МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

На правах рукописи

Халявин Андрей Вячеславович

# О построении и оценках характеристик корреляционно-иммунных булевых функций и смежных комбинаторных объектов

Специальность 05.13.19 — методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2011

Работа выполнена на Механико-математическом факультете Московского государственного университета имени М. В. Ломоносова.

| | |
|---|---|
| Научный руководитель: | кандидат физико-математических наук, доцент *Таранников Юрий Валерьевич.* |
| Официальные оппоненты: | доктор физико-математических наук *Черемушкин Александр Васильевич*; |
| | кандидат физико-математических наук *Кузнецов Юрий Владимирович.* |
| Ведущая организация: | Институт математики имени С. Л. Соболева СО РАН. |

Защита состоится 28 декабря 2011 г. в 16 час. 45 мин. на заседании диссертационного совета Д 501.002.16 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП-1, Ленинские горы, д. 1, Московский государственный университет имени М. В. Ломоносова, Механико-математический факультет, ауд. 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

Автореферат разослан 28 ноября 2011 г.

Ученый секретарь
диссертационного совета,
доктор физико-математических наук, профессор А. А. Корнев

# Общая характеристика работы

**Актуальность темы.** Стремительное развитие в настоящее время информационных технологий приводит к тому, что защита информации приобретает все большее значение. Основным инструментарием защиты информации является шифрование данных. Качество шифрования определяется его криптографической стойкостью, скоростью шифрования, удобством использования (в частности длиной ключа) и простотой его описания и реализации. Улучшение этих характеристик является одним из направлений совершенствования средств защиты информации.

Криптографическая стойкость определяется вычислительной сложностью наиболее быстрого известного алгоритма ее вскрытия. Адекватность оценки криптографической стойкости определяется наличием большого числа попыток анализа алгоритма шифрования, что в немалой степени зависит от его простоты и распространенности на практике. Последнее же напрямую связано со скоростью и удобством использования алгоритма. По этой причине создание новых шифров является непростой задачей, в которой нужно учитывать сложную взаимосвязь различных факторов. Для решения этой задачи создаются открытые международные конкурсы, призванные найти и стандартизировать наилучшие алгоритмы[1,2].

Большим классом быстрых алгоритмов, которые используются как сами по себе, так и в качестве примитивов (например s-боксов или раундовых преобразований) для более сложных шифров с секретным ключом являются комбинирующие и фильтрующие генераторы. Они преобразуют с помощью некоторой нелинейной булевой функции $f$ выходы регистров сдвига с линейными обратными связями (Linear feedback shift register, LFSR) в шифрующую последовательность. Комбинирующие генераторы подают на входы функции $f$ выходы нескольких LFSR, а фильтрующие генераторы подают на входы $f$ последовательные выходы одного LFSR. Ключом этих систем являются начальные состояния регистров. Анализ этих алгоритмов естественно приводит к необходимости изучения и решения систем булевых уравнений, которые связывают элементы неизвестного ключа с известными данными.

[1]Конкурс eSTREAM (the ECRYPT Stream Cipher Project) призван собрать новые перспективные потоковые шифры.

[2]NIST проводит конкурс на новый государственный стандарт хэширования SHA-3.

Несмотря на то, что общая задача решения системы нелинейных булевых уравнений является $NP$-трудной, разработано большое число статистических, теоретико-вероятностных, теоретико-кодовых, алгебраических и иных подходов, которые позволяют решить задачу быстрее чем за $O(2^n)$ в конкретных частных случаях. Поэтому анализ конкретных систем уравнений является важной и нетривиальной научной задачей. Отсюда следует, что функцию $f$ нельзя выбирать произвольным способом. Например, корреляционная атака накладывает требование высокой корреляционной иммунности, а методы линеаризации накладывают требования высокой нелинейности. Как следствие, возникает естественное желание построить функции, обладающие как можно более лучшими значениями криптографических характеристик и, как следствие, наилучшим образом сопротивляющиеся известным методам криптоанализа. Разумеется, оптимальные значения всех характеристик не могут достигаться одновременно, поэтому при разработке стойких систем шифрования приходится решать трудную многокритериальную оптимизационную задачу выбора булевой фукции $f$. В связи с актуальностью этой задачи, имеется множество работ, устанавливающих или уточняющих соотношения между разными криптографическими параметрами.

**Цель работы** состоит в изучении соотношений между нелинейностью и корреляционной иммунностью булевых функций и построении примеров функций с экстремальными характеристиками исследуемых параметров. Кроме того, доказывается оценка количества элементов в ортогональном массиве большой силы.

**Научная новизна.** Автором разработаны новые эффективные методы построения булевых функций с экстремальными характеристиками. С помощью этих методов получены функции с недостижимыми ранее параметрами. Кроме того, предложен новый подход к исследованию сумм биномиальных коэффициентов, позволяющий улучшить оценку нелинейности корреляционно-иммунных функций. Разработан новый подход к исследованию булевых функций с большой корреляционной иммунностью, который обобщается на ортогональные массивы большой силы и позволяет доказать нижнюю оценку их мощности.

**Теоретическая и практическая ценность.** Полученные результаты отвечают на ряд известных открытых вопросов теории булевых функций о соотношении между нелинейностью и свойствами корреляционной иммунности и устойчивости. В частности, в случае 9 переменных удается доказать равенство верхних и нижних оценок нелинейности. Кроме того, в работе по-

лучены точные нижние оценки на размер ортогональных массивов большой силы.

