

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи



Логачев Олег Алексеевич

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

05.13.19 — методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
доктора физико-математических наук

Москва 2019

Работа выполнена на кафедре информационной безопасности факультета вычислительной математики и кибернетики ФГБОУ ВО "Московский государственный университет имени М. В. Ломоносова"

Официальные оппоненты: **Алиев Физули Камилович**,
доктор физико-математических наук,
доцент, Департамент информационных
систем Министерства обороны РФ.

Никонов Владимир Глебович,
доктор технических наук,
профессор, Академия криптографии РФ.

Фомичев Владимир Михайлович,
доктор физико-математических наук,
профессор, ФГБОУ ВО "Финансовый
университет при Правительстве Российской
Федерации", кафедра информационной
безопасности.

Защита состоится 25 декабря 2019 года в 16:45 на заседании диссертационного совета МГУ.05.01 при ФГБОУ ВО "Московский государственный университет имени М. В. Ломоносова" по адресу: Российская Федерация, 119234, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, Механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО МГУ имени М. В. Ломоносова, по адресу: Москва, Ломоносовский проспект, д. 27 и на сайте истина ИАС "ИСТИНА":

<https://istina.msu.ru/dissertations/241701632/>

Автореферат разослан 24.10.2019 года.

Ученый секретарь
диссертационного совета МГУ.05.01
кандидат физико-математических
наук



Кривчиков Максим Александрович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертация посвящена решению проблемы обращения дискретных функций в математических моделях информационной безопасности. Разработан математический аппарат для обращения дискретных функций, определенных на конечных абелевых группах. Предложены и обоснованы новые способы координатизации таких функций (т.е. способов конструирования новых параметров дискретных функций и исследования свойств этих параметров). Получены соотношения, связывающие параметры функций на конечных абелевых группах и влияющие на эффективность методов обращения.

Актуальность темы. Методы анализа систем (средств) обеспечения информационной безопасности (ИБ) имеют математическую природу и используются в рамках математических моделей, описывающих функционирование таких систем, действия противника и возможные угрозы ИБ.

Фундаментальной проблемой в области анализа систем обеспечения ИБ является получение обоснованных оценок уровня защиты информации. Одним из важнейших элементов анализа является задача оценки сложности обращения (инвертирования) дискретных функций, ассоциированных с системой обеспечения ИБ. Параметры, определяемые сложностью обращения, вносят существенный вклад в итоговую оценку уровня защищенности информации.

Таким образом, тема диссертации, посвященной разработке математического аппарата решения задачи обращения дискретных функций в математических моделях информационной безопасности, актуальна как в теоретическом, так и в прикладном смысле.

Области исследования. Диссертация представляет результаты исследований в области информационной безопасности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 05.13.19 по следующим областям 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.

Исследования базируются на известных теоретических положениях алгебры, дискретной математики, теории вероятностей, математического анализа, теории алгоритмов и теории кодирования.

Цель работы — совершенствование математических моделей и повышение на основе полученных результатов эффективности алгоритмов решения задач обращения дискретных функций. Развитие методов координатизации¹ и изучение параметров функций, влияющих на эффективность алгоритмов обращения. Описание особенностей классов функций, обладающих эффективными алгоритмами обращения.

Для достижения поставленной цели в диссертации приводятся новые теоретические результаты, существенно расширяющие возможности использования алгебраических методов для решения задач обращения. Приводятся результаты исследований параметров дискретных функций, позволяющие использовать методы частичного и методы локального обращения, а также сводить исходную задачу к решению систем линейных уравнений.

Научная новизна работы состоит в строго доказанных новых утверждениях и характеризуется следующими результатами:

- 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 свойств, аналогичных свойствам кодов Рида-Маллера;
- 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;
- для группового отображения предложено представление, обобщающее аффинное расщепление булевых отображений. На основе параметров этого представления введена характеристика "нелинейности" исходного группово-

¹Шафаревич И.Р. Основные понятия алгебры. Итоги науки и техники, т. 11, Москва, ВИНТИ, 1986, с. 289.

го отображения. Получен ряд соотношений и неравенств, связывающих эту характеристику "нелинейности" с основными параметрами отображения;

– предложена новая нормальная форма булевой функции на основе понятия локальной аффинности булевой функции. Строение и особенности этой нормальной формы определяют перспективность ее использования при разработке алгоритмов и методов обращения дискретных функций, основанных на аффинной аппроксимации уравнений;

– 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;

– 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;

– рассмотрена теоретико-автоматная модель частичного обращения ограниченно-детерминированных функций. Получены соотношения, показывающие влияние особенностей функции на параметры частичного обращения;

– 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. Новая теоретико-информационная характеристика семейства совершенно-уравновешенных функций.
12. Математическая модель "нелинейной" аппроксимации булевых функций на основе биортогональных базисов.

