются сужениями функции f^s на соответствующие локальные аффинности.

Пусть функции $f_1, \dots, f_m$ из (23.1) приводятся аффинными преобразованиями переменных к функциям $f_1^{s_1}, \dots, f_m^{s_m}$ вида (23.5), $\pi^*(f_1^{s_1}), \dots, \pi^*(f_m^{s_m})$ — соответствующие этим функциям разбиения на локальные аффинности вида (23.7), а $\mathcal{L}^*(f_1^{s_1}), \dots, \mathcal{L}^*(f_m^{s_m})$ — семейства аффинных функций-сужений вида (23.8), представляющих функции $f_1^{s_1}, \dots, f_m^{s_m}$ на локальных аффинностях разбиений $\pi^*(f_1^{s_1}), \dots, \pi^*(f_m^{s_m})$.

Далее для каждой пары $\{\pi^*(f_i^{s_i}), \mathcal{L}^*(f_i^{s_i})\}$, $i = 1, \dots, m$ необходимо применить аффинные преобразования координат, обратные тем, что были использованы при их (этих пар) построении. Таким образом, мы получим описание:

1. $\pi(f_1, \dots, f_m) = \{\pi(f_1), \dots, \pi(f_m)\}$ — семейства разбиений пространства $\mathbb{F}_2^n$ на локальные аффинности функций $f_1, \dots, f_m$;
2. $\mathcal{L}(f_1, \dots, f_m) = \{\mathcal{L}(f_1), \dots, \mathcal{L}(f_m)\}$ — семейства аффинных функций-сужений, представляющих функции $f_1, \dots, f_m$ на локальных аффинностях разбиений $\pi(f_1), \dots, \pi(f_m)$. Трудоемкость $T_{\text{обр}}$ (дв. оп.) этих преобразований также, очевидно, не превосходит значения некоторого полинома, т.е. $T_{\text{обр}} \leq \sum_{i=1}^m n^{c'_i}$, где $c'_i = \text{const}$, $i = 1, 2, \dots, m$. Следовательно, трудоемкость предварительного этапа ЛАФ-метода для систем квадратных уравнений асимптотически полиномиальна от числа неизвестных в системе.

Рассмотрим теперь возможности использования понятия "локальная аффинность" для решения систем уравнений, описывающих функционирование фильтрующих генераторов псевдослучайных последовательностей (см. Приложение А,г)). Решение этих систем является активно развиваемым в криптоанализе направлением исследований.

В ряде случаев для нахождения решения таких систем используются теоретико-вероятностные, статистические и теоретико-кодовые методы. Существуют подходы к решению, когда исходная система погружается в действительную область, и решение находится с помощью соответствующих псевдобулевых неравенств. Известны алгебраические методы решения таких систем, использующие аппарат базисов Гребнера. В последнее время активно исследуются возможности использования для этих целей решателей задачи КНФ-выполнимости.

Наиболее эффективными методами являются методы линеаризации исходной системы уравнений. Ниже будет рассмотрен метод линеаризации системы уравнений фильтрующего генератора без увеличения размерности задачи.

Для фильтрующего генератора LFSR $(c(\lambda), f)$ система уравнений (23.1) будет иметь вид

$$\left\{ \begin{array}{llll} f_0(x) & = & f(x) & = & f(x_0, \dots, x_{n-1}) & = & y_0 \\ f_1(x) & = & f(Bx) & = & f(B(x_0, \dots, x_{n-1})) & = & y_1 \\ & \vdots & & & & & \\ f_r(x) & = & f(B^r x) & = & f(B^r(x_0, \dots, x_{n-1})) & = & y_r \\ & \vdots & & & & & \\ f_{m-1}(x) & = & f(B^{m-1} x) & = & f(B^{m-1}(x_0, \dots, x_{n-1})) & = & y_{m-1}, \end{array} \right. \quad (23.9)$$

где B — матрица линейного преобразования, реализуемого регистром LFSR $(n, c(\lambda))$, $x = (x_0, \dots, x_{m-1})$ — неизвестное начальное состояние фильтрующего генератора, $(y_0, y_1, \dots, y_{m-1})$ — известный фрагмент последователь-

ности, выработанной фильтрующим генератором. Как и ранее, будем предполагать, что $m > n$.

Пусть $\pi(f) = \pi = \{\pi^1, \dots, \pi^t\}$ — разбиение пространства $\mathbb{F}_2^n$ на локальные аффинности для функции $f_0 = f$, где $\pi^i = L^i \oplus u^i$, L^i — некоторое подпространство в $\mathbb{F}_2^n$, $u^i \in \mathbb{F}_2^n$, $i = 1, 2, \dots, t$. Аффинная нормальная форма функции f_0 имеет вид (см. определение 15.2.b):

$$f(x) = \bigoplus_{i=1}^t \prod_{j=1}^{n-\dim \pi^i} \left(a_1^{i,j} x_1 \oplus \dots \oplus a_n^{i,j} x_n \oplus b^{i,j} \right) l^i(x), \quad (23.10)$$

где $l^i \in \mathcal{A}_n$ и $f_{\pi^i} = l^i$, $i = 1, 2, \dots, t$.

Для удобства положим $r_i = n - \dim \pi^i$ и $l^i(x) = \langle v^i, x \rangle \oplus \varepsilon^i$, $v^i \in \mathbb{F}_2^n$, $i = 1, 2, \dots, t$. Кроме того, для $a^{i,j} = (a_1^{i,j}, \dots, a_n^{i,j}) \in \mathbb{F}_2^n$ имеем

$$a_1^{i,j} x_1 \oplus \dots \oplus a_n^{i,j} x_n \oplus b^{i,j} = \langle a^{i,j}, x \rangle \oplus b^{i,j}.$$

Для произвольного x из $\mathbb{F}_2^n$ будем называть конечный набор векторов

$$(x, Bx, \dots, B^k x, \dots, B^{m-1} x) \quad (23.11)$$

траекторий вектора x относительно линейного преобразования, определяемого матрицей B . Поскольку $\pi = \{\pi^1, \dots, \pi^t\}$ является разбиением пространства $\mathbb{F}_2^n$, то существует однозначно определенный набор

$$(i_0, i_1, \dots, i_{m-1}) \in \{1, \dots, t\}^m$$

такой, что

$$x \in \pi_{i_0}, Bx \in \pi_{i_1}, \dots, B^{m-1}x \in \pi_{i_{m-1}}.$$

Набор плоскостей

$$(\pi_{i_0}, \pi_{i_1}, \dots, \pi_{i_{m-1}}), \quad (23.12)$$

$\pi_{i_k} \in \pi, k = 0, 1, \dots, m - 1$ будем называть аффинной траекторией вектора x относительно линейного преобразования, определяемого матрицей B .

Пусть нам известен набор $(y_0, y_1, \dots, y_{m-1})$ правых частей системы (23.9). Основная идея нахождения неизвестного набора $x = (x_0, x_1, \dots, x_{n-1})$ состоит в сведении решения нелинейной системы (23.9) к решению некоторой совокупности линейных систем от того же числа переменных, определяемых аффинной нормальной формой функции f , матрицей B , аффинными траекториями вида (23.12) и набором $(y_0, y_1, \dots, y_{m-1})$. Будем опробовать аффинные траектории вида (23.12). Всего таких траекторий будет t^m .

Предположение о том, что $B^k x \in \pi_{i_k}$ влечет за собой выполнение равенств

$$\begin{aligned} f(B^k x) &= \bigoplus_{i=1}^t I_{\pi_i}(B^k x) l^i(B^k x) = \\ &= I_{\pi_{i_k}}(B^k x) l^{i_k}(B^k x) = y_k, \end{aligned}$$

т. е.

$$I_{\pi_{i_k}}(B^k x) = 1, l^{i_k}(B^k x) = y_k.$$

Последние равенства эквивалентны системе линейных уравнений вида:

$$\left\{ \begin{array}{l} \langle a^{i_k, 1}, B^k x \rangle \oplus b^{i_k, 1} = 1 \\ \vdots \\ \langle a^{i_k, r_{i_k}}, B^k x \rangle \oplus b^{i_k, r_{i_k}} = 1 \\ \langle v^{i_k}, B^k x \rangle \oplus \varepsilon^{i_k} = y_k. \end{array} \right. \quad (23.13)$$

Систему (23.13) можно привести к виду

$$\left\{ \begin{array}{l} \langle (B^k)^\top a^{i_k,1}, x \rangle = b^{i_k,1} \oplus 1 \\ \vdots \\ \langle (B^k)^\top a^{i_k, r_{i_k}}, x \rangle = b^{i_k,1} \oplus 1 \\ \langle (B^k)^\top v^{i_k}, x \rangle = \varepsilon^{i_k} \oplus y_k \end{array} \right. \quad (23.14)$$

или

$$\mathcal{B}^k x = (b^{i_k,1} \oplus 1, \dots, b^{i_k, r_{i_k}}, \varepsilon^{i_k} \oplus y_k)^\top, \quad (23.15)$$

где $\mathcal{B}^k$ — $(r_{i_k} + 1) \times n$ -матрица.

Для удобства обозначим правую часть равенства (23.15) через $z^k = (z_1^k, \dots, z_{r_{i_k}}^k, z_{r_{i_k}+1}^k)^\top$.

Предположим, что вектор x имел аффинную траекторию (23.12). Это предположение приводит нас к системе линейных уравнений

$$\mathcal{B}x = \begin{bmatrix} \mathcal{B}^0 \\ \mathcal{B}^1 \\ \vdots \\ \mathcal{B}^{m-1} \end{bmatrix} x = \begin{bmatrix} z^0 \\ z^1 \\ \vdots \\ z^{m-1} \end{bmatrix} = z, \quad (23.16)$$

где $\mathcal{B} = \left(\sum_{i=0}^{m-1} r_{i_k} + m \right) \times n$ -матрица.

Опробование аффинных траекторий.

Этап 1.

1.1 Исходной совокупностью перебора является разбиение на локальные аффинности области определения фильтрующей функции.

1.2 Из $\pi(f) \times \pi(f)$ выделяем $\mathcal{M}_2$ — множество аффинных траекторий длины 2, для которых выполнено равенство

$$\text{rank} \begin{bmatrix} \mathcal{B}_0 \\ \mathcal{B}_1 \end{bmatrix} = \text{rank} \begin{bmatrix} \mathcal{B}_0 & | & z_0 \\ \mathcal{B}_1 & | & z_1 \end{bmatrix}.$$

1.3 Из $\mathcal{M}_2 \times \pi(f)$ выделяем $\mathcal{M}_3$ — множество аффинных траекторий длины 3, для которых выполнено равенство

$$\text{rank} \begin{bmatrix} \mathcal{B}_0 \\ \mathcal{B}_1 \\ \mathcal{B}_2 \end{bmatrix} = \text{rank} \left[\begin{array}{c|c} \mathcal{B}_0 & z_0 \\ \mathcal{B}_1 & z_1 \\ \mathcal{B}_2 & z_2 \end{array} \right].$$

$$\vdots \quad \vdots \quad \vdots$$

1.k Из $\mathcal{M}_{k-1} \times \pi(f)$ выделяем $\mathcal{M}_k$ — множество аффинных траекторий длины k , для которых выполнено равенство

$$\text{rank} \begin{bmatrix} \mathcal{B}_0 \\ \mathcal{B}_1 \\ \vdots \\ \mathcal{B}_{k-1} \end{bmatrix} = \text{rank} \left[\begin{array}{c|c} \mathcal{B}_0 & z_0 \\ \mathcal{B}_1 & z_1 \\ \vdots & \\ \mathcal{B}_{k-1} & z_{k-1} \end{array} \right].$$

$$\vdots \quad \vdots \quad \vdots$$

1.m Из $\mathcal{M}_{m-1} \times \pi(f)$ выделяем $\mathcal{M}_m$ — множество аффинных траекторий длины m , для которых выполнено равенство

$$\text{rank} \begin{bmatrix} \mathcal{B}_0 \\ \mathcal{B}_1 \\ \vdots \\ \mathcal{B}_{m-1} \end{bmatrix} = \text{rank} \left[\begin{array}{c|c} \mathcal{B}_0 & z_0 \\ \mathcal{B}_1 & z_1 \\ \vdots & \\ \mathcal{B}_{m-1} & z_{m-1} \end{array} \right].$$

Этап 2. Для аффинных траекторий множества $\mathcal{M}_m$ находим решения соответствующих линейных систем.

Этап 3. Проверяем все полученные на предыдущем этапе возможные начальные состояния фильтрующего генератора на соответствие выходной после-

довательности длины большей m . После отбраковки ложных вариантов начальных состояний находим истинное начальное состояние.

Замечание 23.3. При расчетах трудоемкости этапа 1 можно в предварительном порядке использовать особенности аффинной нормальной формы функции f вне зависимости от выходного набора генератора y . Для этого проводится последовательное выделение наборов локальных аффинностей из $\pi(f)$ на основе выполнения равенства рангов для систем уравнений без учета уравнений вида $\langle v^{i,k}, B^k x \rangle \oplus \varepsilon^{i_k} = y_k, k = 0, 1, \dots, m$ (см. (23.13)). Этот процесс позволяет выделить "запретные наборы" (пары, тройки и т. д.) и использовать эту информацию для определения неизвестного начального состояния фильтрующего генератора для индивидуального входного набора y .

Замечание 23.4. Как уже было отмечено ранее, представления булевых функций в реализациях средств информационной безопасности должны удовлетворять свойству эффективной вычислимости их значений. Это обстоятельство предопределяет выбор используемых функций. Например, если булева функция от достаточно большого числа переменных $n = 128, 256$ реализуется в полиномиальном базисе, то, как правило, число мономов в алгебраической нормальной форме не превосходит $O(n)$. Если используется табличный способ, то естественно приемлемым вариантом реализации функции будет суперпозиция функций от меньшего числа переменных.

В работах [ЛСФ 19.1] и [ЛСФ 19.2] приведены примеры систем булевых уравнений, для которых данный метод нахождения решения имеет асимптотически полиномиальную трудоемкость от числа переменных.

§24 Синтез совершенно уравновешенных функций на основе операции "сдвиг-композиция"

Пусть, как и ранее, $A = \{a_1, a_2, \dots, a_q\}$ — конечное множество символов (алфавит) мощности q , $q \geq 2$. Для произвольных натуральных чисел m и n через $\mathcal{F}_{n,m,q}$ будем обозначать множество всех функций вида $f : A^n \rightarrow A^m$. Функция $f(x_1, \dots, x_n)$ из $\mathcal{F}_{n,m,q}$ существенно зависит от переменной x_i , $1 \leq i \leq n$, если для некоторой пары наборов $u, v \in A^n$ таких, что

$$u_i \neq v_i, (u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_n) = (v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n),$$

выполнено условие $f(u) \neq f(v)$. Переменные x_1 и x_n для функции $f(x_1, \dots, x_n)$ будем называть крайними. Будем говорить, что функция $f(x_1, x_2, \dots, x_n)$ из $\mathcal{F}_{n,1,q}$ перестановочна по переменной x_i , $1 \leq i \leq n$, если для любого набора $c = (c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n) \in A^{n-1}$ функция

$$\varphi(x_i) = f(c_1, \dots, c_{i-1}, x_i, c_{i+1}, \dots, c_n)$$

является некоторой перестановкой элементов алфавита A .

Для произвольной функции $f \in \mathcal{F}_{n,1,q}$ и произвольного натурального m через f_m будем обозначать функцию из $\mathcal{F}_{n,m,q}$ вида:

$$\begin{aligned} f_m(x_1, \dots, x_{m+n-1}) = \\ = (f(x_1, \dots, x_n), f(x_2, \dots, x_{n+1}), \dots, f(x_m, \dots, x_{m+n-1})). \end{aligned} \tag{24.1}$$

Определение 24.1. Функция $f \in \mathcal{F}_{n,1,q}$ называется совершенно уравновешенной, если для любого натурального m и для любого набора $y \in A^m$ выполнено

равенство

$$\#f_m^{-1}(y) = \# \{x \in A^{m+n-1} : f_m(x) = y\} = q^{n-1}$$

(другое название — сильно равновероятная функция).

Пример 24.2. Функция $f \in \mathcal{F}_{n,1,q}$ перестановочная по переменной x_1 (либо перестановочная по переменной x_n) является совершенно уравновешенной функцией. Необходимо отметить, что свойство перестановочности булевой функции по некоторой переменной означает линейность по данной переменной ее АНФ (полинома Жегалкина).

