

ОБ АННИГИЛЯТОРАХ БУЛЕВЫХ ПОЛИНОМОВ

В. К. Леонтьев^{1,2,a}, Э. Н. Гордеев^{2,b}

¹ Вычислительный центр им. А. А. Дородницына ФИЦ ИУ РАН,
ул. Вавилова, 42, 119991 Москва, Россия

² Московский государственный технический университет им. Н. Э. Баумана,
2-я Бауманская ул., 5, 105005 Москва, Россия

E-mail: ^a vkleontiev@yandex.ru, ^b werhorn@yandex.ru

Аннотация. Булевы функции вообще и булевы полиномы (полиномы Жегалкина, алгебраические нормальные формы (АНФ)), в частности, — предмет теоретических и прикладных исследований в различных областях информатики. В работе рассматриваются линейные преобразования пространства булевых полиномов от n переменных, одним из следствий которых является получение результатов, касающихся проблемы нахождения минимальной степени аннигилятора для заданного булева полинома. Эта задача является актуальной в различных аналитических и алгоритмических аспектах криптографии. Булевы полиномы и их комбинаторные свойства изучаются в дискретном анализе. Теоретические основы информационной безопасности включают изучение свойств булевых полиномов в связи с вопросами криптографии. В работе доказана теорема о минимальной степени аннигилятора. Описан класс булевых полиномов, для которых степень аннигилятора не превосходит единицы. Приведён ряд комбинаторных характеристик, связанных со свойствами пространства булевых полиномов. Даны оценки минимальной степени аннигилятора. Рассмотрен случай симметрических полиномов. Библиогр. 26.

Ключевые слова: булев полином, симметрический полином, аннигилятор, линейное преобразование, криптосистема.

Исследование выполнено при финансовой поддержке Министерства науки и высшего образования РФ (госзадание № 0063–2016–0003) и Российского фонда фундаментальных исследований (проект № 17–01–00300).

© В. К. Леонтьев, Э. Н. Гордеев, 2020

Введение

Пусть $B = \{0, 1\}$, B^n — n -мерный булев куб, $g(x): B^n \rightarrow B$ — булева функция в базисе $\{1, \wedge, \oplus\}$. Как обычно, $\|x\|$ — норма булевого вектора — это его вес Хэмминга, т. е. число единиц в этом векторе.

Пусть $F_2 = \{0, 1\}$ — поле Галуа и $F_2[x_1, \dots, x_n]$ — кольцо полиномов от n переменных над F_2 . Если профакторизовать это кольцо по модулю идеала $I = (x_1 + x_1^2, x_2 + x_2^2, \dots, x_n + x_n^2)$, то получится кольцо $P_2^n[x] = F_2[x_1, \dots, x_n]/I$ булевых полиномов с обычными операциями сложения и умножения и равенствами $x_i = x_i^2$, $i = 1, \dots, n$. Оно является стандартным объектом в теории кодирования, дискретном анализе и криптографии.

Каждый элемент кольца $P_2^n[x]$ вида x^w называется мономом, а вес Хэмминга $\|w\|$ — степенью монома x^w .

Упорядочим все мономы по степени, а внутри множества мономов одной степени — лексикографически. Тогда получим следующее подмножество R_n кольца $P_2^n[x]$:

$$R_n = \{1, x_1, x_2, \dots, x_n, x_1x_2, \dots, x_{n-1}x_n, \dots, x_1x_2 \dots x_n\}. \quad (1)$$

Очевидно, что R_n — коммутативный моноид относительно умножения и $|R_n| = 2^n$.

Любой элемент кольца $g(x)$ можно представить в виде

$$g(x) = \sum_{w \in B^n} c_w x^w, \quad (2)$$

где

$$c_w \in B, \quad w = (w_1, \dots, w_n) \in B^n, \quad x^w = x_1^{w_1} \dots x_n^{w_n},$$

$$x_k^{w_k} = \begin{cases} x_k, & \text{если } w_k = 1, \\ 1, & \text{если } w_k = 0. \end{cases}$$

Представление (2) называется булевым полиномом, или полиномом Жегалкина, или алгебраической нормальной формой (АНФ). Здесь конъюнкция x^w будет мономом, а число $\deg x^w = \sum_{k=1}^n w_k$ — степенью этого монома. Степенью всего полинома $g(x)$ будет число $\deg g(x) = \max_{c_w=1} \deg x^w$.