Построенные примеры булевых функций могут быть использованы в практических шифрах на основе комбинирующих и фильтрующих генераторов. Использованные для построения этих функций методы весьма универсальны и могут быть применены к решению других задач на поиск булевых функций с заданными свойствами.

**На защиту выносятся следующие основные результаты диссертации:**

- Доказана нижняя оценка на количество элементов ортогонального массива, если его сила не меньше $\frac{2n-2}{3}$, где $n$ — число его факторов.

- Найден новый детерменированный метод построения 3-устойчивых булевых функций от 9 переменных с наибольшей возможной нелинейностью 240. Полученные функции обладают симметрией 7 порядка, в то время как ранее известные подходы использовали эвристики и выдавали функции без какой-либо симметрии.

- Впервые построены булевы функции от 9 переменных корреляционно-иммунные 4 порядка с наибольшей возможной нелинейностью 240. С их помощью получены функции от 10 переменных, корреляционно-иммунные 5 порядка с наибольшей возможной нелинейностью 480.

- Показано, что верхняя граница нелинейности $nl(f) \leq 2^{n-1} - 2^m$ для корреляционно-иммунных функций порядка $0 < m < n-1$ от $n$ переменных может достигаться только при $n = 2^{s+1} + 1$, $m = 2^s$ и $n = 2^{s+1} + 2$, $m = 2^s + 1$, где $s \geq 0$, $s \in \mathbb{Z}$.

**Основные методы исследования.** Для построения булевых функций используются свойства коэффициентов Уолша, метод “meet-in-the-middle” и его обобщения. Кроме того, в случае 3-устойчивых функций используется симметрия 7 порядка, а в случае корреляционно-иммунных функций 4 порядка используется решение систем линейных уравнений, связывающих значения булевой функции и коэффициентов Уолша. Нижняя оценка на количество элементов ортогонального массива доказывается с помощью теоремы Титсворта. Верхняя граница нелинейности доказывается с помощью сочетания асимптотических оценок биномиальных коэффициентов и свойств их делимости на степени двойки.

**Апробация результатов.** Результаты диссертации докладывались на X Международном семинаре «Дискретная математика и ее приложения» в Москве (2010), Седьмой общероссийской научной конференции «Математика и безопасность информационных технологий» в Москве (МаБИТ-2008), конференции NATO Information and Communication Security в Звенигороде (2007) и на семинарах кафедры дискретной математики механико-математического факультета МГУ (2007–2010).

**Публикации по теме диссертации.** По теме диссертации опубликовано 5 работ [1–5], две из которых — в печатном издании из перечня ВАК [1,2].

**Личный вклад автора.** Все результаты диссертации были получены автором самостоятельно. Разработаны программы, реализующие описанные в диссертации алгоритмы поиска экстремальных функций.

**Структура диссертации.** Диссертация состоит из введения, 4 глав, заключения и списка литературы, включающего 27 наименований. Объем работы 101 страница.

# Краткое содержание диссертации

**Во введении** описывается взаимосвязь между различными характеристиками булевых функций и приводится обзор результатов исследований по теме диссертации.

**В первой главе** рассматриваются булевы функции с большим порядком корреляционной иммунности. В разделе 1.1 вводятся основные определения. В разделе 1.2 обсуждается вопрос связи корреляционной иммунности и устойчивости. Известно[3], что если порядок корреляционной иммунности $m$ не меньше $\frac{2n-2}{3}$, то булева функция является уравновешенной, а следовательно $m$-устойчивой. В разделе 1.2 приводится известный пример функции с $m = [\frac{2n-1}{3}]$, для которой это утвердение не верно, поэтому эта оценка является точной.

Раздел 1.3 посвящен обобщению этого результата на ортогональные массивы. *Ортогональным массивом* с $N$ строками, $n$ факторами над алфавитом из $s$ символов силы $m$ называется таблица $N \times n$ с элементами из алфавита, в которой при выборе любых $m$ столбцов, любая из $s^m$ комбинаций символов в этих столбцах встречается среди строк одинаковое число раз.

[3]Fon-Der-Flaass D. G., A bound on correlation immunity, Siberian Electronic Mathematical Reports (http://semr.math.nsc.ru), V. 4, 2007, pp. 133–135.

Для ортогональных массивов принято краткое обозначение $OA(N, n, s, m)$. Если все строки массива различны, то он называется *простым*. Поскольку любому простому ортогональному массиву силы $m$ можно сопоставить корреляционно-иммунную функцию порядка $m$, то из этого свойства булевых функций немедленно получается нижняя оценка $2^{n-1}$ мощности простого ортогонального массива. В разделе 1.3 эта оценка обобщается на общий случай не обязательно простых ортогональных массивов. Более того показывается, что если оценка мощности достигается, то ортогональный массив является простым.

**Теорема 1** *Если* $m \geq \dfrac{2n-2}{3}$, *то для* $OA(N, n, 2, m)$ *выполнено* $N \geq 2^{n-1}$. *А если при этом* $N = 2^{n-1}$, *то ортогональный массив является простым.*

Доказательство основано на представлении ортогонального массива как целочисленной функции $x_\alpha = 2n_\alpha - 1$ на булевом кубе, где $n_\alpha$ равно количеству наборов $\alpha$ в ортогональном массиве. Величина $x_\alpha$ может принимать лишь значения $-1, 1, 3, \ldots$ Если ортогональный массив является простым, то $x_\alpha = \pm 1$, что соответствует булевой функции. Для целочисленной функции $x_\alpha$ можно ввести коэффициенты Уолша аналогично булевым функциям: $W_\beta = \sum_\alpha x_\alpha (-1)^{(\alpha,\beta)}$. Для ортогональных массивов силы $m$ выполнено $W_\beta = 0$ при $1 < |\beta| \leq m$.