Для произвольной $f \in \mathcal{F}_{n,1,q}$ и произвольного натурального числа m рассмотрим множество

$$J(f,m) = \{y \in A^m : \forall x \in A^{m+n-1} f_m(x) \neq y\}.$$

Определение 24.3. Функция $f \in \mathcal{F}_{n,1,q}$ имеет дефект нуль, если для любого натурального m выполнено условие $\#J(f,m) = 0$. Функции, обладающие этим свойством называют функциями дефекта нуль (другое название — функции без запрета).

Определение 24.4. Функция $f \in \mathcal{F}_{n,1,q}$ называется функцией без потери информации, если при любом натуральном $r > 2n$ не существует двух различных наборов $x, x' \in A^r$ таких, что

$$(x_1, \dots, x_n) = (x'_1, \dots, x'_n), (x_{r-n+1}, \dots, x_r) = (x'_{r-n+1}, \dots, x'_r)$$

и

$$f_{r-n+1}(x) = f_{r-n+1}(x').$$

Справедливо утверждение, устанавливающее связь между определенными выше понятиями.

Теорема 24.5 ([Hed 69], [Сум 94]). Пусть $f \in \mathcal{F}_{n,1,q}$, n — произвольное натуральное. Тогда следующие условия эквивалентны:

1. f — совершенно уравновешенная функция;
2. f — функция дефекта нуль;
3. f — функция без потери информации.

Некоторые преобразования булевых функций, оставляющие инвариантным свойство совершенной уравновешенности, рассмотрены в [Сум 94]. Их аналоги для функций над произвольным конечным алфавитом могут быть определены следующим образом.

Пусть на конечном алфавите A определена групповая операция, т.е. $G = (A, +)$ — конечная группа порядка q . Рассмотрим следующие преобразования на $\mathcal{F}_{n,1,q}$:

$$\begin{aligned}\gamma_1^c &: f(x_1, \dots, x_n) \rightarrow f(x_1, \dots, x_n) + c, \quad c \in A; \\ \gamma_2^c &: f(x_1, \dots, x_n) \rightarrow f(x_1 + c, \dots, x_n + c), \quad c \in A; \\ \gamma_3 &: f(x_1, \dots, x_n) \rightarrow f(x_n, \dots, x_1).\end{aligned}\tag{24.2}$$

Нетрудно заметить, что отображения (24.2) обладают следующим свойством: класс функций из $\mathcal{F}_{n,1,q}$, перестановочных по крайней мере по одной из крайних переменных, инвариантен относительно этих преобразований (см. пример 24.2). Таким образом, преобразования вида (24.2) не могут быть использованы для порождения широких классов совершенно уравновешенных функций на основе функций из примера 24.2.

Для произвольных функций $f \in \mathcal{F}_{k,1,q}$, $g \in \mathcal{F}_{l,1,q}$ определим операцию

$$\begin{aligned}f \triangleleft g(x_1, \dots, x_{k+l-1}) &= h(x_1, \dots, x_{k+l-1}) = \\ &= f(g(x_1, \dots, x_k), g(x_{k+1}, \dots, x_{k+l-1}))\end{aligned}\tag{24.3}$$

Соотношение (24.3) показывает, что операция " $\triangleleft$ " является частным видом суперпозиции функций, который обычно называют сдвиг-композиция (см. [Сол 07]) функций f и g . Справедливо следующее утверждение.

Теорема 24.6. Пусть $f \in \mathcal{F}_{k,1,q}$, $g \in \mathcal{F}_{l,1,q}$. Функция $h = f \triangleleft g \in \mathcal{F}_{k+l-1,1,q}$ является совершенно уравновешенной тогда и только тогда, когда функции f и g совершенно уравновешенны.

Доказательство. Пусть $f \in \mathcal{F}_{k,1,q}$ и $g \in \mathcal{F}_{l,1,q}$ — совершенно уравновешенные функции, m — произвольное натуральное число. Тогда для любого набора $z \in A^m$ имеем $\#f_m^{-1}(z) = q^{k-1}$, а для произвольного набора $y \in f_m^{-1}(z) \subseteq A^{m+k-1}$ выполняется равенство $\#g_{m+k-1}^{-1}(y) = q^{l-1}$. Воспользовавшись этими соотношениями для функции $h = f \triangleleft g$ и произвольного $z \in A^m$ получаем

$$\#h_m^{-1}(z) = \#(f \triangleleft g)^{-1}(z) = \sum_{y \in f_m^{-1}(z)} \#g_{m+k-1}^{-1}(y) = q^{k+l-2} = q^{(k+l-1)-1}.$$

Следовательно, функция $h \in \mathcal{F}_{k+l-1,1,q}$ является совершенно уравновешенной.

Обратно. Предположим, что функция $h = f \triangleleft g$ из $\mathcal{F}_{k+l-1,1,q}$ является совершенно уравновешенной. Пусть функция $f \in \mathcal{F}_{k,1,q}$ не является совершенно уравновешенной. Тогда в соответствии с утверждением теоремы 24.5 существует натуральное m , что $\#J(f, m) \neq 0$. Поэтому существует $z \in J(h, m)$, т.е. для функции h выполняется $\#J(h, m) \neq 0$. Следовательно, в соответствии с утверждением теоремы 24.5 функция h не является совершенно уравновешенной, что противоречит нашему предположению о ней. Тогда f — совершенно уравновешенная функция.

Пусть теперь функция $g \in \mathcal{F}_{l,1,q}$ не является совершенно уравновешенной. Тогда существует натуральное число r и набор $\tilde{y} \in A^r$ такой, что $\#g_r^{-1}(\tilde{y}) \neq 2^{l-1}$. Поскольку сумма мощностей прообразов наборов из A^r относительно функ-

ции $g_r \in \mathcal{F}_{l+r-1,r,q}$ равна q^{r+l-1} , то существует набор $y^* \in A^r$ такой, что

$$\#g_r^{-1}(y^*) = p^{l-1} + \alpha,$$

где $\alpha \geq 1$. Используя набор y^* , строим множество наборов $M_{r,t} \subseteq A^{r(t+1)+(l-1)t}$, $t = 1, 2, \dots$ вида

$$y = (y^*, y_{r+1}, \dots, y_{r+l-1}, y^*, \dots, y^*, y_{rt+(t-1)(l-1)+1}, \dots, y_{rt+t(l-1)}, y^*), \quad (24.4)$$

где компоненты набора y , не отмеченные звездочкой, произвольны. Тогда $\#M_{r,t} = (q^{l-1})^t$, $t = 1, 2, \dots$. Для произвольного $y \in M_{r,t}$ такого, что

$$g_{r(t+1)+t(l-1)}^{-1}(y) \neq \emptyset$$

выполнено включение

$$g_{r(t+1)+t(l-1)}^{-1}(y) \subseteq \underbrace{g_r^{-1}(y^*) \times \dots \times g_r^{-1}(y^*)}_{t+1}.$$

Кроме того, заметим, что

$$g_{r(t+1)+t(l-1)} \left(\underbrace{g_r^{-1}(y^*) \times \dots \times g_r^{-1}(y^*)}_{t+1} \right) \subset M_{r,t}.$$

Обозначим через λ_t — среднее число наборов из множества $g_r^{-1}(y^*) \times \dots \times g_r^{-1}(y^*)$, приходящихся на каждый набор из множества $M_{r,t}$. Тогда

$$\lambda_t = \frac{(q^{l-1} + \alpha)^{t+1}}{(q^{l-1})^t} = q^{l-1} \left(1 + \frac{\alpha}{q^{l-1}} \right)^{t+1}.$$

Так как $\left(1 + \frac{\alpha}{q^{l-1}}\right) > 1$, то существует натуральное число t_0 такое, что $\lambda_{t_0} > q^{(k+l-1)-1}$. Следовательно, существует набор $y \in M_{r,t_0}$, для которого

$$\#g_{r(t_0+1)+(l-1)t_0}^{-1}(y) > q^{(k+l-1)-1}. \quad (24.5)$$

Пусть $z = f_{r(t_0+1)+(l-1)t_0-k+1}(y)$. Воспользовавшись неравенством (24.5), получаем, что для функции $h = f \triangleleft g$, зависящей от $k + l - 1$ переменных, выполнено

$$\#h_{(t_0+1)(r+l-1)-(k+l-1)+1}^{-1}(z) > q^{(k+l-1)-1},$$

т.е. функция $h = f \triangleleft g$ не является совершенно уравновешенной. Полученное противоречие доказывает утверждение теоремы. $\square$

Рассмотрим некоторые примеры использования утверждения теоремы 24.6 для синтеза совершенно уравновешенных функций, не являющихся перестановочными по крайним переменным (но существенно зависящих от них), над произвольным примарным алфавитом, т.е. $q = p^c$, p — простое число. В качестве алфавитов будем выбирать поля Галуа.

Пример 24.7 ([Log 07]). Пусть $A = \mathbb{F}_2$ ("⊕" и "." — сложение и умножение по (mod 2)). Рассмотрим пару совершенно уравновешенных функций:

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3 \in \mathcal{F}_{3,1,2}, g(x_1, x_2, x_3) = x_1 x_2 \oplus x_3 \in \mathcal{F}_{3,1,2}.$$

Тогда

$$\begin{aligned} h(x_1, x_2, \dots, x_5) &= f \triangleleft g(x_1, x_2, \dots, x_5) = \\ &= f(g(x_1, x_2, x_3), g(x_2, x_3, x_4), g(x_3, x_4, x_5)) = \\ &= x_3 \oplus x_1 x_2 \oplus x_3 x_4 \oplus x_4 x_5 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 = \end{aligned}$$

совершенно уравновешенная функция, не являющаяся линейной ни по одной из крайних переменных.

Пример 24.8. Пусть $A = \mathbb{F}_3$ ("⊕" и "." — сложение и умножение по (mod 3)). Рассмотрим пару совершенно уравновешенных функций:

$$f(x_1, x_2, x_3) = x_1x_2 + x_3 \in \mathcal{F}_{3,1,3}, g(x_1, x_2, x_3) = x_1 + x_2x_3^2 \in \mathcal{F}_{3,1,3}.$$

Тогда

$$\begin{aligned} h(x_1, x_2, \dots, x_5) &= f \triangleleft g(x_1, x_2, \dots, x_5) = \\ &= (x_1 + x_2x_3^2)(x_2 + x_3x_4^2) + x_3x_4x_5^2 = \\ &= x_1x_2 + x_1x_3x_4^2 + x_2^2x_3^2 + x_2x_3^3x_4^2 + x_3 + x_4x_5^2 — \end{aligned}$$

совершенно уравновешенная функция из $\mathcal{F}_{5,1,3}$, существенно зависящая от всех переменных. Непосредственной проверкой легко убедиться, что функция h не является перестановочной ни по одной из крайних переменных.

Пример 24.9. Пусть $A = \mathbb{F}_p$ — произвольное конечно поле из q элементов, $q > 3$ ("+" и "." — сложение и умножение в $\mathbb{F}_q$). Рассмотрим пару совершенно уравновешенных функций:

$$f(x_1, x_2) = x_1 + x_2^{q-1} \in \mathcal{F}_{2,1,q}, g(x_1, x_2) = x_1^{q-1} + x_2 \in \mathcal{F}_{2,1,q}.$$

Тогда

$$h(x_1, x_2, x_3) = f \triangleleft g(x_1, x_2, x_3) = x_1^{q-1} + x_2 + (x_2^{q-1} + x_3)^{q-1} —$$

совершенно уравновешенная функция из $\mathcal{F}_{3,1,q}$, существенно зависящая от всех переменных. Непосредственной проверкой легко убедиться, что функция h не является перестановочной ни по одной из крайних переменных.

Пример 24.10. Пусть $A = \mathbb{F}_q$ — произвольное поле из q элементов ("+" и "." — сложение и умножение в $\mathbb{F}_q$). Для натурального $k \geq 3$ определим множество

функций из $\mathcal{F}_{k,1,q}$ вида:

$$C_{k,1,q} = \{f \in \mathcal{F}_{k,1,q} : f(x_1, \dots, x_k) = x_1 + f'(x_2, \dots, x_{k-1}) + x_k, f' \in \mathcal{F}_{k-2,1,q}\}.$$

Очевидно, что $\#C_{k,1,q} = q^{q^{k-2}}$. Пусть функция g из $\mathcal{F}_{l,1,q}$ ($l \geq 3$) существенно зависит от всех своих переменных, совершенно уравновешена и не является перестановочной по крайним переменным. Определим множество функций из $\mathcal{F}_{k+l-1,1,q}$ с помощью операции "сдвиг — композиция":

$$\mathcal{D}_{k+l-1,1,q}(g) = \{f \triangleleft g : f \in C_{k,1,q}\}.$$

Легко видеть, что функции из $\mathcal{D}_{k+l-1,1,q}(g)$ существенно зависят от крайних переменных $\{x_1, x_{k+l-1}\}$ и не являются по ним перестановочными. Так как g — совершенно уравновешенная функция, то в случае $f_1 \neq f_2$ ($f_1, f_2 \in C_{k,1,q}$) имеем $f_1 \triangleleft g \neq f_2 \triangleleft g$. Тогда $\#\mathcal{D}_{k+l-1,1,q}(g) = q^{q^{k-2}}$. Для синтеза функции g могут быть использованы конструкции, использованные в примерах 24.7, 24.8, 24.9.

Пример 24.11. Пусть $A = \mathbb{F}_q$ — произвольное конечное поле из q элементов ("+" и "." — сложение и умножение в $\mathbb{F}_q$). Пусть $\text{char}\mathbb{F}_q > 2, k \geq 2$ и множество совершенно уравновешенных функций из $\mathcal{F}_{k+1,1,q}$ имеет вид:

$$\mathcal{Q}_{k+1,1,q} = \left\{ f(x_1, \dots, x_{k+1}) = x_1^2 + \sum_{2 \leq i \leq j \leq k} a_{ij} x_i x_j + x_{k+1} : a_{ij} \in \mathbb{F}_q \right\}.$$

Пусть функция g из $\mathcal{F}_{l,1,q}$ ($l \geq 3$) существенно зависит от всех переменных, совершенно уравновешена и не является перестановочной по крайним переменным, а функция $g(x_1, \dots, x_l) \cdot g(x_1, \dots, x_l)$ не является перестановочной по первой переменной. Определим множество функций из $\mathcal{F}_{k+l,1,q}$ с помощью операции "сдвиг-композиция":

$$\mathcal{E}_{k+l,1,q}(g) = \{f \triangleleft g : f \in \mathcal{Q}_{k+1,1,q}\}.$$

Непосредственно проверяется, что функции из $\mathcal{E}_{k+l,1,q}(g)$ существенно зависят от крайних переменных $\{x_1, x_{k+l}\}$ и не являются по ним перестановочными. Очевидно (как и в примере 24.10), если $f_1 \neq f_2$ ($f_1, f_2 \in \mathcal{Q}_{k+1,1,q}$), то $f_1 \triangleleft g \neq f_2 \triangleleft g$. Тогда

$$\#\mathcal{E}_{k+l,1,q}(g) = q^{\binom{k-1}{2} + k - 1}.$$

Операция "сдвиг-композиция" позволяет использовать разнообразные алгебраические и комбинаторные конструкции для синтеза совершенно уравновешенных функций.

§25 Теоретико-информационная характеристика совершенно уравновешенных функций

В данном параграфе рассматривается и доказывается критерий совершенной уравновешенности (см. §24) дискретных функций над конечным алфавитом, использующий понятия и терминологию теории информации.

Напомним некоторые необходимые нам понятия. Для случайной величины ξ , принимающей значения из S в соответствии с законом распределения $\mathcal{P}$, будем, как и ранее, пользоваться обозначением $\xi \in_{\mathcal{P}} S$. В частности, для равномерного распределения используем символ $\mathcal{U}$.