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 Рида-Маллера, а также максимально-нелинейные (бент) функции. Результаты исследований в этом направлении представлены в работах А.С. Амбросимова², О.А. Логачева, А.А. Сальникова, В.В. Яценко^{3 4 5}, сформировавших новое направление в изучении свойств дискретных функций. В последнее десятилетие эти исследования были продолжены. Их результаты можно найти, например, в работах В.И. Солодовникова^{6 7}, А.В. Черемушкина^{8 9 10} 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 указанием, сколько раз это значение встречается, когда g пробегает K . По-

²Амбросимов А.С. Свойства бент-функций q -значной логики над конечными полями. // Дискр. математика., том 6, вып. 3, 1994, с. 50-60.

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

⁴Логачев О.А., Яценко В.В. Коды типа Рида-Маллера на конечной абелевой группе. // Проблемы передачи информации, том 34, вып. 2. 1998, с. 32-46.

⁵Логачев 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.

⁶Солодовников В.И. Бент-функции из конечной абелевой группы в конечную абелеву группу. // Дискретн. математика, том 14, вып. 1, 2002, с. 99-113.

⁷Солодовников В.И. Три подхода к понятию функций, максимально отличающихся от гомоморфизмов. // Матем. вопр. криптографии, том 7, №3, 2016, с. 115-136.

⁸Черемушкин А.В. Аддитивный подход к определению степени нелинейности дискретной функции. // Прикл. дискретн. математика, № 2, 2010, с. 22-33.

⁹Черемушкин А.В. Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка. // Прикл. дискретн. математика, №2, 2013, с. 26-38.

¹⁰Черемушкин А.В. Вычисление степени нелинейности функции на циклической группе примарного порядка. // Прикл. дискретн. математика, том 24, №2, с. 37 - 47.

казано (теорема 2, [3]), 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 1, [3]) группы G . Подгруппа L_f характеризует скрытую "линейность" (по аналогии с булевым случаем¹¹) 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 (другими словами 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 4, [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 4 является необходимый признак нетривиальности группы L_f — наличие некоторого количества нулей среди коэффициентов Фурье функции f (лемма 2, [3]). Это связано с тем, что преобразование Фурье любого характера имеет только одно ненулевое значение.

Для аффинно эквивалентных функций f и f^σ , где $x^\sigma = e^\sigma x^\varphi$, $\varphi \in \text{Aut}(G)$, для любых $x \in G$, показано (теорема 5, [3]), что $L_{f^\sigma} = (L_f)^\varphi$.

¹¹Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. Булевы функции в теории кодирования и криптологии. М.: Ленанд, 2015, с. 576.

При использовании аппарата производных и работе со скалярным произведением функций из T^G полезно следующее соотношение (лемма 3, [3])

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

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 характеристам 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 $\#RM_1(G) = qn$.

Аналогию с классическим вариантом кода продолжает утверждение о строении группы автоморфизмов кода $RM_1(G)$. Показано (теорема 1, [3]), что $\text{Aut}(RM_1(G)) = \text{Aff}(G)$. Доказана также максимальность группы линейных трансляторов для функций из $RM_1(G)$ (теорема 3, [3]):

$$RM_1(G) = \{f \in T_q^G : L_f = G\},$$

что является дополнительной характеристикой кода $RM_1(G)$.

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 6, [3]). Непосредственным следствием из этого свойства является принадлежность всех кодом 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 полу-группу 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 $\mathbb{Z}_q G$ 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 4, [3]), 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 $\mathbb{Z}_q G$, 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 $\mathbb{Z}_q G$.

Выполнение равенства

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

эквивалентно существованию такого натурального N , что в 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 $\mathbb{Z}_q G$. Показано (лемма 5, [3]), 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 2, [3]), 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 (лемма 6, [3]) 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 7, теорема 7, [3]) 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 кодов¹². 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 В.А. Зиновьева и Т. Эриксона¹³. Для линейных кодов, построенных с помощью идеалов коммутативных колец и подмодулей квазифробениусовых модулей, эта концепция рассмотрена в работе А.А. Нечаева¹⁴.