Коэффициенты Уолша для функции $x_\alpha^2$ вычисляются как свертка $W_\beta$ с самим собой. Поскольку сумма над $Z_2$ двух векторов веса больше $m$ не может быть вектором веса больше $m$, то для коэффициентов Уолша функции $x_\alpha^2$ веса больше $m$ большинство попарных произведений в свертке равны 0 и для них можно получить простое выражение $\frac{W_0}{2^{n-1}} W_\alpha$. Этого оказывается достаточно для вычисления нулевого коэффициента Уолша функции $x_\alpha^3$ и получения равенства

$$\sum_\alpha (x_\alpha^3 - x_\alpha) = \frac{W_0}{2^n} \left( 3\Phi_0 - \frac{2}{2^n} W_0^2 - 2^n \right), \qquad (1)$$

где $\Phi_0 = \sum_\alpha x_\alpha^2$. Исходя из того, что левая часть не отрицательна, удается получить требуемую оценку на $W_0 = 2N - 2^n$ и, как следствие, размер ортогонального массива. В случае $N = 2^{n-1}$ правая часть (1) равна 0 благодаря $W_0 = 0$. Поэтому в этом случае все слагаемые в левой части равны 0, откуда следует простота ортогонального массива.

**Во второй главе** мы переходим к исследованию нелинейности устойчивых функций. Чем больше нелинейность булевой функции, тем труднее

она поддается линейному криптоанализу. Поэтому возникает вопрос о максимальной возможной нелинейности $m$-устойчивой булевой функции. Из равенства Парсеваля следует ограничение $nl(f) \leq 2^{n-1} - 2^{n/2-1}$ на нелинейность любых булевых функций. При $m > n/2 - 2$ это неравенство было усилено до $nl(f) \leq 2^{n-1} - 2^{m+1}$ за счет делимости коэффициентов Уолша $m$-устойчивых булевых функций тремя группами авторов[4,5,6]. Отсюда возникает вопрос, о достижимости этой оценки. Функции, на которых эта оценка достигается, мы будем называть *экстремальными*. У экстремальных функций коэффициенты Уолша принимают значения $\{0, \pm 2^{m+2}\}$. Это свойство оказывается интересным само по себе. Функции, у которых коэффициенты Уолша принимают значения $\{0, \pm 2^k\}$ для некоторого $k$, называют *платовидными*.

В разделе 2.1 приводится актуальное состояние проблемы построения экстремальных функций. Наилучшие теоретические результаты получены с помощью рекурсивных конструкций[7] экстремальных функций для $n-2 \geq m \geq 0.6n - 1$, а доведение этих конструкций до совершенства[8] позволяет получить экстремальные функции с параметрами $n-2 \geq m \geq \frac{1}{\log_2(\sqrt{5}+1)} n + O(\log_2 n)$ (это немного лучше: $\frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$). Как видим, основную сложность представляют случаи $m$ близких к $n/2$. Последующие разделы второй главы посвящены построению функции для случая $n = 9$, $m = 3$, который долгое время оставался открытым. Эти функции уже были получены[9,10] с помощью эвристического поиска, но в данной диссертации приводится совершенно новый способ их построения. Рассматриваются только булевые функции, симметричные относительно циклических перестановок

[4]Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient boolean functions // In Advanced in Cryptology: Eurocrypt 2000, Lecture Notes in Computer Science. — V. 1880. — 2000. — P. 515–532.

[5]Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity // Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/005, March 2000, 18pp.

[6]Zheng Y., Zhang X. M. Improved upper bound on the nonlinearity of high order correlation immune functions // Selected Ares in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science. — V. 2012. — P. 264–274. — Springer-Verlag, 2001.

[7]Tarannikov Yu. New constructions of resilient Boolean functions with maximal nonlinearity, Preproceedings of 8th Fast Software Encryption Workshop, Yokohama, Japan, April 2–4, 2001, pp.70–81, also available at Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/069, December 2000, 11pp.

[8]Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Springer-Verlag, 2001, Lecture Notes In Computer Science, V. 2247, pp. 254–266. Статья также доступна на Cryptology ePrint archive (http://eprint.iacr.org/2001/083), Report 2001/083, 16 pp.

[9]Saber Z.,Faisal Uddin M., Youssef A. On the existance of (9, 3, 5, 240) resilient functions. IEEE Transactions on Information Theory, 52(5):2269-2270, May 2006.

[10]Kavut S., Yucel M., Maitra S. Construction of resilient functions by the concatenation of boolean functions having nonintersecting Walsh spectra. In Third Internation Workshop on Boolean Functions: Cryptography and Applications, BFCA 07, May 2-3, 2007, Pairs, France.

первых 7 переменных, но благодаря этому среди них удается найти все экстремальные функции.