Энтропия К. Шеннона (далее энтропия, см. [Фано 65]) случайной величины ξ (или распределения $\mathcal{P} = \{\Pr[\xi = x], x \in S\}$) определяется соотношением

$$H(\xi) = - \sum_{x \in S} \Pr[\xi = x] \log_2 \Pr[\xi = x],$$

где всегда полагают $0 \cdot \log_2 0 = 0$. Для пары случайных величин ξ, η , принимающих значения в множествах S и T соответственно, известны ([Фано 65]. [Ash 65]) следующие виды энтропии:

– совместная энтропия:

$$H(\xi, \eta) = - \sum_{x \in S} \sum_{y \in T} \Pr[\xi = x, \eta = y] \log_2 \Pr[\xi = x, \eta = y];$$

– условная энтропия случайной величины η относительно случайной величины ξ :

$$H(\eta | \xi) = - \sum_{x \in S} \sum_{y \in T} \Pr[\xi = x, \eta = y] \log_2 \Pr[\eta = y | \xi = x].$$

Далее нам понадобится величина, называемая средней взаимной информацией случайных величин ξ и η :

$$\begin{aligned} I(\eta | \xi) &= I(\xi | \eta) = H(\xi) + H(\eta) - H(\xi, \eta) = \\ &= H(\xi) - H(\xi | \eta) = H(\eta) - H(\eta | \xi). \end{aligned} \quad (25.1)$$

Средняя взаимная информация характеризует среднее значение информации о случайной величине η , содержащейся в случайной величине ξ (и наоборот).

Пусть $f \in \mathcal{F}_{n,1,q}$ и последовательность случайных величин $\{\xi_m\}_{m=1}^{\infty}$, $\xi_m = (\xi_{m,1}, \xi_{m,2}, \dots, \xi_{m,m+n-1})$ удовлетворяет условию

$$\xi_m \in_{\mathcal{U}} A^{m+n-1}, m = 1, 2, \dots$$

Для каждой ξ_m определим случайную величину

$$\eta_m^f = f_m(\xi_m). \quad (25.2)$$

Справедливо следующее утверждение.

Предложение 25.1. *Для любого натурального числа m случайная величина η_m^f удовлетворяет условию $\eta_m^f \in_{\mathcal{U}} A^m$ тогда и только тогда, когда $f \in \mathcal{F}_{n,1,q}$ — совершенно уравновешенная функция.*

Доказательство. Непосредственно вытекает из определения совершенно уравновешенной функции и соотношения (25.2). $\square$

Для случайных величин ξ_m и η_m^f определим среднюю на знак взаимную информацию как

$$i_m(f) = m^{-1} I(\eta_m^f | \xi_m). \quad (25.3)$$

Теорема 25.2. Пусть $f \in \mathcal{F}_{n,1,q}$, $\xi_m \in_{\mathcal{U}} A^{m+n-1}$ и $\eta_m^f = f_m(\xi_m)$, $m = 1, 2, \dots$. Функция f — совершенно уравновешенная тогда и только тогда, когда для любого натурального m выполнено $i_m(f) = \log_2 q$.

Доказательство. Заметим, что для любых $u \in A^{m+n-1}$ и $v \in A^m$ справедливы следующие соотношения

$$\pi_u = \Pr [\xi_m = u] = q^{-(m+n-1)};$$

$$\pi_{v/u} = \Pr [\eta_m^f = v | \xi_m = u] = \begin{cases} 1 & , \text{ если } u \in f_m^{-1}(v), \\ 0 & , \text{ если } u \notin f_m^{-1}(v); \end{cases}$$

$$\pi_{v,u} = \Pr [\eta_m^f = v, \xi_m = u] = \begin{cases} q^{-(m+n-1)} & , \text{ если } u \in f_m^{-1}(v), \\ 0 & , \text{ если } u \notin f_m^{-1}(v); \end{cases}$$

$$\tilde{\pi}_v = \sum_{u \in A^{m+n-1}} \pi_{v,u} = q^{-(m+n-1)} \cdot \# f_m^{-1}(v).$$

Воспользовавшись этими соотношениями, можно показать справедливость следующей цепочки равенств

$$\begin{aligned}
i_m(f) &= m^{-1} I(\eta_m^f \mid \xi_m) = m^{-1} [H(\eta_m^f) - H(\eta_m^f \mid \xi_m)] = \\
&= m^{-1} \sum_{v \in A^m} \sum_{u \in f_m^{-1}(v)} \pi_{v,u} [\log_2 \pi_{v/u} - \log_2 \tilde{\pi}_v] = \\
&= m^{-1} \sum_{v \in A^m} \sum_{u \in f_m^{-1}(v)} q^{-(m+n-1)} [(m+n-1)\log_2 q - \log_2 (\#f_m^{-1}(v))] = \\
&= m^{-1} \sum_{v \in A^m} (\#f_m^{-1}(v)) q^{-(m+n-1)} [(m+n-1)\log_2 q - \log_2 (\#f_m^{-1}(v))] = \\
&= m^{-1} \left[(m+n-1)\log_2 q - q^{-(m+n-1)} \sum_{v \in A^m} (\#f_m^{-1}(v)) \log_2 (\#f_m^{-1}(v)) \right].
\end{aligned} \tag{25.4}$$

Пусть f — совершенно уравновешенная функция из $\mathcal{F}_{n,1,q}$. Тогда для любого натурального числа m и любого набора $v \in A^m$ справедливо равенство

$$\#f_m^{-1}(v) = q^{n-1}. \tag{25.5}$$

Воспользовавшись соотношениями (25.4) и (25.5) для произвольного m получаем $i_m(f) = \log_2 q$.

Докажем теперь обратное утверждение. Пусть $f \in \mathcal{F}_{n,1,q}$ и для любого натурального числа m выполняется равенство $i_m(f) = \log_2 q$. Тогда из соотношения (25.4) следует, что

$$- \sum_{v \in A^m} \frac{\#f_m^{-1}(v)}{q^{m+n-1}} \log_2 \left(\frac{\#f_m^{-1}(v)}{q^{m+n-1}} \right) = m \log_2 q. \tag{25.6}$$

Кроме того,

$$\sum_{v \in A^m} \frac{\#f_m^{-1}(v)}{q^{m+n-1}} = 1.$$

Следовательно, энтропия распределения $\mathcal{P} = \left\{ \frac{\#f_m^{-1}(v)}{q^{m+n-1}}, v \in A^m \right\}$ имеет максимальное значение. Это возможно (см. [Ash 65]) лишь в случае, когда

$$\frac{\#f_m^{-1}(v)}{q^{m+n-1}} = q^m \quad (25.7)$$

для любого $v \in A$, т.е. $\#f_m^{-1}(v) = q^{n-1}$. Поскольку в наших рассуждениях m — произвольное, то функция f — совершенно уравновешенная, $\square$

Следствие 25.3. *Если функция $f \in \mathcal{F}_{n,1,q}$ не является совершенно уравновешенной, то существует такое натуральное число m_0 , что $i_{m_0}(f) < \log_2 q$.*

Доказательство. Непосредственно вытекает из определения совершенно уравновешенной функции и утверждения теоремы (25.2). $\square$

Полученный результат характеризует процессы обработки информации, осуществляемые неавтономными регистрами сдвига с фильтрующими функциями (см. приложение А, рис. А.4). Средняя на знак взаимная информация $I_m(f)$ характеризует пропускную способность дискретного канала связи, моделируемого неавтономным регистром сдвига с фильтрующей функцией $f \in \mathcal{F}_{n,1,q}$. Утверждение теоремы 25.2 свидетельствует о том, что совершенно уравновешенные функции обеспечивают максимально возможную пропускную способность этого канала передачи информации. В данном случае естественно ожидать в рамках теоретико-сложностного подхода существования эффективных алгоритмов восстановления информации (обращения каналов связи). Приведем один из возможных полиномиальных (по входу) алгоритмов обращения совершенно уравновешенных функций.

Пусть f — произвольная функция из $\mathcal{F}_{n,1,q}$ и $F(f) = \{f_m \in \mathcal{F}_{n,m,q}, m \in \mathbb{N}\}$ — счетное семейство функций, порожденное f . Задачу обращения функций из семейства $F(f)$ можно сформулировать следующим образом: для произвольного натурального m по известному набору $y = (y_1, y_2, \dots, y_m)$ из $f_m(A^{m+n-1})$

найти по крайней мере один набор $x = (x_1, x_2, \dots, x_{m+n-1})$ из $f_m^{-1}(y)$. Рассмотрим следующий алгоритм решения этой задачи.

Алгоритм $\mathfrak{A}_f$ обращения функций из семейства $F(f)$.

Пусть $m \in \mathbb{N}$, $y = (y_1, y_2, \dots, y_m) \in f(A^{m+n-1})$. Строим последовательно m наборов из q непересекающихся подмножеств A^n :

$$(S_1(1), S_1(2), \dots, S_1(q)),$$

$$(S_2(1), S_2(2), \dots, S_2(q)),$$

...

$$(S_m(1), S_m(2), \dots, S_m(q));$$

если $i = 1$, то

$$S_1(1) = \{(u_1, \dots, u_{n-1}, a_1) \in A^n : f(u_1, \dots, u_{n-1}, a_1) = y_1\},$$

$\vdots$

$$S_1(q) = \{(u_1, \dots, u_{n-1}, a_q) \in A^n : f(u_1, \dots, u_{n-1}, a_q) = y_1\},$$

$$S_1 = \bigcup_{j=1}^q S_1(j) \neq \emptyset;$$

если набор подмножеств $(S_{i-1}(1), \dots, S_{i-1}(q))$, $1 < i \leq m$, построен, то

$$S_i(1) = \{(v_2, \dots, v_n, a_1) : \exists v = (v_1, v_2, \dots, v_n) \in S_{i-1}, f(v_2, \dots, v_n, a_1) = y_i\},$$

$\vdots$

$$S_i(q) = \{(v_2, \dots, v_n, a_q) : \exists v = (v_1, v_2, \dots, v_n) \in S_{i-1}, f(v_2, \dots, v_n, a_q) = y_i\},$$

$$S_i = \bigcup_{j=1}^q S_i(j) \neq \emptyset, i = 2, 3, \dots, m;$$

вычисление набора $x \in f_m^{-1}(y)$: для y_m , поскольку $S_m \neq \emptyset$, существует

$$(x_m, x_{m+1}, \dots, x_{m+n-1}) \in S_m,$$

такой, что $f(x_m, x_{m+1}, \dots, x_{m+n-1}) = y_m$; для y_{m-1} , поскольку $S_{m-1} \neq \emptyset$, существует

$$(x_{m-1}, x_m, \dots, x_{m+n-2}) \in S_{m-1},$$

такой, что $f(x_{m-1}, x_m, \dots, x_{m+n-2}) = y_{m-1}$ и т. д. для $i = m-2, m-3, \dots, 1$; полученные в результате m наборов

$$(x_m, x_{m+1}, \dots, x_{m+n-1}),$$

$$(x_{m-1}, x_m, \dots, x_{m+n-2}),$$

...

$$(x_1, x_2, \dots, x_n)$$

определяют набор $x = (x_1, x_2, \dots, x_{m+n-1}) \in A^{m+n-1}$ такой, что $f_m(x) = y$.

Остановимся подробнее на некоторых параметрах описанного выше алгоритма. Основными операциями, используемыми в ходе реализации алгоритма $\mathfrak{A}_f$, являются следующие:

1. запись в память (считывание из памяти) n -наборов в алфавите A ;
2. переход от набора $(v_1, v_2, \dots, v_n)$ к набору $(v_2, \dots, v_n, a)$,
 $v_1, v_2, \dots, v_n, a \in A$;
3. проверка выполнения соотношения $f(v_2, \dots, v_n, a) = b$, $v_2, \dots, v_n, a, b \in A$;
4. сравнение содержимого двух ячеек памяти.

Будем называть их единичными операциями (ед. оп.). Используемую память будем представлять в виде массивов ячеек памяти, необходимых для хранения n -наборов в алфавите A , т.е. способных хранить $n \log_2 q$ бит информации.

Обозначим через $T_f : \mathbb{N} \rightarrow \mathbb{N}$ и $M_f : \mathbb{N} \rightarrow \mathbb{N}$ — трудоемкость алгоритма $\mathfrak{A}_f$ и память, необходимую для его реализации соответственно.

Из описания алгоритма $\mathfrak{A}_f$ легко видеть, что

$$T_f \leq C_1(n, q) \cdot t \text{ ед. оп.}, \quad (25.8)$$

$$M_f \leq C_2(n, q) \cdot t \text{ бит.} \quad (25.9)$$

Очевидно, что алгоритм $\mathfrak{A}_f$ является детерминированным полиномиальным (по t) и улучшить асимптотическую оценку (25.8) не представляется возможным. Действительно, в ходе реализации данного алгоритма обращения функций из $F(f)$ необходимо будет по крайней мере просмотреть набор $y = (y_1, y_2, \dots, y_m)$. Нетрудно заметить, что $C_1(n, q) \leq (5q^n + 1)$ и $C_2(n, q) \leq q^n \cdot n \cdot \log_2 q$.

В случае, если f является совершенно уравновешенной, из утверждения теоремы 25.2 следует, что набор $y = f_m(x)$ содержит в среднем максимально возможное количество информации о наборе x . Естественнo ожидать, что для совершенно уравновешенных функций величины $C_1(n, q)$ и $C_2(n, q)$ могут быть значительно меньшими. Например, воспользовавшись эквивалентностью свойства функций быть без потери информации (см. §24) свойству совершенной уравновешенности несложно получить оценки

$$C_1(n, q) \leq (5q^{n-1} + 1), \quad C_2(n, q) \leq q^{n-1} \cdot n \cdot \log_2 q.$$

Описание алгоритма $\mathfrak{A}_f$ может быть перенесено на теоретико-автоматную модель с соответствующей заменой некоторых единичных операций на операции, соответствующие функциям переходов и выходов конечного автомата. Таким образом, для любой ограниченно-детерминированной функции (см. [КАП 85]) существует детерминированный полиномиальный алгоритм обращения.

Заключение

В диссертации поставлена и решается задача совершенствования математических моделей и повышение на основе полученных результатов эффективности методов анализа сложности обращения дискретных функций, используемых при синтезе средств обеспечения информационной безопасности. Решение этой задачи существенным образом влияет как на уровень обоснованности оценок информационной безопасности в конкретных информационно-телекоммуникационных системах, так и на развитие принципов создания перспективных средств защиты информации.

Основные результаты диссертации состоят в следующем.

1. Для множества комплекснозначных функций на конечной абелевой группе предложен и развит математический аппарат, обобщающий понятие "алгебраической степени нелинейности" и другие параметры классических колец полиномов. На основе использованного подхода к координатизации для групповых комплекснозначных функций получен ряд их свойств, аналогичных свойствам классических кодов Рида-Маллера. Предложены новые виды координатизации и описания алгебраических и комбинаторных свойств для конечных модулей.

2. Для произвольной конечной абелевой группы введено новое понятие комплекснозначной бент-функции, обобщающее понятие бент-функции на элементарной абелевой p -группе. Доказаны аналогии основных свойств бент-функций для рассмотренного обобщения, а также описан ряд его новых свойств.

Эти результаты являются перспективными в теоретическом плане, как основа дальнейшего обобщения и координатизации метаматического понятия "бент-функция". С практической точки зрения они расширяют возможности синтеза новых классов дискретных функций, используемых для обеспечения информационной безопасности.

3. Рассмотрено новое понятие циклотомически приведенного полинома над конечным полем. Используя данное понятие, удалось уточнить оценку Вейля для сумм аддитивных характеров конечного поля. С теоретической точки зрения данные результаты позволяют сформулировать новые необходимые условия для достижимости оценки Вейля. С практической точки зрения они позволяют скорректировать в ходе анализа средств обеспечения информационной безопасности значения параметров (или оценки параметров) дискретных функций, вычисляемых с использованием сумм аддитивных характеров конечных полей.

4. Для произвольной функции $f : G \rightarrow H$ (G, H — конечные абелевы группы) предложено и изучено представление, обобщающее аффинное расщепление булевых функций. На основе параметров этого представления введена характеристика "нелинейности" исходной групповой функции. Получен ряд соотношений и неравенств, связывающих эту характеристику "нелинейности" с основными параметрами групповой функции.

Проведенная координатизация и выделенные новые параметры групповой функции позволяют, например, исследовать криптографические свойства таких функций с помощью алгебраических методов (метод линеаризации) или корреляционных методов (линейный или дифференциальный методы). Кроме того, исследованное представление позволяет синтезировать групповые функции с определенными, заранее заданными параметрами.

5. Введено понятие невырожденной булевой функции f , как функции с тривиальным пространством $L_f^{\deg(f)-2}$. Невырожденная булева функция характеризуется тем, что при действии на нее дифференциального оператора она имеет наименьшие признаки "алгебраического" вырождения. Доказано, что любая булева функция RM-эквивалентна некоторой невырожденной форме.