Если двоичные векторы w полинома $g(x)$ записать в виде матрицы, то получим матрицу M_g мономов полинома $g(x)$. (Если мономы сначала упорядочены по длине, а мономы одинаковой длины — лексикографически, то получим однозначное отображение множества булевых полиномов в множество матриц мономов.)

Задача поиска аннигиляторов булевых функций долгое время привлекала незначительное внимание специалистов в области дискретной

математики. В то же время многие свойства булевых функций применялись при конструкции систем защиты информации. Например, булевы функции давно используются в потоковых шифрах в качестве нелинейных фильтров, а также они применяются в блочных шифрах в S-блоках.

Требование устойчивости криптографических систем к атакам разного вида приводит к тому, что в них используются булевы функции с определёнными свойствами. Конечно, эти свойства зависят от принципов построения самих конструкций. Например, требуемые свойства булевых функций, используемых в качестве нелинейных фильтров, характеризуются ограничениями на алгебраическую иммунность и нелинейность высоких порядков.

Перечень подобных требований, их значение и взаимосвязи можно найти в учебниках по криптографии, например, в [1]. Алгебраическая иммунность задаётся минимальной степенью аннигилятора. Поэтому результаты, которые в дискретном анализе касались значения или оценок минимальной степени аннигилятора, в криптоанализе можно интерпретировать как исследование алгебраической иммунности.

Важным прогрессом в области разработки теоретических основ упомянутых выше систем, достигнутым в 2003 г., стало введение Куртуа и Майером понятий алгебраических атак и быстрых алгебраических атак, которые являются очень мощными концепциями анализа и могут применяться ко многим алгоритмам. Для изучения устойчивости к алгебраическим атакам и было введено понятие алгебраической иммунности.

В 2003 г. появилась работа [2], в которой была предложена точная нижняя оценка нелинейности (первого порядка) через значение алгебраической иммунности функции. Значение её в том, что для алгебраической иммунности функции уже тогда было предложено несколько алгоритмов, а для подсчёта нелинейности высоких порядков эффективных алгоритмов не существовало. Это обусловило интерес разработчиков прикладных систем в этой области к результатам дискретного анализа, а специалисты в последней области обратили внимание на прикладные аспекты своей деятельности.

С тех пор в этой области исследований можно условно выделить три главных направления, которые, опять-таки условно, можно обозначить следующим образом.

1. Работы математиков, специалистов по дискретному анализу, в которых ищутся в прикладных системах, описанных выше, обоснования постановкам чисто «теоретических» задач.

2. Работы, где математики пытаются найти связь между разными прикладными областями, которые базируются на одной теоретической основе.

3. Разработки специальных прикладных криптографических систем с привлечением результатов из различных областей дискретного анализа для получения новых свойств этих систем или оценки их эффективности.

Примером первого направления может служить работа [3], где получена новая верхняя граница вероятности ошибки блока после декодирования по каналу со стиранием. Оценка работает для всех линейных кодов и выражена в терминах обобщённых весов Хэмминга. Это оказывается весьма полезным для кодов Рида — Маллера, для которых известны все обобщённые веса Хэмминга, тогда как полное распределение весов известно лишь частично. Для этих кодов вероятность ошибки дана в связи с понятием алгебраической иммунности. Далее с использованием этой оценки решается уже другая задача: находится алгебраическая иммунность и её асимптотика для случайной «сбалансированной» булевой функции.

В [4] несколькими способами обобщается понятие алгебраической иммунности булевых функций на вектор-функции над произвольными конечными полями и получены верхние оценки для такой обобщённой алгебраической иммунности. Доказано, что верхние границы могут быть достигнуты с использованием свойств кодов Рида — Маллера.

Направление исследований работы [3] продолжается, например, в [5]. Эта статья расширяет результат [3] по алгебраической иммунности случайных сбалансированных булевых функций на асимптотическую нижнюю границу алгебраической иммунности специального класса функций (random balanced Boolean functions).

Примерами результатов во втором направлении служит цикл работ М. С. Лобанова [6–8]. В [6] предложен новый подход к получению для булевой функции как можно более сильных нижних оценок её нелинейности высоких порядков через значение алгебраической иммунности. Проблема сведена к оценке размерности определённых линейных подпространств в пространстве всех булевых функций фиксированного числа переменных. Приведена универсальная оценка нелинейности r -го порядка через значение алгебраической иммунности функции. Эта оценка является точной в том смысле, что для любых допустимых значений параметров существует функция, достигающая оценки.