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

$$\begin{aligned} A \subseteq U &\longrightarrow A^* \in V, \\ B \subseteq V &\longrightarrow B^+ \in U, \end{aligned}$$

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 1, [4] получены тождества, связывающие дуальные ρ -структуры для дуальных кодов. В следствии 1, [4] полученные общие соотношения интерпретируются для классического вида ρ -структур — весовых характеристик двоичных линейных кодов (тождество Мак-Вильямс).

¹²MacWilliams 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.

¹³Зиновьев 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.

¹⁴Зиновьев 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.

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

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

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 1, [2]) 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 работе А.С. Амбросимова¹.

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 1, [2]), что

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

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

Бент-функция на группе G обладает также одним интересным свойством. Функция $f \in T^G$ является бент-функцией (теорема 2, [2]) 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 3, [2]) между множеством таких бент-базисов $\text{BB}(G)$ и множеством нормированных бент-функций $\text{BNF}(G)$.

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

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

Для $f \in T^G$ и $Q < G$ найдены (теорема 4, [2]) необходимые и достаточные условия того, что $Q \setminus e \subseteq \text{PC}(f)$.

Понятие дуальной функции к бент-функции f определяется соотношением $\sqrt{n}\tilde{f}(u) = \hat{f}(u), u \in G$. Показано (теорема 6, [2]), 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 $\deg(P) = n$. Естественно 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 1, следствие 1, [5]) 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 2, [5] доказано, что каждый полином из $\mathcal{K}$ эквивалентен по следу некоторому cr -полиному. В соответствии с теоремой 2, [5] для любого полинома $P(x) \in \mathcal{K}$ 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 2, [5] и оценки Вейля позволяет улучшить оценку Вейля. В теореме 4, [5] (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^{15 16 17} 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 1, теорема 2, теорема 3, следствие 1, [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 3, следствие 1, [6]). В лемме 3, [4] получены алгебраические соотношения, позволяющие реализовать приведение булевой функции к невырожденной нормальной форме.

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 кодирования¹⁸ 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.

¹⁵Menezes A., van Oorschot P., and Vanstone S. Handbook of Applied Cryptography. CRC Press. 1996, pp. 810.

¹⁶Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф, Москва, 2003, с. 816.

¹⁷Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. Булевы функции в теории кодирования и криптологии. М.: Ленанд, 2015, с. 576.

¹⁸Сидельников В.М. Теория кодирования. М.: Физматлит, 2008, с. 324.

В работе [16] 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 (Уолша-Адамара). Один из основных вопросов в исследовании свойств данной кластеризации — это описание пустых секций (т.е. пересечений ортантов со сферой). В теореме 3 ([16]) доказано, что секции, соответствующие булевым функциям, обладающим линейными трансляторами, пусты. Для произвольной квадратичной функции от четного числа переменных доказан критерий (лемма 6, [16]) пустоты, соответствующей ей секции.

В работе [17] 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 характеристики 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 теореме 6 ([17]) рассмотрены связи глобальных лавинных характеристик булевых функций (σ_f, σ_g) с их обобщенной глобальной лавинной характеристикой $(\sigma_{f,g})$, а в теореме 7 ([17]) доказывается неизменность обобщенной глобальной лавинной характеристики для любой пары булевых функций, взятых из двух фиксированных классов Δ -эквивалентности.

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 1, [9]). 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 (лемма 6, [9]) новую характеристику (критерий) свойства корреляционной иммунности (наряду с имеющими

ся 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 1,2,3, [24]) 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 алгоритмах 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 [10], [11], [12], а также в работе М.Л. Бурякова рассмотрены связи этих параметров с различными криптографическими свойствами булевых функций. В частности, в [10] полностью описан класс булевых функций, обладающих максимальным возможным значением уровня аффинности. В работе¹⁹, а также в

¹⁹Буряков М.Л. Асимптотические оценки уровня аффинности для почти всех булевых функций. // Дискр. математика, том 20, вып.3, 2008, с. 73-79.

[11] получены нижние оценки уровня аффинности (обобщенного уровня аффинности) для почти всех булевых функций при стремлении к ∞ числа переменных. В работе [12] для $la(f)$ и $\mathcal{L}a(f)$ получены верхние оценки для почти всех булевых функций при стремлении к ∞ числа переменных. Указанные выше результаты позволяют доказать (теорема 3, [12]), 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.