Для Фурье-кластеризации булевых функций описаны новые классы пустых секций, соответствующие функциям, обладающим нетривиальными пространствами линейных трансляторов. Получены новые соотношения, связыва-

ющие взаимную глобальную лавинную характеристику пары булевых функций с глобальными лавинными характеристиками каждой из них.

6. Предложен универсальный подход к изучению вопросов наследования комбинаторных и спектральных свойств при сужении булевых функций на плоскостях на основе $(H, 0^n)$ -стабильности. Получен ряд соотношений, связывающих комбинаторные, спектральные, криптографические параметры булевой функции с параметрами $(H, 0^n)$ -стабильности этой функции. Эти соотношения могут способствовать эффективному вычислению характеристик, являющихся существенными при проведении анализа криптографических дискретных функций.

На основе свойства $(H, 0^n)$ -стабильности булевой функции получена новая характеристика хорошо известного класса корреляционно-иммунных булевых функций.

7. С целью развития аппарата анализа булевых функций и отображений рассмотрена концепция локальных аффинностей булевых функций при сужении их на плоскости в пространстве Хэмминга. Введены параметры, характеризующие структуру семейства локальных аффинностей булевой функции. Доказаны соотношения, показывающие влияние этих параметров на различные свойства булевых функций.

Исследован параметр "уровень аффинности" булевой функции, описывающий максимальную размерность локальной аффинности функции при сужении ее на плоскости, описываемые фиксацией переменных функции. В частности показано, что асимптотически при $n \rightarrow \infty$ для почти всех булевых функций от n переменных уровень аффинности принимает одно или два значения (в зависимости от примарности числа n). Представители указанного семейства плоскостей в качестве локальных аффинностей играют чрезвычайно важную роль в комбинаторных алгоритмах обращения дискретных функций, содержащих этапы перебора части описывающих функцию параметров.

Предложена новая нормальная форма булевой функции на основе понятия локальной аффинности — аффинная нормальная форма булевой функции

(АффНФ). Получен ряд соотношений, выявляющих влияние АффНФ булевой функции на ее комбинаторные и спектральные параметры. Строение и особенности этой нормальной формы определяют перспективность ее использования при разработке алгоритмов и методов обращения дискретных функций, основанных на аффинной аппроксимации уравнений.

8. Рассмотрена и исследована теоретико-автоматная модель частичного обращения ограниченно-детерминированных функций. Получены новые соотношения, показывающие влияние особенностей функции (конечного автомата) на параметры частичного обращения. Данные результаты могут быть полезны при разработке теоретико-автоматных методов криптоанализа, а также при анализе теоретико-автоматных моделей скрытых каналов.

9. Для автоматов Мили без потери информации рассмотрена и изучена модель локального обращения. Доказан критерий, показывающий, что наличие свойства, локального для такого автомата, связано со свойством синхронизируемости у ассоциированного с ним автомата без выхода. Описаны новые классы двоичных регистров сдвига с фильтрующими булевыми функциями, обладающие свойством локальной обратимости. Данные результаты могут быть использованы при разработке теоретико-автоматных методов обращения дискретных функций.

10. Предложен эффективный метод синтеза совершенно уравновешенных дискретных функций на основе операции "сдвиг-композиция". Доказан критерий совершенной уравновешенности "сдвиг-композиции" пары дискретных функций.

С использованием теоретико-информационного понятия "средняя взаимная информация" пары случайных величин получена новая характеристика класса совершенно уравновешенных функций.

11. Исследованы метрические параметры "нелинейной" аппроксимации булевых функций с помощью биортогональных базисов, построенных на основе бент-функций. Показано, что потенциальные возможности (точность) "нелиней-

ной" аппроксимации не меньше, чем у "линейной (аффинной)" аппроксимации. Найден радиус покрытия для класса обобщенных кодов Адамара, построенных с помощью бент-функций.

12. В целом результаты диссертации можно квалифицировать как новое крупное научное достижение в области развития математических моделей и совершенствования методов решения задач обращения дискретных функций, используемых при синтезе средств информационной безопасности. Развитие математических моделей, новые виды координатизации и углубленные исследования взаимосвязей параметров дискретных функций способствуют совершенствованию методов обращения дискретных функций и повышению уровня обоснованности оценок информационной безопасности.

Список литературы

- [Амб 94] Амбросимов А.С. Свойства бент-функций q -значной логики над конечными полями. // Дискр. математика., том 6, вып. 3, 1994, с. 50-60.
- [АЗКЧ 01] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Москва, Гелиос АРВ, 2001, с. 480.
- [Бел 76] Беллман Р. Введение в теорию матриц. Наука, Москва, 1976.
- [Бирк 84] Биркгоф И. Теория решеток. М.: Наука, 1984, с. 568.
- [Буг 15] Бугров А.Д. Кусочно-аффинные подстановки конечных полей. // Прикл. дискретн. математика, №4 (30), 2015, с. 5-23.
- [БуЛо 05,1] Буряков М.Л., Логачев О.А. О распределении уровня аффинности на множестве булевых функций. // Математика и безопасность информационных технологий. М.: МЦНМО, 2005, с. 141-146.
- [БуЛо 05,2] Буряков М.Л., Логачев О.А. Об уровне аффинности булевых функций. // Дискр. математика, том 17, вып.4, 2005, с. 98-107.
- [Бур 08] Буряков М.Л. Асимптотические оценки уровня аффинности для почти всех булевых функций. // Дискр. математика, том 20, вып.3, 2008, с. 73-79.
- [Бур 09] Буряков М.Л. Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций. // Дисс. на соиск. уч. ст. канд. физ.-мат. наук, Москва, 2009, с. 114.
- [Вас 03] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО, Москва, 2003, с. 328.
- [ВоКу 84] Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления. Наука, Москва, 1984.

- [Ги 66] Гилл А. Введение в теорию конечных автоматов. Наука, Москва 1966, с. 272.
- [Ги 74] Гилл А. Линейные последовательностные машины. Анализ, синтез и применение. Наука, Москва 1974, с. 287.
- [Глу 10] Глухов М.М. К анализу некоторых систем распределения ключей, основанных на неабелевых группах. // Математические вопросы криптографии, том 1, 2010, с. 9-22.
- [ГКН 08] Григорьев Д.Ю., Кожевников. А., Николенко С.И. Алгебраическая криптография: новые конструкции и их надежность относительно доказуемого взлома. // Алгебра и анализ, том 20, №6, 2008, с. 119-147.
- [ГоТа 09] Горшков С.П., Тарасов А.В. О максимальных группах инвариантных преобразований мультиаффинных, биюнктивных, слабоположительных и слабоотрицательных булевых функций. // Дискрет. математика, том 21, вып. 2, 2009, с. 94-101.
- [ГоТа 17] Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. Курс, Москва, 2017, с. 192.
- [ГэДж 82] Гэри М., Джонсон Д. Вычислительные машины и трудно решаемые задачи. Мир, Москва, 1982, с. 416.
- [ЖуЧи 94] Жуков А.Е., Чистяков В.П. Матричный подход к исследованию прообразов выходных последовательностей конечных автоматов. // Обозрение прикладной и промышленной математики. М: ТВП, том 1, №1, 1994, с. 108-117.
- [ЗиЭр 96] Зиновьев В.А., Эриксон Т. О Фурье-инвариантных разбиениях конечных абелевых групп и тождестве Мак-Вильямс для групповых кодов. // Пробл. передачи информации, том 32, вып. 1, 1996, с. 137-143.

- [КАП 85] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. Наука, Москва 1985, с. 316.
- [КеС 70] Кемени Дж., Снелл Дж. Конечные цепи Маркова. Наука, Москва 1970, с. 271.
- [Кло 88] Клосс Б.Б. Некоторые свойства помехоустойчивых автоматов. // Кибернетика, №1, 1988, Киев, Наукова думка, с.10-15.
- [КМН 08] Кузьмин А.С., Марков В.Т., Нечаев А.А. и др. Бент-функции и гипербент-функции над полем из 2^l элементов. // Проблемы передачи информации, том 44, №1, 2008, с. 15-37.
- [Коло14] Коломеец Н.А. Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных. // Прикл. дискретн. математика, №3, 2014, с. 28-39.
- [Кур 72] Курмит А.А. Автоматы без потери информации конечного порядка. Зинатне, Рига 1972, с. 264.
- [Лал 85] Лаллеман Ж. Полугруппы и комбинаторные приложения. Мир, Москва 1985, с. 440.
- [Лам 71] Ламбек И. Кольца и модули. М.: Мир, 1971, с. 279.
- [ЛиНи 88] Лидл Р., Нидерайтер Г. Конечные поля, т. 1,2, Мир, Москва, 1988.
- [Лог 07] Логачев О.А. О локальной обратимости одного класса булевых отображений. // Материалы 9 Международного семинара «Дискретная математика и ее приложения». Москва, 18 -23 июня 2007г. Изд. Мех. - мат. факультета МГУ, Москва, 2007, с. 440 - 442.
- [Лог 08] Логачев О.А. Нижняя оценка уровня аффинности для почти всех булевых функций. // Дискр. математика, том 20, вып.4, 2008, с. 85-88.

- [Лог 09] Логачев О.А. Об использовании аффинных нормальных форм булевых функций для определения ключей фильтрующих генераторов. // Математика и безопасность информационных технологий. М. МЦНМО, 2009, с. 101-110.
- [Лог 10] Логачев О.А. О значениях уровня аффинности для почти всех булевых функций. // Прикл. дискр. математика, №3, 2010, с. 17-21
- [Лог 17] Логачев О.А. Критерий совершенной уравновешенности сдвиг-композиции функций над конечным алфавитом. // Дискретн. математика, том 29, вып. 4, 2017, с. 59-65.
- [Лог 18,1] Логачев О.А. О локальной обратимости конечных автоматов без потери информации. // Прикл. дискр. математика, №39, 2018, с. 78-93.
- [Лог 18,2] Логачев О.А. Теоретико-информационная характеристика совершенно уравновешенных функций. // Информатика и ее применение, том 12, вып. 4, 2018, с. 70-74.
- [ЛоНа 07] Логачев О.А., Назарова Д.С. Локальное аффинное обращение.// Математика и безопасность информационных технологий. М.: МЦНМО, 2007, с. 227-248.
- [ЛПЯ 95] Логачев О.А., Проскурин Г.В., Яценко В.В. Локальное обращение конечного автомата с помощью автоматов. // Дискр. математика, том 7, вып. 2, 1995, с. 19-33.
- [ЛоСм 13] Логачев О.А., Смышляев С.В. О неавтономных регистрах сдвига, обладающих свойством синхронизации. // Электроника инфо, №6, 2013, с. 183-185.

- [ЛССЯ 15] Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. Булевы функции в теории кодирования и криптологии. М.: Ленанд, 2015, с. 576.
- [ЛСФ 19.1] Логачев О.А., Сукаев А.А., Федоров С.Н. Об одном методе решения систем квадратичных булевых уравнений, использующем локальные аффинности булевых функций. // Информатика и ее применения, т. 13, вып. 2, 2019, с. 56-65.
- [ЛСФ 19.2] Логачев О.А., Сукаев А.А., Федоров С.Н. Полиномиальные алгоритмы вычисления локальных аффинностей квадратичных булевых функций. // Информатика и ее применения, т. 13, вып. 1, 2019, с. 67-74.
- [ЛСЯ 97] Логачев О.А., Сальников А.А., Яценко В.В. Бент-функции на конечной абелевой группе. // Дискр. математика, том 9, вып. 4, 1997, с. 3-20.
- [ЛСЯ 98] Логачев О.А., Сальников А.А., Яценко В.В. Спаривание конечных модулей, дуальность линейных кодов и тождества Мак-Вильямс. // Пробл. передачи информации, том 34, вып. 3, 1998, с. 50-59.
- [ЛСЯ 99] Логачев О.А., Сальников А.А., Яценко В.В. О свойствах сумм Вейля на конечных полях и конечных абелевых группах. // Дискр. математика, том 11, вып. 2, 1999, с. 66-85.
- [ЛСЯ 00,1] Логачев О.А., Сальников А.А., Яценко В.В. Невырожденная нормальная форма булевых функций. // Докл. РАН, том 373, № 2, 2000, с. 164-167.
- [ЛСЯ 00,2] Логачев О.А., Сальников А.А., Яценко В.В. Об одном свойстве ассоциированных представлений группы $GL(n,k)$. // Дискретн. математика, том 12, вып. 2, 2000, с. 154-159.

- [ЛСЯ 01] Логачев О.А., Сальников А.А., Яценко В.В. Некоторые характеристики «нелинейности» групповых отображений. // Дискр. анализ и иссл. операций, серия 1, том 8, № 1, 2001, с. 40-54.
- [ЛСЯ 02] Логачев О.А., Сальников А.А., Яценко В.В. О наследовании свойств при сужениях булевых функций. // Дискретн. математика, том 14, вып. 2, 2002, с. 9-19.
- [ЛСЯ 04,1] Логачев О.А., Сальников А.А., Яценко В.В. Комбинирующие k-аффинные функции. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, с. 176-178.
- [ЛСЯ 04,2] Логачев О.А., Сальников А.А., Яценко В.В. Аппроксимация булевых функций элементами биортогонального базиса. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, с. 171-175.
- [ЛСЯ 04,3] Логачев О.А., Сальников А.А., Яценко В.В. Корреляционная иммунность и реальная секретность. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, с. 165-170.
- [ЛСмЯ 10] Логачев О.А., Смышляев С.В., Яценко В.В. Новые методы изучения совершенно уравновешенных булевых функций. // Дискр. математика, том 21, вып. 2, 2009, с. 51-74.
- [ЛФЯ 18,1] Логачев О.А., Федоров С.Н., Яценко В.В. Булевы функции как точки на гиперсфере в евклидовом пространстве. // Дискр. математика, ...
- [ЛФЯ 18,2] Логачев О.А., Федоров С.Н., Яценко В.В. О Δ -эквивалентности булевых функций. // Дискретн. математика, том 30, вып. 4, с. ...

- [ЛЯ 98] Логачев О.А., Ященко В.В. Коды типа Рида-Маллера на конечной абелевой группе. // Проблемы передачи информации, том 34, вып. 2. 1998, с. 32-46.
- [Мал 86] Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Наука, 1986, с. 368.
- [Мал 70] Мальцев А.И. Алгебраические системы. М.: Наука, 1970, с. 392.
- [МаМи 72] Маркус М., Минк Х. Обзор по теории матриц и матричных неравенств. Наука, Москва, 1972.
- [Мел 11] Мелузов А.С. Построение эффективных алгоритмов решения систем полиномиальных булевых уравнений методом опробования части переменных. // Дискр. математика, том 23, вып. 4, 2011, с. 51-74.
- [МРРСШ 90] Мельников О.В., Ремесленников В.Н., Романьков В.А., Скорняков Л.А., Шестаков И.П. Общая алгебра, том 1, Наука, Москва 1990, с. 501.
- [МРРСШ 90] Мельников О.В., Ремесленников В.Н., Романьков В.А., Скорняков Л.А., Шестаков И.П. Общая алгебра. Том 2. Наука, Москва 1991, с. 479.
- [Мхлв 94, 1] Михайлов В.Г. О числе прообразов выходной последовательности автомата. // Обзорение прикладной и промышленной математики. М: ТВП, том 1, №1, 1994, с. 118-121.
- [Мхлв 94, 2] Михайлов В.Г. Обобщение теоремы о числе прообразов выходной последовательности автомата. // Обзорение прикладной и промышленной математики. М: ТВП, том 1, №1, 1994, с. 122-125.