Здесь можно отметить и работу В. К. Леонтьева [9], где получены формулы для вычисления степени аннигилятора произвольного булева полинома, а следовательно, и его алгебраической иммунности. Проблема сведена к построению и анализу определённых линейных подпространств над пространством булевых функций фиксированного числа переменных.

Достаточно полную картину деятельности в этой области (до 2008 г.) можно найти в обзорной работе М. Э. Тужилина [10].

В статье [11] в определённом смысле улучшены некоторые известные нижние оценки нелинейности r -го порядка булевой функции с заданной алгебраической иммунностью. Это достигается за счёт того, что вводится понятие дополнительной алгебраической иммунности, а её значение может быть вычислено как часть вычисления алгебраической иммунности без изменения вычислительной сложности.

В работе [12] доказывается новая нижняя граница для профиля нелинейности r -го порядка булевых функций с учётом их алгебраической иммунности, которая значительно улучшается для одной из этих нижних оценок для всех порядков, а для другой — для низких порядков.

В [13] используется параметр, введенный Лю и соавторами, называемый быстрой алгебраической иммунностью (fast algebraic immunity), в качестве инструмента для измерения устойчивости системы кодирования, построенной на основе булевых полиномов, к быстрым алгебраическим атакам. Доказана верхняя оценка значения быстрой алгебраической иммунности, с использованием которой установлена слабость обратных функций следа (trace inverse functions) против быстрых алгебраических атак.

Примерами работ в третьем направлении являются статьи, где строятся булевы функции, максимально пригодные для «хороших» (обладающих оптимальными с точки зрения критериев, предъявляемых к специального рода системам кодирования, характеристиками) конструкций систем защиты информации.

В работе [14] изучается понятие нелинейности эквивалентности булевых функций, при которой многие прикладные свойства не являются инвариантными среди функций в пределах одного и того же класса эквивалентности. Обсуждается количество булевых функций в каждом классе эквивалентности и исследуются их свойства, в том числе алгебраическая иммунность, алгебраическая степень, нелинейность классов эквивалентности и др. Описываются классы эквивалентности с «хорошими» характеристиками и методы построения таких классов.

Известно, что булевы функции, используемые в потоковых и блочных конструкциях кодирования, должны обладать большой алгебраической иммунностью, чтобы противостоять алгебраическим атакам, поэтому активно изучаются конструкции таких функций. Например, в [15] предлагаются несколько конструкций симметричных булевых полиномов с нечётным числом переменных (rotation symmetric Boolean functions) с максимальной алгебраической иммунностью. Это направление продолжается в работах [16, 17], а также [18].

В статье [19] строятся модификации известной функции HWBF (hidden weighted bit function), введенной Брайантом в 1991 г. Новые функции сбалансированы, обладают почти оптимальной алгебраической степенью

и удовлетворяют строгому лавинному критерию. Исследуется их алгебраическая иммунность, размер BDD и другие актуальные прикладные свойства.

Аннигиляторы симметрических полиномов в связи с алгебраической иммунностью и построением «хороших» криптографических конструкций изучаются во многих работах. В качестве примеров можно привести работы [20, 21]. В то же время в [22] изучаются симметрические булевы полиномы с чётным и нечётным числом неизвестных. Для построения булевых функций, «хороших» для специализированных систем кодирования, используется теоретико-числовая техника. Построены классы полиномов с оптимальными, в каком-то смысле, характеристиками: алгебраической иммунностью, степенью и пр.

Всё сказанное выше объясняет актуальность и тематику данной работы. С точки зрения приведённой классификации, кроме уже упомянутых, результаты авторов, принадлежащие к первым двум направлениям, приведены также в работах [23–26].

Хотя данная статья носит преимущественно теоретический характер, явные формулы дают возможность алгоритмической реализации, а полученные на их основе алгоритмы могут быть легко запрограммированы и применены, в частности, в различных прикладных областях.

В разд. 1 приведена краткая сводка необходимых понятий и определений. В разд. 2 рассматриваются случаи минимальных степеней аннигилятора, а в разд. 3 — связь аннигилятора с глубиной матриц.

1. Необходимые понятия и определения

Исходя из (1) и (2), каждому полиному $g(x)$ из $P_2^n[x]$ сопоставим двоичное слово длины 2^n , которое представляет собой вектор коэффициентов \bar{c}_w . Таким образом, длина входа, задающего полином $g(x)$, равна 2^n . Мы рассматриваем 2^n -мерное векторное пространство $P_2^n[x]$ над полем F_2 и линейные преобразования $\{T_n\}$ этого пространства, задаваемые матрицами размера $2^n \times 2^n$, элементы которых будем нумеровать мономами из R_n . Таким образом,

$$T_n: P_2^n[x] \rightarrow P_2^n[x].$$

Рассмотрим специальные виды преобразований из $\{T_n\}$, связанные со следующей задачей.