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 алгебраи-

ческой 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 Уолша-Адамара этой функции. В теореме 2, ([24]) получен общий вид коэффициента Уолша-Адамара булевой функции, зависящий от параметров ее АффНФ. Данный вид нормальной формы позволяет описывать некоторые классы криптографических функций. В частности, на основе так называемых центрально дуальных разбиений на локальные аффинности (теорема 3, [24]) 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 4, ([24]) 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 [20] было показано, что возможности "нелинейной" аппроксимации не меньше, чем у "линейной". Для конкретного "нелинейного" базиса, являющегося комбинацией линейных и бент-функций, получено выражение (теорема 2, [20]) 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 1, ([20]) 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 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

графа (сильная связность, синхронизируемость, минимальные мощности вершин и др.) описаны в торемах 4 и 5, леммах 1 и 2, следствиях 1 и 2 работы [1]. 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 (БПИ-автомата) $\mathcal{M}$ получены интерпретации величины $d_{\mathcal{M}}$ через слипшиеся состояния автомата $\mathcal{M}$ (лемма 4, [1]) и через минимальный ранг некоторой полугруппы, ассоциированной с автоматом $\mathcal{M}$ (лемма 5, [1]).

Для характеристики процесса обращения конечного БПИ-автомата $\mathcal{M}$ использована теоретико-вероятностная модель конечных цепей Маркова. Показано (лемма 6, [1]), 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 3 ([1]) получены значения $\rho^{\mathcal{M}}$ для случаев $d_{\mathcal{M}} = 1$ и $d_{\mathcal{M}} = \#Q$. Показано также (теорема 9, [1]), 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 [22] был назван локальным обращением.

Для конечного БПИ-автомата Мили $\mathcal{M}$ вводится понятие ассоциированного с ним автомата без выхода $\mathcal{B}(\mathcal{M})$. Доказано (теорема 1, [14]), что приведенный конечный БПИ-автомат Мили $\mathcal{M}$ обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним авто-

мат $\mathcal{B}(\mathcal{M})$ — 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 2, [14]). Содержательный смысл этого утверждения обусловлен отличием параметров локального обращения для этого класса автоматов от параметров, определяемых теоремой 1 ([14]).

Ранее в работе [26] 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 4,5, [14]).

Дискретные совершенно уравновешенные функции над конечным алфавитом A начали систематически исследоваться в работах Г.А. Хедлунда²⁰ и С.Н. Сумарокова²¹. 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. В теореме 2 ([13]) получены необходимые и достаточные условия совершенной уравновешенности сдвиг-композиции пары булевых функций.

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 1, [15]). В теореме 1 ([15]) 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 урав-

²⁰Hedlund G.A. Endomorphism and Automorphism of the Shift Dynamical System. // Math. Systems Th. 3 (1969), pp. 320-375.

²¹Сумароков С.Н. Запреты двоичных функций и обратимость одного класса кодирующих устройств. // Обозрение прикладной и промышленной математики, 1994, № 1, с. 35-55.

новешенная булева функция. По существу, это еще одна теоретико-информационная характеристика класса совершенно уравновешенных функций.

Апробация работы

Результаты работы обсуждались на следующих кафедрах **МГУ имени М.В. Ломоносова**:

Дискретной математики механико-математического факультета,
Математической кибернетики факультета вычислительной математики и кибернетики,
Информационной безопасности факультета вычислительной математики и кибернетики,

и других организациях:

в Лаборатории по математическим проблемам криптографии МГУ имени М.В. Ломоносова,
в Институте проблем информационной безопасности МГУ имени М.В. Ломоносова,
в Институте проблем передачи информации имени А.А. Харкевича РАН,
в Математическом институте имени В.А. Стеклова РАН,
в в/ч 43753,

на конференциях:

Formal Power Series and Algebraic Combinatorics (Moscow, Russia, 2000),
Математика и безопасность информационных технологий (2003, 2004, 2005, 2006, 2009, Москва),
Дискретная математика и ее приложения (2007, Москва),
Boolean Functions in Cryptology and Information Security (Zvenigorod. Russia, 2007),
Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes (Veliko Tarnovo, Bulgaria, 2008),
XVIII Научно-практическая конференция "Комплексная защита информации" (Республика Беларусь, Брест, 2013).

Результаты работы опубликованы 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).

Теоретическая значимость. В ходе исследования получены результаты, существенно развивающие математические модели, используемые при синтезе и анализе средств обеспечения информационной безопасности. Доказанные соотношения, связывающие алгебраические, комбинаторные, спектральные, теоретико-кодвые и криптографические параметры дискретных функций, представляют собой качественное развитие математического аппарата, используемого при синтезе и анализе дискретных функций, являющихся основополагающими элементами средств обеспечения информационной безопасности.