- [Мхлв 94, 3] Михайлов В.Г. Асимптотическая нормальность числа прообразов выходной последовательности автомата. // Обозрение прикладной и промышленной математики. М: ТВП, том 1, №1, 1994, с.126-135.
- [МхЧ 94] Михайлов В.Г., Чистяков В.П. О задачах теории конечных автоматов, связанных с числом прообразов выходной последовательности. // Обозрение прикладной и промышленной математики. М: ТВП, том 1, №1, 1994, с. 7-31.
- [Неч 95] Нечаев А.А. Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам. // Фундаментальная и прикладная математика. Том 1, №1, 1995, с. 229-254.
- [Ром 13] Романьков В.А. Алгебраическая криптография. Изд-во Омского Гос. Ун-та, Омск, 2013, с. 136.
- [Рос 07] Росошек С.К. Криптосистемы в группах автоморфизмов групповых колец абелевых групп. // Фундамент. и прикл. математика, том 13, вып. 3, 2007, с. 157-164.
- [Рыс 94] Рысцов И.К. Возвратные слова для разрешимых автоматов. // Кибернетика и системный анализ, № 6, 1994, с. 21-26.
- [Рыс 00] Рысцов И.К. О длине возвратных слов для автоматов с простыми идемпотентами. // Кибернетика и системный анализ, том 3, 1995, с. 32-39.
- [Сид 65] Сидельников В.М. О статистических свойствах преобразований, осуществляемых конечными автоматами. // Кибернетика, №6, 1965, с. 18-23.
- [Сид 08] Сидельников В.М. Теория кодирования. М.: Физматлит, 2008, с. 324.
- [Сол 02] Солодовников В.И. Бент-функции из конечной абелевой группы в конечную абелеву группу. // Дискретн. математика, том 14, вып. 1, 2002, с. 99-113.

- [Сол 07] Солодовников В.И. Гомоморфизмы регистров сдвига в линейные автоматы. // Труды по дискретной математике, том 10, 2007, с. 287-300.
- [Сол 16] Солодовников В.И. Три подхода к понятию функций, максимально отличающихся от гомоморфизмов. // Матем. вопр. криптографии, том 7, №3, 2016, с. 115-136.
- [Спе 71] Сперанский Д.В. Автоматы существенно без потери информации. // Автоматика и телемеханика, №10, 1971, с. 181-184.
- [Спе 72,1] Сперанский Д.В. Об автоматах существенно без потери информации конечного порядка. // Автоматика и телемеханика, №6, 1972, с. 90-95.
- [Спе 72,2] Сперанский Д.В. Об автоматах без потери информации. // Изв. АН СССР, №6, 1972, с. 109-113.
- [Степ 91] Степанов С.А. Арифметика алгебраических кривых. Наука, Москва, 1991. с. 109-113.
- [Сум 94] Сумароков С.Н. Запреты двоичных функций и обратимость одного класса кодирующих устройств. // Обзорение прикладной и промышленной математики, 1994, № 1, с. 35-55.
- [Тар 02] Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях. Матем. вопросы кибернетики, 11, 2002, с. 91-148.
- [ТраБ 70] Трахтенброт Б.А., Барздинь Я.М. Конечные автоматы(поведение и синтез). Наука, Москва 1970, с. 400.
- [Фано 65] Фано Р. Передача информации. Статистическая теория связи. Мир, Москва 1965.
- [Холл 62] Холл М. Теория групп. ИЛ, Москва, 1962, с. 468.

- [Цим 11] Циммерман К.-Х. Методы теории модулярных представлений в алгебраической теории кодирования. МЦНМО, Москва 2011, с. 245.
- [Чаш 97] Чашкин А.В. Об областях, полностью определяющих булевы функции. // Дискр. математика, том. 9, вып. 4, 1997, с. 21-23.
- [Чаш 12] Чашкин А.В. Дискретная математика. М.: Изд. Центр «Академия», 2012, с. 352.
- [Чер 10] Черемушкин А.В. Аддитивный подход к определению степени нелинейности дискретной функции. // Прикл. дискретн. математика, № 2, 2010, с. 22-33.
- [Чер 13] Черемушкин А.В. Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка. // Прикл. дискретн. математика, №2, 2013, с. 26-38.
- [Чер 14] Черемушкин А.В. Вычисление степени нелинейности функции на циклической группе примарного порядка. // Прикл. дискретн. математика, том 24, №2, с. 37 - 47.
- [Шаф 86] Шафаревич И.Р. Основные понятия алгебры. Итоги науки и техники, том 11. Москва, ВИНТИ, 1986, с. 289.
- [Ши 15] Шишков А.Б. О бент-функциях на группе $\mathbb{Z}_{p^n}$. // Математические вопросы криптографии, том 6, вып.4, 2015, с. 127-138.
- [Шна 03] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф, Москва, 2003, с. 816.
- [Ябл 10] Яблонский С.В. Введение в дискретную математику. М.: «Высшая школа», 2010, с. 384.

- [Ящ 97,1] Ященко В.В. Свойства булевых отображений, сводимые к свойствам их координатных функций. // Вестн. МГУ. Сер. Математика, Механика, 1997 . № 4, с. 11-13.
- [Ящ 97,2] Ященко В.В. О критерии распространения для булевых функций и бент-функциях. // Проблемы передачи информации, Том 33, № 1, с. 52-63.
- [Ящ 98] Ященко В.В. О двух характеристиках нелинейности булевых отображений. Дискретный анализ и исследование операций. Серия 1, том 5, № 2, 1998, с. 90-96.
- [Angl 92] Angluin D. Computational learning theory: survey and selected bibliography. Proc. 24th Annu. Symp. on Theory of Computing, 1992, pp. 351-369.
- [Ant 10] Anthony M. Probabilistic Learning and Boolean Functions. In Boolean Models and Methods in Mathematica, Computer Science, and Engineering. Ed. Crama Y. and Hammer P.L., Cambridge University Press, 2010, pp. 197-220.
- [ArBa 09] Arora S., Barak B. Computational Complexity. A Modern Approach. Cambridge University Press, Cambridge 2009, pp.578.
- [Ash 65] Ash R. Information Theory. John Wiley and Sons, Inc., NewYork 1965, pp. 339.
- [Bar 09] Bard G.V. Algebraic Cryptanalysis. Springer 2009, p. 368.
- [Bell 99] Bellare M. Practice-Oriented Provable Security. Lectures on Data Security. (Ed. I.Damgard), LNCS 1561, Springer 1999, pp. 1-15.
- [BGS 94] Bierbrauer J., Gopalakrishnan K., and Stinson D.R. Bounds for Resilient Functions and Orthogonal Arrays.// Proc. Of CRYPTO '94, LNCS 839, pp. 247-256, 1994.

- [BiSh 91,1] Biham E., Shamir A. Differential Cryptanalysis of DES-like cryptosystems. // CRYPTO '90, LNCS vol. 537. Berlin: Springer-Verl., 1991. pp. 2-21.
- [BiSh 91,2] Biham E., Shamir A. Differential Cryptanalysis of DES-like cryptosystems. // Journal of Cryptology, v.4, №1, 1991, pp. 12-23.
- [Br Pr 05] Braeken A. and Preneel B. On the Algebraic Immunity of Symmetric Boolean Functions. // Proc. of INDOCRYPT'05, LNCS 3348, pp. 120-135, 2005.
- [CaCh 03] Canteaut A. and Charpin P. Decomposing Bent Functions. // IEEE Trans. on Inform. Theory, vol.49, no.8, August 2003, pp. 2004-2019.
- [CaVi 05] Canteaut A. and Videau M. Symmetric Boolean Functions. IEEE Trans. On Information Theory 51(8), pp. 2791-2811, 2005.
- [Car 10,1] Carlet C. Boolean Functions for Cryptography and Error-Correcting Codes. In "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, 2010, pp. 257-397.
- [Car 10,2] Carlet C. Vectorial Boolean Functions for Cryptography. In "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, 2010, pp. 398-469.
- [Car 04] Carlet C. On the Degree, Nonlinearity, Algebraic Thickness and Non-normality of Boolean Functions, with Developments on Symmetric Functions. IEEE Trans. On Inform. Theory 50, pp. 2178-2185, 2004.
- [Cer 64] Cerny J. Poznámka k homogenným experimentom s konečnými automatami. Matematicko- fyzikálny Casopis Slovensk. Akad. Vied, 14, no. 3, 1964, pp. 208-216 [in Slovak].

- [CDDL 06] Canteaut A., Daum M., Dobbertin H., Leandr G. Finding Non-normal Bent Functions. // Discrete Applied Mathematics 154, 2006, pp. 202-218.
- [CDPS 10] Carlet C., Danielsen L.E., Parker M.G., Sole P. Self-Dual Bent Functions. // Int. J. Inform. and Coding Theory, 1(4) 2010, pp. 384-399.
- [CHM 04] Clark W.E., Hou X.D. and Mihailovs A. The Affinity of Permutations of a Finite Vector Space. // Tennessee Technological University, Department of Mathematics. Technical Report No.2004-3, July 2004, pp. 25.
- [CJS 00] Chepyzov V., Johansson T., Smeets B. Simple Algorithm for Correlation Attacks on Stream Ciphers. // FSE' 2000, Springer LNCS V. 1978, pp. 181-195.
- [CuSt 09] Cusick Th.W. And Stanica P. Cryptographic Boolean Functions and Applications. AP-Elsevier, San Diego, 2009, pp. 248.
- [DiHe 76] Diffie W. and Hellman M.E. New Directions in Cryptography. // IEEE Trans. on Inform. Theory, v. IT-22, №6, nov. 1976, pp. 644-654.
- [Dot 70] Doty K.L. On Information-lossless on Automata on Finite Order. // IEEE Trans. Electronic Computers. 19, №6, 1970, pp.548-551.
- [Dub 98] Dubuc L. Surles automates circularies eta la conjecture le Cerny. // RAIRO Theor. Inform. and Appl., v.32, 1998, pp.21-34.
- [ECR 04] <http://www.ecrypt.eu.org>
- [Ev 65] Even S. On Information-lossless Automa on Finite Order. // IEEE Trans. Electronic Computers. 4, №4, 1965, pp. 561-569.
- [FeRe 07] Federal Register / Vol. 72, No. 212.

- [FiFo 98] Filiol E. and Fontaine C. Highly Nonlinear Balanced Boolean with a Good Correlation- Immunity. // Proc. of EUROCRYPT'98, LNCS 1403, pp. 475-488, 1998.
- [Fra 82] Frankl P. An external problem for two families of sets. // Eur. J. Comb., v.3, 1982, pp. 125-127.
- [GeP 72] Gecseg F. and Peak I. Algebraic Theory of Automata. Akademiai Kiado, Budapest 1972, pp. 325.
- [Gol 01] Goldreich O. Foundations of Cryptography. Volume 1: Basic Tools. Cambridge University Press. Cambridge 2001, pp. 372.
- [Gol 04] Goldreich O. Foundations of Cryptography. Volume 2: Basic Applications. Cambridge University Press. Cambridge 2004, pp. 426.
- [GoLe 89] Goldreich O. and Levin L.A. A Hard-core Predicate for All One-way Functions. Proc. 21st Annual ACM Symp. on Theory of Computing, 1989, pp. 25-32.
- [GHS 93] Gopalakrishnan K., Hoffman D.G., and Stinson D.R. A Note on a Conjecture Concerning Symmetric Resilient Functions. // Inform. Processing Letters 47(3), pp. 139-143, 1993.
- [Goug 04] Gouget A. On the Propagation Criterion of Boolean Functions. Proc. of the Workshop on Coding, Cryptography and Combinatorics, 2003, pp. 153-168. Birkhauser Verlag, Basel, Switzerland, 2004.
- [Hed 69] Hedlund G.A. Endomorphism and Automorphism of the Shift Dynamical System. // Math. Systems Th. 3 (1969), pp. 320-375.
- [HeRo 63] Hewitt E. and Ross K.A. Abstract Harmonic Analysis. // Volume 1. Springer-Verlag, Berlin-Gottingen-Heidelberg, 1963.

- [Hou 06] Hou X.D. Affinity of Permutations of P_2^n . // Discrete Applied Mathematics 154(2), 2006, pp. 313-325.
- [Huf 59,1] Huffman D.A. Canonical Forms for Information-lossless Finite-state Logical Machines. // IRE Trans. Circuit Theory, 6, 1959, pp. 45-49.
- [Huf 59,2] Huffman D.A. Notes on Information-lossless Finite-state Automata. // Nuovo Cimento, 13, 1959, pp. 89-95.
- [Kar 03] Kari T. Synchronizing finite automata on eulerian digraphs. // Theor. Comput. Sci., v.295, 2003, pp. 223-232.
- [LaVi 08] Lauradoux C. and Videau M. Matriochka Symmetric Boolean Functions. // Proc. of ISIT'08.
- [LiQi 06] Li N. and Qi W. Symmetric Boolean Functions Depending on an Odd Number of Variables with Maximum Algebraic Immunity. // IEEE Trans. On Information Theory 52(5), pp. 2271-2273, 2006.
- [KMY 07] Kavut S., Maitra S., and Yusel M.D. Search for Boolean Functions with Excellent Profiles in the Rotation Symmetric Class. // IEEE Trans. on Inform. Theory 53(5), pp. 1743-1751, 2007.
- [LaRu 69] Laemmel A.E., Rudner B. Study of the Applications of Coding Theory. Report PIBER-69-034, Politechnic Inst. Brooklyn, Dept. Electrophysics, N.Y., pp. 94
- [LiMa 95] Lind D. and Marcus B. Symbolic Dynamics and Coding. Cambridge University Press, 1995, pp. 495.
- [LiuF 07] Liu F. and Feng K. On the 2- variable Symmetric Boolean Functions with Maximum Algebraic Immunity 2 . Proc. of the WCC'07, pp. 225-232, 2007.
- [Log 07] Logachev O.A. "On Perfectly Balanced Boolean Functions <http://eprint.iacr.org/2007/022>.

- [LSSY 09] Logachev O.A., Salnikov A.A., Smyshlyaev S.V., and Yashchenko V.V. Symbolic Dynamics, Codes and Perfectly Balanced Functions. // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, B. Prenel et al (Eds). NATO Advanced Research Workshop, Veliko Tarnovo, Bulgaria, 6-9 October, 2008. IOS Pressm 2009, pp. 222-233.
- [LYD 08] Logachev O.A., Yashchenko V.V., Denisenko M.P. Local Affinity of Boolean Mappings. // Boolean Functions in Cryptology and Information Security, B. Prenel and O.A. Logachev (Eds). NATO Advanced Study Institute, Zvenigorod, Russia, 8-18 September, 2007. IOS Press, 2008, pp. 148-172.
- [MaSa 02] Maitra S. and Sarkar P. Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables. // IEEE Trans. On Information Theory 48, pp. 2626-2630, 2002.
- [MeOV 96] Menezes A., van Oorschot P., and Vanstone S. Handbook of Applied Cryptography. CRC Press. 1996, pp. 810.
- [Mit 90] Mitchell C.J. Enumerating Boolean Functions of Cryptographic Signifians. // Journal of Cryptology 2(3), pp. 155-170, 1990.
- [MWS 77] MacWilliams F.J. and Sloane N.J.A. The theory of Error-Correcting Codes. Parts 1,2. North-Holland Publishing Company, Amsterdam, New-York, Oxford, 1977.
- [MZK 95] Moreno O., Zinoviev V.A., Kumar P.V. An extension of the Weil-Carlitz-Uchiyama bound. Finite Fields and their Appl. (1995)1, №3, p. 360-371.
- [MyShU 08] Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. Advanced courses in Math. CRM, Barselona. Basel-Berlin-New York: Birkhauser Verlag, 2008, p. 183.

- [MyShU 11] Myasnikov A., Shpilrain V., Ushakov A. Non-commutative cryptography and complexity of group-theoretic problems. // Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc., 2011, p. 385.
- [NIST 97] http://csrc.nist.gov/archiv/aes/pre-round1/aes_9701.txt
- [Pin 83] Pin T. On two combinatorial problems arising from automata theory. // Ann. Discrete Math., v.17, 1983, pp. 535-548.
- [Poin 13] Poinot L. Harmonic Analysis and a Bentness-Like Notion in Certain Finite Abelian Groups Over Some Finite Fields. // arXiv:1304.1731v2, 21 Apr. 2013, pp. 23.
- [Poin 12] Poinot L. Non Abelian Bent Functions. // Cryptography and Communications, 4(1), 2012, pp. 1-23.
- [Pre 66] Preparata F.P. Convolutional Transformations of Binary Sequences: Boolean Functions and Their Resynchronizing Properties. // IEEE Trans. Electronic Computers.15, №6, 1966, pp. 561-569.
- [QLF 07] Qu L., Li C., and Feng K. A Note on Symmetric Boolean Functions with Maximum Algebraic Immunity in Odd Number of Variables. // IEEE Trans. on Inform. Theory53, pp. 2908-2910, 2007.
- [Rog 67] Rogers H. Theory of Recursive Functions and Effective Computability. McGraw-Hill Book Company, New York-London-Sydney, 1967.
- [Rot 76] Rothaus O.S. On "Bent" Functions. // Journal of Combinatorial Theory (A), v. 20, № 3, 1976, pp. 300-305.
- [Rys 95] Rystsov I.K. Quasioptimal bound for the length of reset words for regular automata. // Acta Cybernetica, v.12, 1995, pp. 145-152.