Определение 1. Полином $g(x) \in P_2^n[x]$ называется *аннигилятором* для $f(x) \in P_2^n[x]$, если выполняется условие

$$f(x)g(x) \equiv 0 \quad \text{или} \quad g(x)[f(x) + 1] \equiv 0. \quad (3)$$

Задача состоит в поиске для заданного полинома $f(x)$ ненулевого аннигилятора минимальной степени, которую обозначим через $\alpha(f)$.

Пусть $Z_f = \{x \in B^n \mid f(x) = 0\}$ и $N_f = \{x \in B^n \mid f(x) = 1\}$ — множества нулей и единиц полинома $f(x)$ соответственно.

Известно простое соотношение между числом нулей Z_f полинома $f(x)$ и его аннигилятором.

Утверждение 1. Если d — минимальная степень аннигилятора, то

$$\sum_{i=0}^{d-1} C_n^i \leq 2^n - Z_f \leq \sum_{i=0}^{n-d} C_n^i.$$

В общем случае условие (3) можно выразить в виде

$$N_f \cap N_g = \emptyset \quad \text{или} \quad N_{f+1} \cap N_g = \emptyset. \quad (4)$$

Тогда требуется найти полином минимальной степени, удовлетворяющий условию (4).

Пример 1. 1) Так как $f(1+f) \equiv 0$, то $\alpha \leq \deg f$. Это следует из (4) с учётом того, что $\bar{f} = 1+f$.

2) Если $f(x) = x_1 F_1 + x_2 F_2$, где F_1, F_2 — произвольные полиномы из $P_2^n[x]$, то полином $g(x) = x_1 x_2 + x_1 + x_2 + 1$ является аннигилятором для $f(x)$, так как $f(x)g(x) \equiv 0$. Отсюда следует неравенство

$$\alpha(f) \leq 2.$$

Заметим, что если L_f — множество всех аннигиляторов f , то L_f — подпространство $P_2^n[x]$. Задача о вычислении $\alpha(f)$ сводится к нахождению в подпространстве L_f ненулевого полинома минимальной степени.

Формально пространство L_f может быть описано следующим образом. Рассмотрим линейное преобразование

$$Tg = fg. \quad (5)$$

Матрицу линейного преобразования обозначим через A_f . В этом случае L_f является нуль-пространством матрицы A_f или, что то же самое,

$$L_f = \{g \mid gA_f = 0\}. \quad (6)$$

В силу представления

$$f(x) = \sum_w c_w x^w$$

для матрицы A_f имеем следующее выражение:

$$A_f = \sum_w c_w A^w,$$

где $A^w = A_{x_1}^{w_1} A_{x_2}^{w_2} \dots A_{x_n}^{w_n}$ и A_{x_k} — матрица линейного преобразования $Tg = x_k g$. Тем самым для каждого монома полинома f можно найти соответствующее ему линейное преобразование и, сложив их, получить матрицу A_f .

Пример 2. 1) Если $n = 2$, то нужно рассматривать матрицу следующего вида:

$$A_{x_1x_2} = \begin{matrix} & 1 & x_1 & x_2 & x_1x_2 \\ \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \end{matrix} & \left\| \begin{matrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{matrix} \right\| \end{matrix}. \quad (7)$$

Чтобы построить матрицу линейного преобразования A_g , соответствующего моному g , достаточно посмотреть, во что переходят мономы из A_f при умножении на g . В частности, если $g = x_1x_2$, то получаем матрицу преобразования $A_{x_1x_2}$.