В разделе 2.2 преобразование Уолша записывается с учетом симметрии рассматриваемых функций. Обозначим $c_1, \ldots, c_{80}$ классы эквивалентности булевых наборов длины 9 при циклических перестановках первых 7 координат. Коэффициенты Уолша на наборах из одного класса эквивалентности равны друг другу. Сопоставим функции $f$ столбец $v$, в котором в позиции $i$ стоит 1, если $f(x) = 0, x \in c_i$, и $-1$, если $f(x) = 1, x \in c_i$. Коэффициенты Уолша запишем в столбец $w$, в котором на $i$-й позиции стоит число $W_f(u),\ u \in c_i$. Тогда $w = Av$, где матрица $A$ имеет коэффициенты

$$a_{ij} = \sum_{x \in c_j} (-1)^{<u,x>},$$

где $u \in c_i$. Построенная матрица $A$ обладает важным свойством.

**Теорема 2** *Пусть $c_i$ и $c_j$ — классы эквивалентности, у представителей которых восьмой бит установлен в 0. А $c_{i'}$ и $c_{j'}$ — классы эквивалентности, полученные из $c_i$ и $c_j$ установкой восьмого бита в 1. Тогда $a_{ij} = a_{i'j} = a_{ij'} = -a_{i'j'}$.*

В разделе 2.3 приводится алгоритм нахождения экстремальных функций в нашем классе. Из предыдущей теоремы следует, что матрица $A$ после некоторой перестановки строк и столбцов может быть представлена в виде $\begin{pmatrix} B & B \\ B & -B \end{pmatrix}$. Соответственно вектора значений функций и коэффициентов Уолша можно так же разбить на две части: $w_0 = Bv_0 + Bv_1$ и $w_1 = Bv_0 - Bv_1$. Из 3-устойчивости следует, что координаты $w_i$ делятся на 32, откуда выводится, что координаты $Bv_0$ и $Bv_1$ делятся на 16. Нахождение всех $v_i$ таких, что $Bv_i$ делится на 16 выполняется с помощью дальнейшего деления вектора $v_i$ и матрицы $B$ на две части: $Bv_i = C_0 v_{i0} + C_1 v_{i1}$. Далее перебираются все $2^{20}$ вариантов для $v_{ij}$ и сортируются по остаткам от деления на 16 вектора $C_j v_{ij}$. Дальнейшее нахождение подходящих пар $v_{i0}$, $v_{i1}$ может быть выполнено за линейное время. Остается найти подходящие пары $v_0$ и $v_1$. В разделе 2.3 показывается, что если пара таких векторов дает нужную булеву функцию, то остатки $Bv_0$ и $Bv_1$ по модулю 32 совпадают и у этих векторов не найдется ни одной общей координаты со значением $\pm 32$. Первое условие позволяет разбить вектора $v_i$ на группы в зависимости от остатка $Bv_i$ по модулю 32 и проверять только пары векторов из одной группы. Алгорит-

мы сокращения перебора за счет второго условия приведены в следующем разделе.

Сопоставим вектору $v_i$ маску, в которой единичка стоит на позициях, где координата $Bv_i$ равна $\pm 32$. Получаем, что маски векторов $v_0$ и $v_1$ не должны пересекаться. В разделе 2.4 решается общая задача о поиске не пересекающихся масок. Время работы предложенных алгоритмов оценивается в предположении, что маски имеют равномерные и независимые в совокупности распределения. Первый алгоритм использует разбиение масок по одному биту.

**Теорема 3** *Обозначим $k = n^2\left(\frac{3}{4}\right)^t$ — среднее число пар непересекающихся битовых масок. Тогда существует алгоритм их нахождения, среднее время работы которого равно $O(n^\alpha + k)$ при $n \to \infty$, где $\alpha = \log_2(1+\varphi) = 1.388...$, $\varphi = 1.618...$ — золотое сечение.*

Второй алгоритм использует отделение в отдельные группы масок, у которых $s$ битов все равны 0 или все равны 1.

**Теорема 4** *Для любого $s$ существует алгоритм нахождения всех пар непересекающихся масок, который работает в среднем (предполагая, что все маски равновероятны) за $O(n^\alpha + n^2\beta^{t/s})$ действий, где $\beta = 1 - 2\cdot 2^{-s} + 3\cdot 2^{-2s}$, $\alpha = 1 + 1/s$, $|A| \le n$, $|B| \le n$.*

В разделе 2.5 приводится статистика по 423634 построенным функциям. Особое внимание уделяется функциям, которые разбиваются на две 3-устойчивые подфункции от 8 переменных. Из таких функций можно построить целую серию экстремальных функций[11].

**Теорема 5** *Существуют булевы функции от $n = 9 + 3i$ переменных устойчивые порядка $m = 3 + 2i$ с нелинейностью $2^{n-1} - 2^{m+1}$ при $i \ge 0$.*

**В третьей главе** исследуется максимальная возможная нелинейность корреляционно-иммунных функций. В разделе 3.1 приводится оценка их нелинейности $nl(f) \le 2^{n-1} - 2^m$. Если эта оценка при некоторых $n$ и $m$ не достигается, то выполнено $nl(f) \le 2^{n-1} - 2^{m+1}$, что совпадает с оценкой нелинейности $m$-устойчивых функций. Поэтому случай $nl(f) = 2^{n-1} - 2^m$,

[11]Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune boolean functions achieving upper bounds on nonlinearity, Workshop on Coding and Cryptography - WCC 2001, Paris, January 8–12, 2001, Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

при котором эти оценки различаются, представляет особый интерес. Функции с такими параметрами будем также называть экстремальными. Последующие разделы посвящены решению открытой проблемы построения корреляционно-иммунной функции с параметрами $n = 9$, $m = 4$, $nl(f) = 2^8 - 2^4 = 240$.