- [SaMa 07] Sarkar P. and Maitra S. Balancedness and Correlation Immunity of Symmetric Boolean Functions. // Discrete Mathematics 307, pp. 2351-2358, 2007.
- [Ser 67] Serre J.-P. Representations Lineaires des Groupes Finis. Collection Methodes, Hermann, Paris, 1967.
- [Sho 08] Shoup V. A Computational Introduction to Number Theory and Algebra, Cambridge University Press 2008, p. 580.
- [Sieg 84] Siegenthaler T. Correlation-immunity of Nonlinear Combining Functions for Cryptographic Applications. // IEEE Trans. on Information Theory. V/ IT-30, no. 5, 1984, pp. 776-780.
- [Sieg 85] Siegenthaler T. Decrypting a Class of Stream Ciphers Using Ciphertext Only. // IEEE Trans. on Computers. V. C-34, no. 1, 1985, pp. 81-85.
- [SMC 04] Stanica P., Maitra S., and Clark J. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. // Proc. of FSE'04, LNCS 3017, pp. 161-177, 2004.
- [SST 10] Sloan R.H., Szorenyi B., and Turan G. Learning Boolean Functions with Queries. In Boolean Models and Methods in Mathematica, Computer Science, and Engineering. Ed. Crama Y. and Hammer P.L., Cambridge University Press, 2010, pp. 221-256.
- [Tao 08] Tao R. Finite Automata and Application to Cryptography. Springer, 2008, pp. 441.
- [Terr 01] Terras A. Fourier Analysis on Finite Groups and Applications. Cambridge University Press, Cambridge, 2001, pp. 453.
- [Val 84] Valiant L.G. A theory of the learnable. Comm. ACM, v.27, №11, pp. 1134-1142.

- [Vol 08] Volkov M.V. Synchronizing automata and the Cerny conjecture. // Lect. Notes Comp. Sci., v.5196, pp. 11-27.
- [Wash 08] Washington L.C. Elliptic Curves — Number Theory and Cryptography. CRC Press, 2008, pp. 513.
- [Wiel 64] Wielandt H. Finite Permutation Groups. Academic Press, New York-London, 1964, pp. 124.
- [WuD 00] Wu C., Dowson E. Construction of correlation immune Boolean functions7 Australian Journal of Combinatorics, 21, 2000, pp. 141-166.
- [YaGu 95] Yang Y.X., and Guo B. Furter Enumerating Boolean Functions of Cryptographic Signifians. // Journal of Cryptology 8(3), pp. 115-122,1995.
- [Yao 82] A.C.-C.Yao Protocols for Secure Computations (Extended Abstract). FOCS 1982, pp. 160-164.
- [ZXX 10] Zhou Y., Xie M., Xiao G.Z. On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Information Sciences, 180, 2, 2010, pp. 256-265.

Приложение А

Некоторые примитивы, используемые при синтезе средств обеспечения информационной безопасности

а) Регистры сдвига с линейными обратными связями (см. рис. [A.1](#)) длины n с полиномом обратных связей $c(\lambda) = 1 \oplus c_1\lambda \oplus \dots \oplus c_n\lambda^n \in \mathbb{F}_2[\lambda]$, $c_0 = c_n = 1$. Будем обозначать этот регистр $\text{LFSR}(n, c(\lambda))$.

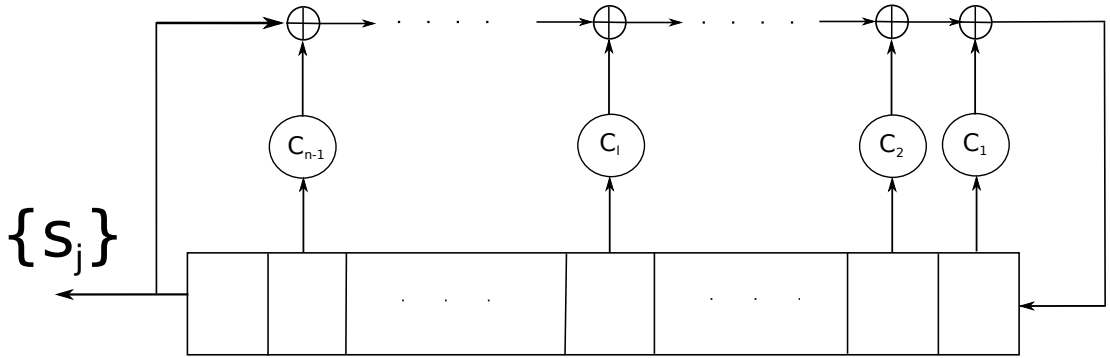


Рисунок А.1 — Регистр сдвига с линейными обратными связями —
 $\text{LFSR}(n, c(\lambda))$

Он генерирует линейную рекуррентную последовательность над полем $\mathbb{F}_2$ вида

$$s_j = c_1 s_{j-1} \oplus c_2 s_{j-2} \oplus \dots \oplus c_n s_{j-n},$$

$j \geq n$, где $(s_0, s_1, \dots, s_{n-1}) = s$ — начальное состояние регистра. Если $c(\lambda)$ — примитивный полином, то последовательность $\{s_j\}$ имеет максимальный возможный период $2^n - 1$, если $s \neq 0^n$ (операция $\oplus$ — сложение по $(\text{mod } 2)$).

б) Автономный регистр сдвига длины n с нелинейной обратной связью мы будем обозначать $\text{AFSR}(n, g)$, $g \in \mathcal{F}_n$, $\deg(g) > 1$ (см. рис. [A.2](#)).

Данный регистр генерирует нелинейную рекуррентную последовательность $\{s_j\}$ над полем $\mathbb{F}_2$, задаваемую начальным состоянием $s = (s_0, s_1, \dots, s_{n-1})$, вида $s_j = g(s_{j-n}, s_{j-n+1}, \dots, s_{j-1})$, $j \geq n$.

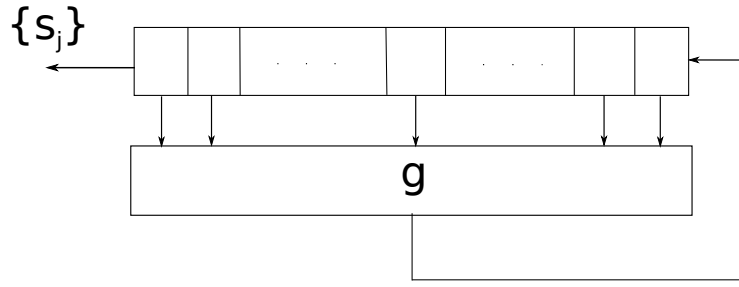


Рисунок А.2 — Автономный регистр сдвига с нелинейной обратной связью — $\text{AFSR}(n, g)$

с) Неавтономный регистр сдвига длины n с нелинейной обратной связью мы будем обозначать $\text{NFSR}(n, g)$, $g \in \mathcal{F}_n$, $\deg(g) > 1$ (см. рис. А.3).

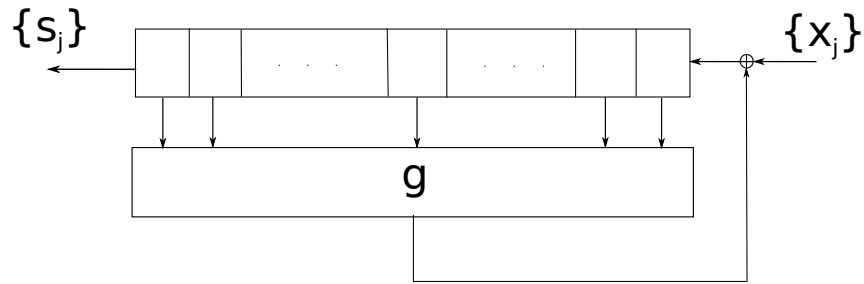


Рисунок А.3 — Неавтономный регистр сдвига — $\text{NFSR}(n, g)$

Начальное состояние регистра $s = (s_0, s_1, \dots, s_{n-1})$ и входная строка $\{x_j\}$ порождают выходную строку $\{s_j\}$, где $s_j = g(s_{j-n}, s_{j-n+1}, \dots, s_{j-1}) \oplus x_{j-n}$, $j \geq n$.

d) Неавтономный регистр сдвига длины n с фильтрующей функцией $f \in \mathcal{F}_n$ (см. рис. А.4) будем обозначать $\text{SR}(n, f)$.

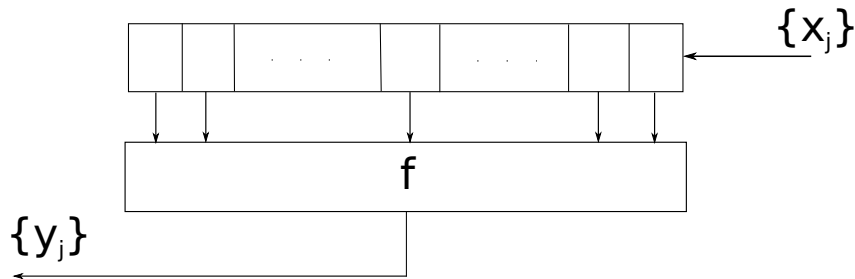


Рисунок А.4 — Неавтономный регистр с фильтрующей функцией — $\text{SR}(n, f)$

На вход регистра поступает строка $\{x_j\}$. На выходе регистра $\text{SR}(n, f)$ вырабатывается строка $\{y_i\}$, где $y_i = f(x_i, x_{i+1}, \dots, x_{i+n-1})$, $i \geq 0$.

е) Поточковый шифр, построенный на основе фильтрующего генератора — FG и шифрующего блока — CS (см. рис. А.5). Фильтрующий генератор со-

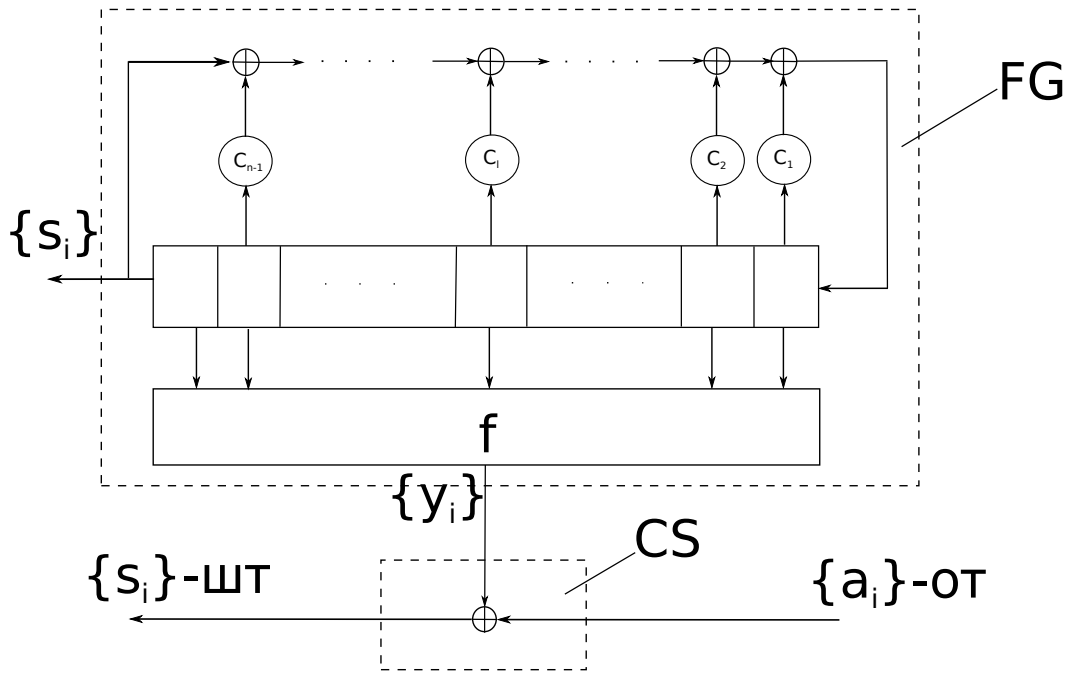


Рисунок А.5 — Поточковый шифр на основе фильтрующего генератора

стоит из регистра сдвига с линейными обратными связями — $\text{LFSR}(n, c(\lambda))$ и фильтрующей функции f из $\mathcal{F}_n$. Мы будем обозначать фильтрующий генератор $\text{LFSR}(c(\lambda), f)$. Выходная строка $\{y_i\}$ фильтрующего генератора определяется соотношениями

$$y_i = f(\mathcal{B}^i s), i = 0, 1, \dots,$$

где

$$\mathcal{B} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ c_n & c_{n-1} & c_{n-2} & \cdots & c_2 & c_1 \end{bmatrix} \quad -$$

матрица линейного преобразования, реализуемого регистром $\text{LFSR}(n, c(\lambda))$, $s = (s_0, s_1, \dots, s_{n-1})$ — начальное состояние фильтрующего генератора. Знаки шифр-текста (ШТ) определяются соотношениями $z_i = a_i \oplus y_i, i = 0, 1, \dots$, где $\{a_i\}$ — знаки открытого текста.

f) Поточковый шифр, построенный на основе комбинирующего генератора — CG и шифрующего блока — CS (см. рис. А.6). Комбинирующий генератор

состоит из m экземпляров регистров сдвига с линейными обратными связями — $\text{LFSR}(n_t, c^t(\lambda))$, $t = 1, 2, \dots, r$ и комбинирующей булевой функции f из $\mathcal{F}_n$. Регистры $\text{LFSR}(n_t, c^t(\lambda))$, $t = 1, 2, \dots, r$ вырабатывают фрагменты линейных рекуррентных последовательностей $\{s_i^t\}$, $t = 1, \dots, r$ над полем $\mathbb{F}_2$. Выходная

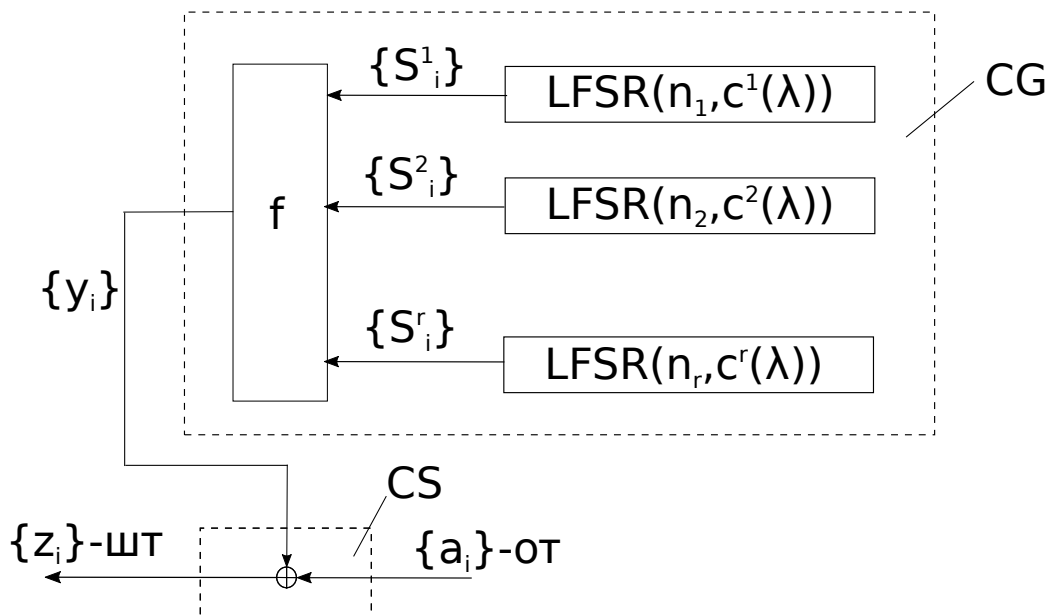


Рисунок А.6 — Поточковый шифр на основе комбинирующего генератора

строка $\{y_i\}$ комбинирующего генератора определяется соотношениями

$$y_i = f(s_i^1, s_i^2, \dots, s_i^m), i = 0, 1, \dots$$

Знаки шифртекста (ШТ) определяются соотношениями $z_i = a_i \oplus y_i$, $i = 0, 1, \dots$, где $\{a_i\}$ — знаки открытого текста (ОТ).