Впервые систематически введена и обоснована координатизация дискретных функций на конечных абелевых группах. Описаны параметры, задающие данную координатизацию, и получены свойства дискретных функций, обобщающие свойства полиномиальных кодов Риды-Маллера. Данная координатизация позволила также описать экстремальные семейства дискретных функций, обобщающих понятие классической бент-функции.

Для дискретных функций на конечных абелевых группах исследовано представление, обобщающее аффинное расщепление булевых отображений. Получены новые соотношения, связывающие параметры данного представления с алгебраическими, комбинаторными и криптографическими параметрами дискретных функций.

Для булевых функций исследованы семейства новых параметров, характеризующих эффективность аффинных аппроксимаций этих функций. Предложена новая нормальная форма булевой функции и получены соотношения, связывающие параметры этой нормальной формы с известными спектральными и криптографическими параметрами соответствующей булевой функции. Предложен и обоснован метод изучения вопросов наследования комбинаторных и спектральных свойств при аффинном сужении булевых функций.

Предложены и обоснованы новые математические модели частичного и локального обращения ограниченно-детерминированных функций. В частности, установлена связь свойства локальной обратимости конечного автомата Мили без потери информации со свойством синхронизируемости ассоциированного с ним автомата без выхода. Описаны новые классы автоматов без потери информации, обладающие свойством локальной обратимости.

Практическая значимость полученных результатов состоит в расширении возможностей разработки методов синтеза и анализа дискретных функций с целью повышения обоснованности оценок уровня защиты информации. Эти результаты могут способствовать выбору параметров дискретных функций, близких к оптимальным, а также использоваться при подготовке учебных пособий и разработке лекционных курсов.

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

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 Риды-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 аналоги 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, связывающие 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 обращения 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) "нелинейной" 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 ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность

- [1] 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 (импакт-фактор Scopus 0,325).
- [2] 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 (импакт-фактор Scopus 0,325).
- [3] Логачев О.А., Яценко В.В. Коды типа Рида-Маллера на конечной абелевой группе. // Проблемы передачи информации, том 34, вып. 2, 1998, с. 32-46 (импакт-фактор Web of Science 0,557).
- [4] 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 (импакт-фактор Web of Science 0,557).
- [5] 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 (импакт-фактор Scopus 0,325).

- [6] Логачев О.А., Сальников А.А., Яценко В.В. Невырожденная нормальная форма булевых функций. // Докл. РАН, том 373, № 2, 2000, с. 164-167 (импакт-фактор Web of Science 0,625).
- [7] 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 (импакт-фактор Scopus 0,325).
- [8] 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 (импакт-фактор Scopus 0,247).
- [9] 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 (импакт-фактор Scopus 0,325).
- [10] Буряков М.Л., Логачев О.А. Об уровне аффинности булевых функций. // Дискр. математика, том 17, вып.4, 2005, с. 98-107 (импакт-фактор Scopus 0,325).
- [11] Логачев О.А. Нижняя граница уровня аффинности для почти всех булевых функций. // Дискр. математика, том 20, вып. 4, 2008, с. 85-88 (импакт-фактор Scopus 0,325).
- [12] Логачев О.А. О значениях уровня аффинности для почти всех булевых функций. // Прикл. дискр. математика, №3, 2010, с. 17-21 (импакт-фактор Scopus 0,265).
- [13] Логачев О.А. Критерий совершенной уравновешенности сдвиг-композиции функций над конечным алфавитом. // Дискретн. математика, том 29, вып. 4, 2017, с. 59-65 (импакт-фактор Scopus 0,325).
- [14] Логачев О.А. О локальной обратимости конечных автоматов без потери информации. // Прикл. дискр. математика, №39, 2018, с. 78-93 (импакт-фактор Scopus 0,265).
- [15] Логачев О.А. Теоретико-информационная характеристика совершенно уравновешенных функций. // Информатика и ее применения, том 12, вып. 4, 2018, с. 70-74 (импакт-фактор Scopus 0,279).
- [16] 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 (импакт-фактор Scopus 0,325).

[17] Логачев О.А., Федоров С.Н., Ященко В.В. О Δ - эквивалентности булевых функций. // Дискретн. математика, том 30, вып. 4, с. 29-40 (импакт-фактор Scopus 0,325).

Другие публикации

[18] 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.

[19] Логачев О.А., Сальников А.А., Ященко В.В. Комбинирующие k -аффин-ные функции. // Математика и безопасность информационных технологий. М.: МЦНМО, 2004, с. 176-178.

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

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