В разделе 3.2 изучаются коэффициенты Уолша этих экстремальных функций. Показывается, что $W_f(u) = 0$ для векторов $u$ веса $1, 2, 3, 4$ и $9$. Остальные коэффициенты Уолша равны $\pm 32$, при этом их значения определяются знаками коэффициентов Уолша на векторах веса 0 и 5.

В разделе 3.3 приводится алгоритм перебора знаков ненулевых коэффициентов Уолша. Все коэффициенты разбиваются на 4 части в зависимости от значений двух последних битов: $W_{00}$, $W_{01}$, $W_{10}$, $W_{11}$. Для каждой из частей можно вычислить соответствующие обратные преобразования Уолша $F_{00}$, $F_{01}$, $F_{10}$, $F_{11}$. Эти обратные преобразования нормированы так, чтобы $F(x, i, j) = \sum_{a,b} F_{ab}(x)(-1)^{a \cdot i + b \cdot j} = \pm 16$, где 16 соответствует нулевым значениям функции $f$, а $-16$ — единичным. В таком случае координаты $F_{ab}$ должны принадлежать множеству $\{0, \pm 8, \pm 16\}$.

Перебор части $W_{00}$ может быть значительно сокращен за счет симметрий множества экстремальных функций. Эти симметрии порождаются преобразованиями четырех типов. Первый тип — смена знаков у всех коэффициентов Уолша или переход от функции к ее отрицанию. Второй тип — смена знаков у всех коэффициентов Уолша с установленным $i$-м битом или сдвиг функции вдоль $i$-го аргумента. Третий тип — перестановка коэффициентов Уолша, порожденная перестановкой аргументов функции. Четвертый тип — преобразование

$$W'(u_1, \ldots, u_9) = W(u_1 \oplus u_i, u_2 \oplus u_i, \ldots, u_i, \ldots, u_9 \oplus u_i).$$

Использование этих симметрий позволяет сократить перебор комбинаций знаков в $W_{00}$ и свести все возможные подходящие варианты к 5 комбинациям.

Сдвиг функции вдоль 8-го и 9-го аргументов позволяет сократить перебор знаков в $W_{01}$ и $W_{10}$ вдвое. Кроме того, показывается, что из этих вариантов можно исключить все случаи, где $F_{00}$ и $F_{01}$ имеют различные остатки от деления на 16 или имеют общие координаты со значениями $\pm 16$. Полный перебор показывает, что количество подходящих вариантов для $W_{01}$ и $W_{10}$ заключено от 10 до 16 миллионов для каждой из 5 комбинаций $W_{00}$.

Наконец, перебор последней части $W_{11}$ выполняется с помощью решения

системы линейных уравнений. Для каждого из вариантов $W_{00}$, $W_{01}$ и $W_{10}$ есть около 90 координат $F_{11}(x)$, которые однозначно определяются из условия $F(x,i,j) = \pm 16$. В результате получается система линейных уравнений на ненулевые коэффициенты Уолша, которая имеет лишь небольшое число свободных переменных. Все возможные значения свободных переменных проверяются перебором.

В конце раздела 3.3 доказывается, что среди экстремальных функций нет функций, симметричных относительно перестановки двух переменных, и приводится формула построения экстремальных функций с параметрами $n = 10$, $m = 5$ из экстремальных функций с параметрами $n = 9$, $m = 4$:

$$g(x_1, \ldots, x_{10}) = f(x_1 \oplus x_{10}, x_2 \oplus x_{10}, \ldots, x_9 \oplus x_{10}).$$

**В четвертой главе** исследуется достижимость оценки нелинейности $nl(f) \le 2^{n-1} - 2^m$ для корреляционно-иммунных функций для всех параметров $n$ и $m$.

В разделе 4.1 приводятся известные свойства коэффициентов Уолша экстремальных функций. Основное их свойство описывается следующей теоремой.

**Теорема 6** *Если корреляционно-иммунная порядка $m$ булева функция $f$ от $n$ переменных, $m \le n-2$, имеет нелинейность $2^{n-1} - 2^m$, то для любого $u \in F_2^n$ выполнено*

$$W_f(u) \equiv \pi_{wt(u)} 2^{m+1} \pmod{2^{m+2}},$$

*где $\pi_0 = 1$, $\pi_1 = \pi_2 = \cdots = \pi_m = 0$, $\pi_i = \sum_{j=0}^{i-1} \pi_j \binom{i}{j} \pmod 2$, $\pi_i \in \{0,1\}$ при $i > m$.*

Это свойство позволяет получить условие на параметры $n$ и $m$.

**Теорема 7** *Если существует корреляционно-иммунная булева функция $f$ порядка $m$ от $n$ переменных, $m \le n-2$, с нелинейностью $2^{n-1} - 2^m$, то выполнено*

$$\sum_{j=0}^{n} \binom{n}{j} \pi_j = 2^{2n-2m-2}. \tag{2}$$

Нахождение всех пар $n$ и $m$, удовлетворяющих этому уравнению, является основной задачей последующих разделов.

В разделе 4.2 вводятся обозначения и доказываются утверждения необходимые для эффективной работы с остатками биномиальных коэффициентов по модулям степеней двойки. Обозначим $F(1) = 1$, $F(x) = \prod_{i=1}^{x-1}(2i+1)$ при $x > 1$, $F(x) = 1/\prod_{i=x}^{0}(2i+1)$ при $x \le 0$. Эта функция равна $F(x) = 2x!/x!$ при $x \ge 0$. Введем функцию $G(x,y) = \frac{F(x)}{F(y)F(x-y)}$. Тогда выполнена следующая теорема.