Необходимо отметить, что приведенные выше криптографические примитивы синтезированы первоначально на основе алфавита $A = \mathcal{F}_2$. Однако, впоследствии аналогичные криптографические примитивы синтезировались на основе различных конечных алфавитов. Наиболее часто в качестве основного алфавита A использовались поля Галуа. В тексте диссертации сокращенные названия данных криптографических примитивов используются для произвольного основного алфавита (каждый раз из контекста ясно какого).

Приложение Б

Аффинная нормальная форма фильтрующей функции генератора псевдослучайных последовательностей шифра LiLi-128

Фильтрующая функция LiLi-128 имеет вид:

$$\begin{aligned} f(x_1, x_2, \dots, x_{10}) = & x_5 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_{10}x_6 \oplus x_{10}x_4 \oplus x_9x_3 \oplus x_9x_1 \oplus \\ & \oplus x_8x_2 \oplus x_8x_1 \oplus x_7x_6 \oplus x_{10}x_9x_5 \oplus x_{10}x_9x_4 \oplus x_{10}x_9x_3 \oplus x_{10}x_9x_2 \oplus x_{10}x_8x_4 \oplus \\ & \oplus x_{10}x_8x_3 \oplus x_{10}x_7x_6 \oplus x_1x_7x_5 \oplus x_{10}x_7x_4 \oplus x_9x_8x_6 \oplus x_9x_8x_3 \oplus x_9x_7x_6 \oplus \\ & \oplus x_9x_7x_4 \oplus x_9x_7x_3 \oplus x_{10}x_9x_8x_6 \oplus x_{10}x_9x_8x_4 \oplus x_{10}x_9x_8x_3 \oplus x_{10}x_9x_8x_1 \oplus \\ & \oplus x_{10}x_9x_7x_6 \oplus x_{10}x_9x_7x_4 \oplus x_{10}x_9x_7x_2 \oplus x_{10}x_8x_7x_5 \oplus x_{10}x_8x_7x_3 \oplus x_9x_8x_7x_4 \oplus \\ & \oplus x_9x_8x_7x_2 \oplus x_9x_7x_6x_5 \oplus x_9x_7x_6x_4 \oplus x_{10}x_9x_8x_7x_4 \oplus x_{10}x_9x_8x_7x_4 \oplus \\ & \oplus x_{10}x_9x_8x_7x_3 \oplus x_{10}x_9x_7x_6x_5 \oplus x_{10}x_9x_7x_6x_4 \oplus x_9x_8x_7x_6x_5 \oplus x_9x_8x_7x_6x_4 \oplus \\ & \oplus x_{10}x_9x_8x_7x_6x_5 \oplus x_{10}x_9x_8x_7x_6x_4. \end{aligned}$$

Аффинная нормальная форма функции $f : f(x) = \bigoplus_{i=1}^{33} \chi_{\pi_i}(x) l_{\pi_i}(x)$. Соответствующее табличное представление приведено в таблицах [2.1](#), [2.2](#).

NN i	χ_{π_i}	NN i	χ_{π_i}
1	$\bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4$	18	$\bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4(x_7 \oplus x_5)$
2	$\bar{x}_1x_2\bar{x}_3\bar{x}_4\bar{x}_5$	19	$x_1\bar{x}_2\bar{x}_3\bar{x}_4(x_7 \oplus x_5)$
3	$x_1x_2\bar{x}_3\bar{x}_4\bar{x}_5$	20	$\bar{x}_1x_2\bar{x}_3\bar{x}_4(x_7 \oplus x_5)$
4	$\bar{x}_1\bar{x}_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus 1)$	21	$x_1x_2\bar{x}_3\bar{x}_4(x_7 \oplus x_5)$
5	$x_1\bar{x}_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus 1)$	22	$\bar{x}_1\bar{x}_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus x_8 \oplus x_5)$
6	$\bar{x}_1x_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus x_5 \oplus 1)$	23	$x_1\bar{x}_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus x_8 \oplus x_5)$
7	$x_1x_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus x_5 \oplus 1)$	24	$\bar{x}_1x_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus x_7 \oplus x_5)$
8	$\bar{x}_1\bar{x}_2\bar{x}_3x_4(x_{10} \oplus x_8 \oplus 1)$	25	$x_1x_2x_3\bar{x}_4(x_{10} \oplus x_9 \oplus x_7 \oplus x_5)$
9	$x_1\bar{x}_2\bar{x}_3x_4(x_{10} \oplus x_8 \oplus 1)$	26	$\bar{x}_1\bar{x}_2\bar{x}_3x_4(x_{10} \oplus x_9 \oplus x_6 \oplus x_5)$
10	$\bar{x}_1\bar{x}_2x_3\bar{x}_4x_5(x_{10} \oplus x_7 \oplus 1)$	27	$x_1\bar{x}_2\bar{x}_3x_4(x_{10} \oplus x_9 \oplus x_6 \oplus x_5)$
11	$x_1\bar{x}_2x_3\bar{x}_4x_5(x_{10} \oplus x_7 \oplus 1)$	28	$\bar{x}_1x_2\bar{x}_3x_4(x_{10} \oplus x_8 \oplus x_7 \oplus x_5)$
12	$\bar{x}_1x_2x_3\bar{x}_4x_5(x_{10} \oplus x_6 \oplus 1)$	29	$x_1x_2\bar{x}_3x_4(x_{10} \oplus x_8 \oplus x_7 \oplus x_5)$
13	$x_1x_2x_3\bar{x}_4x_5(x_{10} \oplus x_6 \oplus 1)$	30	$\bar{x}_1\bar{x}_2x_3x_4(x_{10} \oplus x_8 \oplus x_6 \oplus x_5)$
14	$\bar{x}_1\bar{x}_2x_3x_4(x_9 \oplus x_5 \oplus 1)$	31	$x_1\bar{x}_2x_3x_4(x_{10} \oplus x_8 \oplus x_6 \oplus x_5)$
15	$x_1\bar{x}_2x_3x_4(x_9 \oplus x_5 \oplus 1)$	32	$\bar{x}_1x_2x_3x_4(x_{10} \oplus x_7 \oplus x_6 \oplus x_5)$
16	$x_1x_2x_3x_4(x_8 \oplus x_5 \oplus 1)$	33	$x_1x_2x_3x_4(x_{10} \oplus x_7 \oplus x_6 \oplus x_5)$
17	$\bar{x}_1x_2x_3x_4(x_8 \oplus x_5 \oplus 1)$		

Таблица 2.1

NN i	l_{π_i}	NN i	l_{π_i}
1	$x_{10}x_9 \oplus x_8 \oplus x_7$	18	$x_{10} \oplus x_9 \oplus x_8$
2	$x_{10}x_9 \oplus x_8 \oplus x_7$	19	$x_{10} \oplus x_9 \oplus x_7$
3	$x_{10}x_9 \oplus x_8 \oplus x_7 \oplus 1$	20	$x_{10} \oplus x_9 \oplus x_8$
4	$x_9 \oplus x_8 \oplus x_7$	21	$x_{10} \oplus x_9 \oplus x_8$
5	$x_9 \oplus x_8 \oplus x_7 \oplus 1$	22	$x_8 \oplus x_7$
6	$x_9 \oplus x_8 \oplus x_7$	23	$x_8 \oplus x_7 \oplus 1$
7	$x_9 \oplus x_8 \oplus x_7 \oplus 1$	24	$x_9 \oplus x_7$
8	$x_{10} \oplus x_8 \oplus x_7$	25	$x_9 \oplus x_7 \oplus 1$
9	$x_{10} \oplus x_8 \oplus x_7 \oplus 1$	26	$x_9 \oplus x_8$
10	$x_{10} \oplus x_9 \oplus x_7$	27	$x_9 \oplus x_8 \oplus 1$
11	$x_{10} \oplus x_9 \oplus x_7 \oplus 1$	28	$x_{10} \oplus x_7$
12	$x_{10} \oplus x_9 \oplus x_8$	29	$x_{10} \oplus x_7 \oplus 1$
13	$x_{10} \oplus x_9 \oplus x_8 \oplus 1$	30	$x_{10} \oplus x_8$
14	$x_9 \oplus x_8 \oplus x_7$	31	$x_{10} \oplus x_8 \oplus 1$
15	$x_9 \oplus x_8 \oplus x_7$	32	$x_{10} \oplus x_9$
16	$x_{10} \oplus x_8 \oplus x_7$	33	$x_{10} \oplus x_9 \oplus 1$
17	$x_{10} \oplus x_8 \oplus x_7$		

Таблица 2.2

Приложение В

Локальные аффинности булевых отображений

1. Пример отображения, для которого условие 1° определения 13.4а выполнено, а условие 2° не выполнено. Пусть $n = m = 3$. Рассмотрим отображение $\Phi \in \mathcal{F}_{3,3}$, таблица этого отображения изображена на рис.

В.1.

	$x^{(1)}$	$x^{(2)}$	$x^{(3)}$	$\Phi(x^{(1)}, x^{(2)}, x^{(3)})$	
$\pi =$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$	π'
$\pi' =$	$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	π_1

Рисунок В.1

Пусть

$$\pi = \{(0,0,0)^\top, (0,0,1)^\top, (0,1,0)^\top, (0,1,1)^\top\} \quad —$$

плоскость в пространстве V_3 . Тогда $\pi' = \pi \oplus e^1$ — плоскость и $\dim \pi' = \dim \pi = 2$. Кроме того, $\pi \cup \pi' = V_3$ и $\Phi(\pi) = \pi'$. Легко видеть, что сужение Φ на плоскость π совпадает с сужением аффинного отображения $\Psi : x \rightarrow x \oplus e^1$ на этой плоскости. С другой стороны, $\Phi(\pi') = \pi_1$, где $\pi_1 = \{(0,0,0)^\top, (0,0,1)^\top\}$, $\dim \pi_1 = 1$. Предположим, что сужение отображения Φ на π' совпадает с сужением на π' некоторого аффинного отображения $\psi \in \mathcal{A}_{3,3}$. Отображение ψ имеет вид $x \rightarrow Ax \oplus a$, где $x, a \in V_3$ и A — 3×3 -матрица над $\mathbb{F}_2$. Так как Ψ — аффинное отображение, то для любых $u, v \in V_3$ выполнено равенство

$$\Psi(u \oplus v) \oplus \Psi(0^n) = \Psi(u) \oplus \Psi(v). \quad (\text{B.1})$$

Рассмотрим две пары векторов (u, v) и (u', v') таких, что $u, v, u', v' \in V_3$, $(u, v) \neq (u', v')$ и $u \oplus v = u' \oplus v'$. Тогда из равенства (B.1) следует

$$\Psi(u) \oplus \Psi(v) = \Psi(u') \oplus \Psi(v').$$

Пусть $u = (1, 0, 0)^\top$, $v = (1, 1, 0)^\top$, $u' = (1, 0, 1)^\top$, $v' = (1, 1, 1)^\top$; $u \oplus v = u' \oplus v' = (1, 0, 1)^\top$. Однако,

$$\Psi(u) \oplus \Psi(v) = (0, 0, 0)^\top \neq (0, 0, 1)^\top = \Psi(u') \oplus \Psi(v').$$

Полученное противоречие показывает, что сужение отображения Φ на плоскости π' не может совпадать с каким-либо аффинным отображением из $\mathcal{A}_{3,3}$.

2. Диаграмма Хассе для локальных аффинностей. Пусть $n = 2$ и $\Phi \in \mathcal{F}_{2,2}$ (см. рис. B.2). Легко видеть, что Φ не является аффинным преобразованием.

Для любого натурального n число r -плоскостей из V_n (см. [?]), равно $2^{n-r} \begin{bmatrix} n \\ r \end{bmatrix}$, где

$$\begin{bmatrix} n \\ r \end{bmatrix} = \begin{cases} \frac{(2^n-1)(2^n-2)\dots(2^n-2^{n-1})}{(2^r-1)(2^r-2)\dots(2^r-2^{r-1})}, & \text{если } 1 \leq r \leq n; \\ 1, & \text{если } r = 0, \end{cases}$$

Гауссовский биномиальный коэффициент. Следовательно, общее число плоскостей (за исключением пустой) равно

$$\sum_{r=0}^n 2^{n-r} \begin{bmatrix} n \\ r \end{bmatrix}$$

	$x^{(1)}$	$x^{(2)}$	$\Phi(x^{(1)}, x^{(2)})$
$u_0 =$	$(0, 0)^\top$		$(1, 1)^\top$
$u_1 =$	$(0, 1)^\top$		$(1, 0)^\top$
$u_2 =$	$(1, 0)^\top$		$(1, 1)^\top$
$u_3 =$	$(1, 1)^\top$		$(0, 1)^\top$

Рисунок В.2

Плоскости в V_2 занумерованы в соответствии с порядковыми номерами векторов в V_2 (см. рис. В.3) Всего в V_2 содержится 11 плоскостей (без

r	Число плоскостей разм. r	Множество плоскостей разм. r
0	4	$\pi_0 = \{(0,0)^\top\}, \pi_1 = \{(0,1)^\top\},$ $\pi_2 = \{(1,0)^\top\}, \pi_3 = \{(1,1)^\top\}$
1	6	$\pi_{0,1}, \pi_{0,2}, \pi_{0,3}, \pi_{1,2}, \pi_{1,3}, \pi_{2,3}$
2	1	$\pi = \pi_{0,1,2,3} = V_2$

Рисунок В.3 — Плоскости пространства V_2 .

пустой плоскости). Для множества 0-плоскостей справедливо включение

$$\{\pi_0, \pi_1, \pi_2, \pi_3\} \subset P_{2,2}(\Phi) \subseteq Q_{2,2}(\Phi).$$

Полная аффинная группа $\mathfrak{GA}(n)$ является 2-транзитивной для любого натурального $n \geq 1$ (см. [?]). Следовательно, существует $\mathfrak{g} \in \mathfrak{GA}(n)$ такой, что $\mathfrak{g}((0,0)^\top) = (1,1)^\top$, $\mathfrak{g}((0,1)^\top) = (1,0)^\top$, т.е. $\Phi_{\pi_{0,1}} = \mathfrak{g}_{\pi_{0,1}}$. Поэтому $\pi_{0,1} \in P_{2,2}(\Phi)$.

Так как,

$$\#\Phi(\pi_{0,3}) = \#\Phi(\pi_{1,2}) = \#\Phi(\pi_{1,3}) = \#\Phi(\pi_{2,3}) = 2,$$

то воспользовавшись аналогичными рассуждениями можно доказать справедливость включения

$$\{\pi_{0,1}, \pi_{0,3}, \pi_{1,2}, \pi_{1,3}, \pi_{2,3}\} \subset P_{2,2}(\Phi).$$

Рассмотрим плоскость $\pi_{0,2} : \Phi(\pi_{0,2}) = \{(1,1)^\top\}$. В этом случае легко показать, что аффинное отображение

$$\Psi(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x \oplus \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

удовлетворяет условию $\Psi_{[i_{0,2}} = \Phi_{\pi_{0,2}}$. Следовательно, $\pi_{0,2} \in P_{2,2}(\Phi)$.

Кроме того, ясно, что $\pi_{0,1,2,3} \notin P_{2,2}(\Phi)$ и $\pi_{0,1,2,3} \notin Q_{2,2}(\Phi)$.

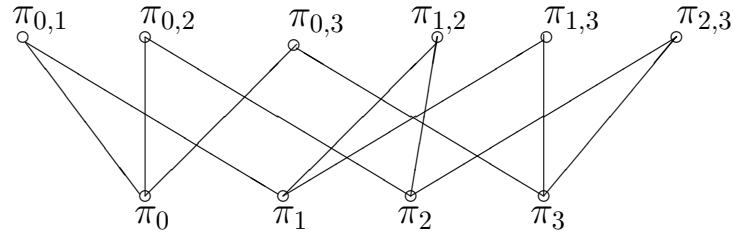


Рисунок В.4 — Диаграмма Хассе для $P_{2,2}(\Phi)$

Таким образом, для отображения Φ , рассмотренного выше, выполнено:

$$Q_{2,2}(\Phi) = P_{2,2}(\Phi) = \{\pi_0, \pi_1, \pi_2, \pi_3, \pi_{0,1}, \pi_{0,2}, \pi_{0,3}, \pi_{1,2}, \pi_{1,3}, \pi_{2,3}\},$$

$$p_{2,2}(\Phi) = (4, 6, 0),$$

$$M_{2,2}(\Phi) = \{\pi_{0,1}, \pi_{0,2}, \pi_{0,3}, \pi_{1,2}, \pi_{1,3}, \pi_{2,3}\}.$$

Диаграмма Хассе для множества $P_{2,2}(\Phi)$ изображена на рис. [В.4](#).