2) Если $n = 2$, $f = 1 + x_1x_2$, то нужно рассматривать матрицу следующего вида: $A_{1+x_1x_2} = A_1 + A_{x_1x_2}$.

$$A_1 = \begin{matrix} & 1 & x_1 & x_2 & x_1x_2 \\ \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \end{matrix} & \left\| \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\| \end{matrix}, \quad A_{x_1x_2} = \begin{matrix} & 1 & x_1 & x_2 & x_1x_2 \\ \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \end{matrix} & \left\| \begin{matrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{matrix} \right\| \end{matrix},$$

$$A_{1+x_1x_2} = \begin{matrix} & 1 & x_1 & x_2 & x_1x_2 \\ \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \end{matrix} & \left\| \begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{matrix} \right\| \end{matrix}. \quad (8)$$

3) Если $n = 2$, $f = x_1$, то нужно рассматривать матрицу вида

$$A_{x_1} = \begin{matrix} & 1 & x_1 & x_2 & x_1x_2 \\ \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \end{matrix} & \left\| \begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{matrix} \right\| \end{matrix}.$$

Заметим, что в общем случае комбинаторное строение матрицы A_{x_i} описывается следующими свойствами:

- каждая строка матрицы A_{x_i} содержит ровно одну единицу;
- в матрице имеется ровно 2^{n-1} нулевых столбцов и ровно 2^{n-1} столбцов с двумя единицами;
- если столбцу соответствует моном, содержащий переменную x_i , то он содержит ровно две единицы.

2. О минимальной степени аннигилятора

В терминах линейных преобразований нахождение числа $\alpha(f)$ — минимальной степени аннигилятора полинома $f(x)$ — выглядит следующим образом.

Если A_f — матрица линейного преобразования (5), а множество всех аннигиляторов полинома $f(x)$ — её нуль-пространство, то для нахождения минимальной степени полинома в этом нуль-пространстве введём следующее определение.

Определение 2. α -Рангом матрицы A_f линейного преобразования, связанного с полиномом f , называется минимальное число r такое, что первые r строк матрицы A_f линейно зависимы.

Теорема 1. Если α -ранг матрицы A_f равен d , то минимальная степень аннигилятора $a(f)$ определяется следующим образом. Если

$$d = \sum_{i=0}^r \binom{n}{i}, \quad (9)$$

то $a(f) = r$. Если же

$$\sum_{i=0}^r \binom{n}{i} < d < \sum_{i=0}^{r+1} \binom{n}{i}, \quad (10)$$

то $a(f) = r + 1$.

ДОКАЗАТЕЛЬСТВО. По определению α -ранга

$$\sum_{i=1}^d \beta_i v_i = 0, \quad \text{где } A_f = \begin{pmatrix} v_1 \\ \vdots \\ v_{2^n} \end{pmatrix}.$$

Если $d = \sum_{i=0}^r \binom{n}{i}$, то степень полинома g , соответствующего вектору $\beta = (\beta_1 \dots \beta_d 0 \dots 0)$, равна r . Если же

$$d = \sum_{i=0}^r \binom{n}{i} + m,$$

где $0 \leq m < \binom{n}{r+1}$, то $\deg g = r + 1$. С другой стороны, из этого же определения α -ранга следует, что если $gA_f = 0$, то степень полинома g не меньше, чем определённая условиями теоремы. Теорема 1 доказана.

Замечание 1. Очевидно, что «обычный» ранг $r(A)$ матрицы A и её α -ранг $r_\alpha(A)$ связаны неравенством

$$r_\alpha(A) \leq r(A).$$

Замечание 2. Доказанная теорема носит «двусторонний» характер в том смысле, что если $a(f) = r$, то α -ранг матрицы A_f определяется соотношениями (9)–(10).

Замечание 3. Если A_f — матрица линейного преобразования (5) и её ранг равен r , то число всех аннигиляторов для полинома f равно 2^{2^n-r} .

Пример 3. 1) Если $f = x_1x_2$, то матрица A_f построена выше (см. (7)). Ясно, что α -ранг A_f равен двум и $1 < 2 < \binom{2}{0} + 2$, поэтому $\alpha(f) = 1$. В частности, полином $g(x) = x_1 + 1$ является аннигилятором для f .

2) Если $f = 1 + x_1x_2$, то матрица A_f была построена выше (см. (8)). Ясно, что α -ранг A_f равен четырём и $4 = \binom{2}{0} + \binom{2}{1} + \binom{2}{2}$, поэтому $\alpha(f) = 2$. В частности, полином $g(x) = x_1x_2$ является аннигилятором для f .

Рассмотрим теперь оптимизационную задачу. Задан полином $f(x)$. Вопрос: имеет ли $f(x)$ линейный аннигилятор? Если имеет, то требуется его найти.

С алгоритмической точки зрения имеем оптимизационную задачу с размером входа $O(2^n)$, поэтому поиск минимальной степени аннигилятора формально имеет полиномиальную сложность по длине входа, но не по n .