**Теорема 8** $\binom{2n+a}{2m+b} \equiv \binom{n}{m} H((2n+a) \bmod 2^k, (2m+b) \bmod 2^k) \pmod{2^k}$, *где* $a, b \in \{0,1\}$, $H(2x,2y) = G(x,y)$, $H(2x+1,2y) = G(x,y)\frac{2x+1}{2x-2y+1}$, $H(2x,2y+1) = G(x,y)\frac{2x-2y}{2y+1}$, $H(2x+1,2y+1) = G(x,y)\frac{2x+1}{2y+1}$.

Обозначим $M_k$ матрицу значений функции $H$ по модулю $2^k$:

$$M_k = \begin{bmatrix} H(0,0) \bmod 2^k & \cdots & H(0,2^k-1) \bmod 2^k \\ \vdots & \ddots & \vdots \\ H(2^k-1,0) \bmod 2^k & \cdots & H(2^k-1,2^k-1) \bmod 2^k \end{bmatrix}.$$

Элемент этой матрицы в $i+1$ строке и $j+1$ столбце будем записывать как $M_k(i,j) = H(i,j) \bmod 2^k$. Пусть $wa = a_{s-1}\ldots a_1 a_0$ и $wb = b_{s-1}\ldots b_1 b_0$ — два двоичных слова. Обозначим $\Pi_k(wa,wb) = \prod_{i=0}^{s-k} M_k\left(\sum_{j=0}^{k-1} a_{i+j}2^j, \sum_{j=0}^{k-1} b_{i+j}2^j\right)$. Тогда для чисел $a = \sum_{j=0}^{s-1} a_j 2^j$ и $b = \sum_{j=0}^{s-1} b_j 2^j$ остаток биномиального коэффициента по модулю $2^k$ можно выразить через $\Pi_k$.

**Лемма 4** $\binom{b}{a} \equiv \Pi_k(wb,wa)\binom{\sum_{j=0}^{k-2} b_{s-k+1+j}2^j}{\sum_{j=0}^{k-2} a_{s-k+1+j}2^j} \pmod{2^k}$.

Для каждой матрицы $M = \{m_{ij}\}$ размера $2^k \times 2^k$ введем функцию $M(wa,wb) = m_{1+[a/2^{s-k}],1+[b/2^{s-k}]}$. Аналогично для строки или столбца $\{m_i\}$ размера $2^k$ введем функцию $M(wa) = m_{1+[a/2^{s-k}]}$. Определим семейство матриц

$$M_k^* = \begin{bmatrix} \binom{0}{0} & \cdots & \binom{0}{2^k-1} \\ \vdots & \ddots & \vdots \\ \binom{2^k-1}{0} & \cdots & \binom{2^k-1}{2^k-1} \end{bmatrix}.$$

Тогда биномиальные коэффициенты по модулю $2^k$ можно полностью выразить через функции от их двоичных записей:

$$\binom{b}{a} \equiv \Pi_k(wb,wa) M_{k-1}^*(wb,wa) \pmod{2^k}$$

Следующий раздел 4.3 посвящен использованию этой формулы для исследования уравнения (2) по модулю $2^k$. Но для этого вначале выводится

формула для чисел $\pi_i$.

**Лемма 6** *При $i > m$ выполнено*

$$\pi_i \equiv \binom{i-1}{m} \pmod 2.$$

Благодаря этому сравнению уравнение (2) преобразуется к виду

$$1 + \sum_{i,\binom{i}{m}\equiv 1 (\mathrm{mod}\ 2)} \binom{n}{i+1} = 2^{2n-2m-2}. \tag{3}$$

Теперь уже легко увидеть, что это уравнение выполнено на двух сериях значений.

**Лемма 7** *Равенство* (3) *верно при $n = 2^{s+1}+1,\ m = 2^s$ и $n = 2^{s+1}+2,\ m = 2^s+1$, где $s \geq 0$.*

Оставшаяся часть главы 4 посвящена доказательству обратного факта. Обозначим отношение мажорирования символом $\preceq$, а длину слова $w$ как $|w|$. Исходя из формулы биномиальных коэффициентов по модулю 2 и выражения биномиальных коэффициентов через функции от их двоичных записей, левая часть уравнения преобразуется к виду

$$1 + \sum_{i,\binom{i}{m}\equiv 1 (\mathrm{mod}\ 2)} \binom{n}{i+1} \equiv$$

$$1 + \sum_{wi \neq 11\ldots1, wm \preceq wi} \Pi_k(wn, wi+1) M^*_{k-1}(wn, wi+1) \pmod{2^k},$$

где $wm$ и $wn$ — двоичные записи $n$ и $m$, а под $wi+1$ понимается слово той же длины, представляющее двоичную запись числа $i+1 \pmod{2^{|w|}}$. Далее доказывается ряд лемм о суммах вида $\sum_{wi \neq 11\ldots1, wm \preceq wi} \Pi_k(wn, wi+1) M(wn, wi+1)$ по модулю $2^k$ для различных $k$, матриц $M$ и ограничений на слова $wn$ и $wm$. Их доказательство основано на разбиении суммы на две части в зависимости от старшего бита $wi$ и последующего их упрощения. С помощью этих лемм удается доказать три теоремы на свойства нужных нам сумм биномиальных коэффициентов.