Приложение Г

Аффинное обращение ограниченно-детерминированных функций, реализуемых конечными автоматами вида $\text{SR}(n, f)$

Функционирование конечного автомата $\mathcal{M} = \text{SR}(n, f)$, $n \in \mathbb{N}$, $f \in \mathcal{F}_n$ (см. Приложение А, d) может быть задано следующей системой булевых уравнений:

$$\begin{cases} y_i = f(x_i, \dots, x_{i+n-1}), \\ i = 0, 1, \dots, m-1 \end{cases}$$

или

$$y = f_m(x),$$

где

$$x = (x_0, x_1, \dots, x_{m+n-2}) \in \mathbb{F}_2^{m+n-1} \text{ —}$$

входное слово автомата $\text{SR}(n, f)$

$$y = (y_0, y_1, \dots, y_{m-1}) \in \mathbb{F}_2^m \text{ —}$$

выходное слово автомата $\text{SR}(n, f)$ и

$$f_m(x) = (f(x_0, \dots, x_{n-1}), \dots, f(x_{m-1}, \dots, x_{m+n-2})).$$

Рассмотрим вариант частичного обращения ограниченно-детерминированной функции, определяемой автоматом $\text{SR}(n, f)$, названный в [?] аффинным обращением.

Пусть A — (k, m) -матрица над полем $\mathbb{F}_2$, $\text{rank} A = k$, $1 \leq k \leq m$; B — $(l \times (m + n - 1))$ -матрица над полем $\mathbb{F}_2$, $\text{rank} B = l$, $1 \leq l \leq m + n - 1$.

Пусть $a \in \mathbb{F}_2^k$, $b \in \mathbb{F}_2^l$ и $\text{rank}[A \mid a] = r$, $\text{rank}[B \mid b] = l$. Будем обозначать $\mathfrak{A} = \{A, a\}$ и $\mathfrak{B} = \{B, b\}$.

Пару $(\mathfrak{A}, \mathfrak{B})$ будем называть аффинным свойством, пару натуральных чисел $(m, m + n - 1)$ — размером аффинного свойства, а пару натуральных чисел $(2^{m-k}, 2^{m+n-l-1})$ — мощностью аффинного свойства. Для натуральных m и n будем обозначать через $\text{Prop}(n, m)$ множество всех возможных аффинных свойств размера $(m, m + n - 1)$.

Автомат $\text{SR}(n, f)$ (булева функция f из $\mathcal{F}_n$) обладает аффинным свойством $(\mathfrak{A}, \mathfrak{B}) \in \text{Prop}(m, n)$, если для любых $x \in \mathbb{F}_2^{m+n-1}$ и $y \in \mathbb{F}_2^m$ таких, что $y = f_m(x)$, из выполнения соотношения $Ay \oplus a = 0^k$ следует выполнение соотношения $Bx \oplus b = 0^l$.

В частности в примере 17.5 показано, что автомат $\text{SR}(n, f)$ с произвольной симметрической функцией из $\mathcal{F}_n$ при $m = 2$, $k = 2$, $l = 1$ обладает аффинными свойствами $(\mathfrak{A}^1, \mathfrak{B}^1)$, где

$$\begin{aligned}\mathfrak{A}^1 &= \{A^1, a^1\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \\ \mathfrak{B}^1 &= \{B^1, b^1\} = \{(1, 0, \dots, 0, 1), (1)\},\end{aligned}$$

и $(\mathfrak{A}^2, \mathfrak{B}^2)$, где

$$\begin{aligned}\mathfrak{A}^2 &= \{A^2, a^2\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}, \\ \mathfrak{B}^2 &= \{B^2, b^2\} = \{(1, 0, \dots, 0, 1), (1)\}.\end{aligned}$$

В работе [ЛoHa 07] на основе аффинных свойств построены полиномиальные алгоритмы нахождения секретных ключей фильтрующих генераторов $\text{LFSR}(c(\lambda), f)$ с симметрическими, либо ротационно-симметрическими фильтрующими функциями f .

Приложение Д

Обращение ограниченно-детерминированной функции, реализуемой комбинирующим генератором с устойчивой функцией усложнения.

Рассмотрим комбинирующий генератор (CG, рис. A.6), построенный с помощью m регистров сдвига с линейными обратными связями - LFSR $(n_i, c^i(\lambda))$, $i = 1, \dots, m$ и k -устойчивой [ЛССЯ 15] булевой функцией f от m переменных, $1 < k < m$.

Задача обращения формулируется следующим образом. Пусть известна строка $y = (y_1, y_2, \dots, y_N)$, выработанная комбинирующим генератором, и задача состоит в нахождении (определении) неизвестных начальных состояний $(s_1^{(1)}, \dots, s_{n_1}^{(1)})$, $(s_1^{(2)}, \dots, s_{n_2}^{(2)})$, $\dots$, $(s_1^{(m)}, \dots, s_{n_m}^{(m)})$ регистров сдвига, при которых была получена строка y . Другими словами, задача состоит в нахождении фрагментов линейных рекуррентных последовательностей $s^{(1)} = \{s_t^{(1)}\}_{t=1}^N, \dots, s^{(m)} = \{s_t^{(m)}\}_{t=1}^N$.

Эту задачу решают с помощью различных вариантов корреляционного анализа: с использованием статистических процедур ([Sieg 85]), на основе ретико-кодowego подхода ([CJS 00]) и т.д. В результате анализа этой задачи в работах [Sieg 84], [Sieg 85] была выдвинута концепция корреляционно-иммунных функций. Основное содержание этой концепции состоит в следующем.

Пусть $x = (x_1, \dots, x_n) \in_u \mathbb{F}_2^n$ и булева функция $f \in \mathcal{F}_m$ удовлетворяет условию: случайные величины $f(x_1, \dots, x_n)$ и $x_{j_1 \dots j_k} = (x_{j_1}, \dots, x_{j_k})$ независимы при любых $1 \leq j_1 < \dots < j_k \leq n$. Это свойство обуславливает необходимость при решении задачи обращения корреляционным методом опробовать на первом этапе начальные заполнения не менее чем $k + 1$ регистров сдвига из имеющихся m . Трудоемкость этой процедуры вносит существенный вклад в общую трудоемкость корреляционного метода.

Данное приложение иллюстрирует формальность и ограниченность подхода к синтезу дискретных функций, обладающих определенным (конечным) набором свойств. В частности, будет показано, что эффективность обращения дискретной функции существенно зависит от более широкого семейства особенностей (известных и неизвестных) данной функции, нежели постулируемый набор свойств, определяемый уровнем исследованности функции.

Введем дополнительное предположение о функции усложнения f комбинирующего генератора. Предположим, что f — k -устойчивая функция из $\mathcal{F}_m$ принадлежит классу Майорана-Макфарланда.

Пусть $p = r$ — натуральные числа, $m \geq r > p$ и $s = m - r \leq k$. Отображение $\Phi : \mathbb{F}_2^s \rightarrow \mathbb{F}_2^r$ удовлетворяет условию $\text{wt}(\Phi(u)) \geq p$ для любого $u \in \mathbb{F}_2^s$ и g — произвольная функция из $\mathcal{F}_s$. Воспользовавшись координатным представлением отображения $\Phi = (\Phi_1, \Phi_2, \dots, \Phi_r)$ имеем

$$f(x) = f_{\Phi, g}(x_1, x_2, \dots, x_m) = \bigoplus_{i=1}^r x_i \Phi_i(x_{r+1}, \dots, x_m) \oplus g(x_{r+1}, \dots, x_m) \quad (\text{Д.1})$$

Известно (см. [Car 10,1]), что функция f является k -устойчивой функцией при некотором $k \geq p$.

Рассмотрим алгоритм обращения комбинирующего генератора с функцией усложнения $f_{\Phi, g}$ по известной строке $y = (y_1, \dots, y_N)$. Будем опробовать начальные состояния регистров с номерами $r + 1, r + 2, \dots, m$, а именно

$$\left\{ \begin{array}{l} \left(x_1^{(r+1)}, x_2^{(r+1)}, \dots, x_{n_{r+1}}^{(r+1)} \right), \\ \left(x_1^{(r+2)}, x_2^{(r+2)}, \dots, x_{n_{r+2}}^{(r+2)} \right), \\ \dots \\ \left(x_1^{(m)}, x_2^{(m)}, \dots, x_{n_m}^{(m)} \right), \end{array} \right.$$

вырабатывая фрагменты линейных рекуррентных последовательностей $x^{(r+1)}, x^{(r+2)}, \dots, x^{(m)}$ длины N .

Пусть $(b_t^{(r+1)}, b_t^{(r+2)}, \dots, b_t^{(m)}) \in \mathbb{F}_2^s$, $t = 1, 2, \dots, N$ — опробуемые фрагменты последовательностей соответствующих регистров. Воспользовавшись соотношением (Д.1), получим систему линейных уравнений относительно оставшихся переменных

$$\begin{cases} y_t = \bigoplus_{i=1}^r x_t^{(i)} \cdot \Phi_i(b_t^{(r+1)}, \dots, b_t^{(m)}) \oplus g(b_t^{(r+1)}, \dots, b_t^{(m)}), \\ t = 1, 2, \dots, N. \end{cases} \quad (\text{Д.2})$$

Обозначим $y'_t = y_t \oplus g(b_t^{(r+1)}, \dots, b_t^{(m)})$, $t = 1, \dots, N$. Поскольку для отображения Φ выполнено условие $\text{wt}(\Phi(u)) \geq p$ для любого $u \in \mathbb{F}_2^s$, то в каждом уравнении из (Д.2) будет нетривиальное линейное соотношение от неизвестных $x_t^{(1)}, x_t^{(2)}, \dots, x_t^{(r)}$. Для каждого фрагмента линейной рекуррентной последовательности $x^{(i)}$, $i = 1, 2, \dots, m$ каждый его элемент $x_t^{(i)}$ является линейной комбинацией первых n_i элементов этого фрагмента $x_1^{(i)}, x_2^{(i)}, \dots, x_{n_i}^{(i)}$. Поэтому его можно представить в виде

$$x_t^{(i)} = c_{t,1}^{(i)} x_1^{(i)} \oplus c_{t,2}^{(i)} x_2^{(i)} \oplus \dots \oplus c_{t,n_i}^{(i)},$$

где $c_{t,1}^{(i)}, \dots, c_{t,n_i}^{(i)} \in \mathbb{F}_2$ определяются полиномом $c^i(\lambda)$. Тогда система (Д.2) принимает вид

$$\begin{cases} c_{1,1}^{(1)} x_1^{(1)} \oplus \dots \oplus c_{1,n_1}^{(1)} x_{n_1}^{(1)} \oplus \dots \oplus c_{1,1}^{(r)} x_1^{(r)} \oplus \dots \oplus c_{1,n_r}^{(r)} x_{n_r}^{(r)} & = y'_1 \\ \dots & \dots \dots \\ c_{N,1}^{(1)} x_1^{(1)} \oplus \dots \oplus c_{N,n_1}^{(1)} x_{n_1}^{(1)} \oplus \dots \oplus c_{N,1}^{(r)} x_1^{(r)} \oplus \dots \oplus c_{N,n_r}^{(r)} x_{n_r}^{(r)} & = y'_N, \end{cases} \quad (\text{Д.3})$$

то есть представляет собой систему N линейных уравнений от $n = n_1 + \dots + n_r$ переменных. Как правило для задач обращения данного вида справедливо неравенство $N \gg n$.

Если мы правильно угадали начальные состояния регистров $(b_1^{(j)}, b_2^{(j)}, \dots, b_{n_j}^{(j)}) \in \mathbb{F}_2^s$, $j = r + 1, \dots, m$, то система (Д.3) совместна. Если же мы не угадали начальные состояния регистров, то система (Д.3) может быть как совместна, так и не совместна. В случае ее несовместности можно отбраковывать на начальные состояния регистров с номерами $r + 1, r + 2, \dots, n$. Для того, чтобы оценить вероятность несовместности системы (Д.3), введем следующую статистическую модель. Будем предполагать, что величины $c_{t,i}^{(j)}$, $j = 1, \dots, r$, $t = 1, \dots, N$, $i = 1, \dots, n_j$ являются независимыми в совокупности одинаково распределенными двоичными случайными величинами, $\Pr [c_{t,i}^{(j)} = 0] = \Pr [c_{t,i}^{(j)} = 1] = 1/2$. Пусть

$$A = \begin{bmatrix} c_{1,1}^{(1)} & \dots & c_{1,n_1}^{(1)} & \dots & c_{1,1}^{(r)} & \dots & c_{1,n_r}^{(r)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{N,1}^{(1)} & \dots & c_{N,n_1}^{(1)} & \dots & c_{N,1}^{(r)} & \dots & c_{N,n_r}^{(r)} \end{bmatrix}$$

и

$$A' = \left[\begin{array}{c|c} A & \begin{matrix} y'_1 \\ \vdots \\ y'_N \end{matrix} \end{array} \right].$$

Необходимым и достаточным условием несовместности системы (Д.3) является неравенство

$$\text{rank } A \neq \text{rank } A'.$$

Для вероятности несовместности π_H системы (Д.3) справедливо неравенство

$$\pi_H \geq \pi_{H,n+1} = \Pr [\text{rank } A' = n + 1].$$

Вычислим вероятность $\pi_{H,n+1}$. При фиксации начальных заполнений регистров с номерами $r + 1, r + 2, \dots, m$ столбец $(y'_1, \dots, y'_N)^\top$ матрицы A' определен. Будем считать, что он не нулевой (выбором параметра N можно вероятность

$\Pr \left[(y'_1, \dots, y'_N)^\top \neq (0, \dots, 0)^\top \right]$ сделать сколь угодно близкой к 1). Для того, чтобы ранг матрицы A' был полный, второй столбец матрицы A' должен быть линейно независим от $(y'_1, \dots, y'_N)^\top$, т.е. он может быть выбран один из $2^N - 2$ способов; далее для того, чтобы ранг матрицы A' был полный, третий столбец матрицы A' должен быть линейно независим от первых двух, т.е. он может быть выбран одним из $2^N - 2^2$ способов. Таким образом

$$\begin{aligned} \pi_{H,n+1} &= \frac{2^N - 2}{2^N} \cdot \frac{2^N - 2^2}{2^N} \cdot \dots \cdot \frac{2^N - 2^n}{2^N} = \\ &= \prod_{i=1}^n \left(1 - \frac{1}{2^{N-i}} \right) \geq \left(1 - \frac{1}{2^{N-n}} \right)^n. \end{aligned}$$

Выберем N кратным n , т.е. $N = \nu \cdot n$, $\nu > 1$ (это упрощает выкладки, но необходимая оценка может быть получена и для произвольного N). Имеем

$$\pi_{H,n+1} \geq \left(1 - \frac{1}{2^{(\nu-1)n}} \right)^n$$

и

$$\begin{aligned} 1 - \pi_{H,n+1} &\leq 1 - \left(1 - \frac{1}{2^{(\nu-1)n}} \right)^n = \\ &= \binom{n}{1} \frac{1}{(2^{\nu-1})^n} - \binom{n}{2} \frac{1}{(2^{\nu-1})^{2n}} + \dots \leq \\ &\leq \frac{n}{2^{(\nu-1)n}} \end{aligned}$$

Следовательно, вероятность $\pi_{H,n+1}$ выбором параметра ν может быть сделана сколько угодно близкой к 1. Поэтому, неверно угадав начальные состояния регистров сдвиг с номерами $r+1, r+2, \dots, t$, мы получим с вероятностью близкой к 1 несовместную систему (Д.3) линейных уравнений и отбракуем эти начальные состояния. Вычисление ранга матрицы A' можно проводить методом Гаусса. Это потребует $O(N^3)$ элементарных операций.

Таким образом, уже на первом шаге алгоритма будут найдены начальные состояния $s \leq k$ регистров, что невозможно осуществить, пользуясь корреляционным методом (см. [ЛСЯ 04,1]).