**Теорема 9** *Пусть для некоторых непустых слов $w_1$ и $w_2$ выполнено $wm =$*

$10w_1$, $wn = 11w_2$ *и* $\overline{w_2} > \overline{w_1}$ *или* $wm = 01w_1$, $wn = 10w_2$ *и* $\overline{w_2} \le \overline{w_1}$, *тогда*

$$1 + \sum_{wi \neq 11\ldots1, wm \preceq wi} \Pi_2(wn, wi+1) M_1^*(wn, wi+1) \equiv 2 \pmod 4.$$

**Теорема 10** *Пусть для некоторых непустых слов* $w_1$ *и* $w_2$ *выполнено* $wm = 010^t0w_1$, $wn = 100^t1w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2}$, $t \ge 0$ *или* $wm = 01w_1$, $wn = 11w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \le \overline{w_1}$ , *тогда*

$$1 + \sum_{wi \neq 11\ldots1, wm \preceq wi} \Pi_3(wn, wi+1) M_2^*(wn, wi+1) \equiv 4 \pmod 8.$$

**Теорема 11** *Пусть для некоторых непустых слов* $w_1$ *и* $w_2$ *выполнено* $wm = 011w_1$, $wn = 110w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \le \overline{w_1}$ *или* $wm = 010^t01w_1$, $wn = 100^t10w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \le \overline{w_1}$, $t \ge 0$ *или* $wm = 010^t100w_1$, $wn = 100^t111w_2$, $\overline{w_2} > \overline{w_1}$, $t \ge 0$, *тогда*

$$1 + \sum_{wi \neq 11\ldots1, wm \preceq wi} \Pi_4(wn, wi+1) M_3^*(wn, wi+1) \equiv 8 \pmod{16}.$$

Каждая из теорем утверждает, что в некоторой области значений $n$ и $m$ сумма биномиальных коэффициентов не может делится на большую степень двойки.

В разделе 4.4 полученные теоремы сравниваются с результатами, полученными на основе оценок биномиальных коэффициентов. В предыдущих работах с помощью этих оценок получено сильное ограничение[12] на значения $n$ и $m$.

**Теорема 12** *При* $n \ge 12$ *выполнение* (3) *влечет*

$$\frac{n}{2} + \frac{1}{2}\log_2 n + \frac{1}{2}\log_2\left(\frac{\pi}{2}e^{8/9}\right) - 1 > m \ge \frac{n-1}{2}.$$

Вычисления показывают, что $\frac{1}{2}\log_2\left(\frac{\pi}{2}e^{8/9}\right) = 0.9669\ldots < 1$, поэтому мы будем пользоваться оценкой $\frac{n}{2} + \frac{1}{2}\log_2 n > m$. Сравнение этой оценки с результатами предыдущего раздела позволяет исключить некоторые значения $n$.

**Лемма 20** *Если* $n \ge 32$, *то двоичная запись* $n$ *не начинается с* 11.

[12]Ботев А. А. О соотношениях между корреляционной иммунностью, нелинейностью и весом для неуравновешенных булевых функций, Математические вопросы кибернетики, Вып. 11, М., Физматлит, 2002, с. 149–162.

Пусть $2^{p-1} \le n < 2^p$. Далее будем рассматривать лишь случай $p \ge 6$. Тогда из теорем раздела 4.3 следует оценка на $m$ снизу.

**Лемма 21** *Пусть* $n = \overline{10^k 1 w_2} = 2^{s+k+1} + 2^s + \overline{w_2}$, $|w_2| = s \ge 3$, $k \ge 1$. *Тогда* $m \ge \frac{n}{2} + 2^{s-3}$.

Получается, что чем дальше $n$ от $2^{p-1}$, тем больше должна быть разница между $m$ и $n/2$. Но, начиная с некоторого момента, это противоречит нашей верхней границе $\frac{n}{2} + \frac{1}{2}\log_2 n > m$. Это позволяет ограничить $n$ значениями, близкими к $2^{p-1}$.

**Лемма 22** *Выполнены неравенства*

$$2^{p-1} \le n < 2^{p-1} + 8p,$$

$$2^{p-2} \le m < 2^{p-2} + \frac{9}{2}p,$$

$$m < 2^{p-1}.$$

С другой стороны, для значений $n$ и $m$, близких к $2^{p-1}$ и $2^{p-2}$ соответственно, можно улучшить оценки на суммы биномиальных коэффициентов. Для оценки суммы биномиальных коэффициентов снизу с учетом доказанных ограничений на $n$ и $m$ получается следующий результат.

**Лемма 23** *Пусть* $m = \overline{10^k w_1}$, $|w_1| = t$, $k \ge 0$, $z$ — *число нулей в слове* $w_1$, $p \ge 9$, *тогда*

$$1 + \sum_{i, \binom{i}{m} \equiv 1 (\mathrm{mod}\ 2)} \binom{n}{i+1} > 2^{n-t-2+z}.$$

Этого неравенства оказывается достаточно для улучшения оценок на $n$ и $m$ до конечной области при фиксированном $p$.

**Лемма 24** *Пусть* $p \ge 9$, *тогда*

$$2^{p-1} \le n < 2^{p-1} + 16,$$

$$2^{p-2} \le m < 2^{p-2} + 8.$$

Дальнейшее сокращение этой области возможно с помощью оценки суммы биномиальных коэффициентов сверху.

**Лемма 25** *Пусть* $p \ge 9$, $m = \overline{10^k w_1}$, $|w_1| = t \le 3$, $z$ — *число нулей в*

*слове* $w_1$. *Тогда выполнено*

$$1 + \sum_{i,\binom{i}{m} \equiv 1 (\mathrm{mod}\ 2)} \binom{n}{i+1} < 2^{n-t+z}.$$

Вместе с оценкой снизу, это позволяет получить соотношение между $n$ и $m$.

**Лемма 26** *Пусть* $p \geq 9$, *тогда* $m = \overline{10^k w_1}$, $|w_1| = t \leq 3$ *и* $n = 2m - t + z + 1$, *где* $z$ — *число нулей в слове* $w_1$.

Далее показывается, что если $m$ четно, то уравнение для пары $n$ и $m$ выполнено тогда и только тогда, когда оно выполнено для пары $n+1$ и $m+1$. Отсюда следует, что достаточно исследовать пары с нечетным $m$. С учетом полученных ограничений на $n$ и $m$ остается лишь три серии значений: $(2^{p-1}+5, 2^{p-2}+3)$, $(2^{p-1}+9, 2^{p-2}+5)$, $(2^{p-1}+12, 2^{p-2}+7)$. Первые две из них откидываются с помощью теорем из раздела 4.3.

Последний случай рассматривается в следующем разделе 4.5 с помощью рассуждений, аналогичных рассуждениям в разделе 4.3.

**Теорема 13** *Пусть* $wm = 010^k111$, $wn = 10^k1100$, *тогда*

$$1 + \sum_{wi \neq 11\ldots1, wm \preceq wi} \Pi_3(wn, wi+1) M_2^*(wn, wi+1) \equiv 4 \pmod 8.$$

Отсюда выводится основной результат, описывающий все решения уравнения (2) при $n \geq 512$.

**Теорема 14** *Если* $n \geq 512$, $0 < m < n-1$ *и пара* $n$, $m$ *не принадлежит сериям* $m = 2^s$, $n = 2^{s+1}+1$ *и* $m = 2^s+1$, $n = 2^{s+1}+2$ *при* $s \geq 8$, *то для всех корреляционно-иммунных порядка* $m$ *булевых функций* $f$ *от* $n$ *переменных выполнено неравенство*

$$nl(f) \leq 2^{n-1} - 2^{m+1}.$$

Для меньших значений $n$ уравнение (2) непосредственно проверено на компьютере, что позволяет избавится от условия $n \geq 512$ в предыдущей теореме.

**Следствие 1** *Если пара* $n$, $m$, $0 < m < n-1$ *не принадлежит сериям* $m = 2^s$, $n = 2^{s+1}+1$ *и* $m = 2^s+1$, $n = 2^{s+1}+2$ *при* $s \geq 0$, *то для всех*

*корреляционно-иммунных порядка $m$ булевых функций $f$ от $n$ переменных выполнено неравенство*

$$nl(f) \leq 2^{n-1} - 2^{m+1}.$$

**В заключении** приведены основные результаты диссертации.

1. Доказана нижняя оценка на количество элементов ортогонального массива, если его сила не меньше $\frac{2n-2}{3}$, где $n$ — число его факторов.

2. Найден новый детерменированный метод построения 3-устойчивых булевых функций от 9 переменных с наибольшей возможной нелинейностью 240. Полученные функции обладают симметрией 7 порядка, в то время как ранее известные подходы использовали эвристики и выдавали функции без какой-либо симметрии.

3. Впервые построены булевы функции от 9 переменных корреляционно-имунные 4 порядка с наибольшей возможной нелинейностью 240. С их помощью получены функции от 10 переменных, корреляционно-иммунные 5 порядка с наибольшей возможной нелинейностью 480.

4. Показано, что верхняя граница нелинейности $nl(f) \leq 2^{n-1} - 2^m$ для корреляционно-иммунных функций порядка $0 < m < n - 1$ от $n$ переменных может достигаться только при $n = 2^{s+1} + 1$, $m = 2^s$ и $n = 2^{s+1} + 2$, $m = 2^s + 1$, где $s \geq 0$, $s \in \mathbb{Z}$.

**Благодарности.** Автор выражает глубокую благодарность и признательность научному руководителю Юрию Валерьевичу Таранникову за постановку задач и внимание к работе. Автор также благодарит сотрудников кафедры дискретной математики Московского Государственного Университета им М. В. Ломоносова и Валерия Александровича Васенина за поддержку и высказанные замечания.

# Список литературы

[1] Халявин А. В. Оценка мощности ортогональных массивов большой силы. // Вестник Московского университета. Серия 1, Математика. Механика. 2010. №3. — с. 49–51.

[2] Халявин А. В. Оценка нелинейности корреляционно-иммунных булевых функций, Прикладная дискретная математика, №1 (11), 2011, с. 34–69.

[3] Халявин А. В. Построение 4 корреляционно-иммунных булевых функций от 9 переменных с нелинейностью 240. // Материалы X Международного семинара «Дискретная математика и ее приложения». Москва, МГУ, 1-6 февраля 2010г. — М.: Изд-во механико-математического факультета МГУ, 2010, 549с. — с. 534.

[4] Халявин А. В. Неравенства для ортогональных массивов большой силы // Материалы Четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. Московский Государственный Университет им. М. В. Ломоносова, 30-31 октября 2008г. Том 2, Материалы Седьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008). — М.: МЦНМО, 2009. — 280с. — с. 33.

[5] Khalyavin A. Constructing boolean functions with extremal properties. // Boolean functions in cryptology and information security. — 2008. — IOS Press. — P. 289–295. (NATO Science for Peace and Security Series D: Information and Communication Security — Vol. 18)