Прямой переборный подход с проверкой линейной зависимости подмножеств n -элементного множества на линейную зависимость (любым критерием, например, с помощью матрицы Грама) имеет полиномиальную сложность по длине входа и позволяет решить задачу. Однако эта сложность экспоненциальна по n . Заметим, что для криптографических моделей такая ситуация типична и не выглядит неестественной.

Перейдём к рассмотрению интересного и важного подкласса полиномов — симметрических полиномов.

Определение 3. Полином называется *симметрическим*, если выполняется соотношение $g(x_1, \dots, x_n) = g(x_{S(1)}, \dots, x_{S(n)})$, где S — произвольная подстановка симметрической группы S_n .

Кольцо симметрических полиномов образует подкольцо кольца $P_2^n[x]$ и порождается множеством элементарных симметрических полиномов $\{\sigma_0(x), \dots, \sigma_n(x)\}$, где $\sigma_k(x) = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}$.

В базисе $\{\sigma_0(x), \dots, \sigma_n(x)\}$ каждый симметрический полином имеет единственное представление в форме

$$g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x), \quad \lambda_k \in F_2.$$

Условие того, что симметрический полином имеет аннигилятор степени не выше единицы, следует из результатов работы [20], где доказана

формула

$$\sigma_p(x)\sigma_q(x) = \sum_{r=p}^n \binom{r}{p}_2 \binom{p}{r-q}_2 \sigma_r(x).$$

Здесь

$$p > q, \quad x = (x_1, \dots, x_n), \quad \binom{n}{k}_2 = \begin{cases} 1, & \text{если } \binom{n}{k} \equiv 1 \pmod{2}, \\ 0, & \text{если } \binom{n}{k} \equiv 0 \pmod{2}. \end{cases}$$

По этой формуле непосредственно строится алгоритм поиска аннигиляторов для симметрических полиномов. В качестве следствия из неё можно получить соотношение

$$\sigma_p(x)\sigma_q(x) = \sum_{s=0}^q \binom{p+s}{r}_2 \binom{p}{q-s}_2 \sigma_{p+q}(x). \quad (11)$$

Из (11) с использованием теоремы Куммера при $q = 1$ в [20] получается выражение

$$\sigma_p(x)\sigma_1(x) = (p)_2\sigma_p(x) + (p+1)_2\sigma_{p+1}(x). \quad (12)$$

Это соотношение справедливо при $n \geq 3$, т. е. если $p \equiv 0 \pmod{2}$, то

$$\sigma_p(x)\sigma_1(x) = \sigma_{p+1}(x), \quad (13)$$

если $p \equiv 1 \pmod{2}$, то

$$\sigma_p(x)\sigma_1(x) = \sigma_p(x). \quad (14)$$

Заметим, что при $n = 2$ имеет место очевидное соотношение:

$$\sigma_2(x)\sigma_1(x) = 0.$$

Кроме того, $g(x) = 1$ не имеет линейного аннигилятора, а для полиномов

$g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x)$, $\lambda_k \in F_2$, следующих трёх «вырожденных» типов:

- 1) $\lambda_k = 1$, $k = 0, \dots, n$;
- 2) $\lambda_n = 1$, $\lambda_k = 0$, $k = 0, \dots, n-1$;
- 3) $\lambda_n = 0$, $\lambda_k = 0$, $k = 0, \dots, n-1$,

легко построить линейные аннигиляторы.

В следующих двух теоремах приведены критерии существования линейных аннигиляторов, которые к вышеприведённым типам полиномов не относятся. Назовём их *полиномами общего вида*.

Теорема 2. Пусть $g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x)$, $\lambda_k \in F_2$, — симметрический полином общего вида и $n > 2$. Для того чтобы линейный полином $l(x) = x_{j_1} + \dots + x_{j_s}$ был аннигилятором $g(x)$, необходимо и достаточно выполнения четырёх условий:

- 1) $k > 0$;
- 2) $l(x) = \sigma_1(x)$;
- 3) для всех $k < n$ таких, что $\lambda_k = 1$, если $k \equiv 0 \pmod{2}$, то $\lambda_{k+1} = 1$;
- 4) а если $k \equiv 1 \pmod{2}$, то $\lambda_{k+1} = 1$.

ДОКАЗАТЕЛЬСТВО. НЕОБХОДИМОСТЬ первого условия очевидна.

Пусть выполняется соотношение

$$\begin{aligned} l(x)g(x) &= (x_{j_1} + \dots + x_{j_s})g(x) = (x_{j_1} + \dots + x_{j_s}) \sum_{k=1}^n \lambda_k \sigma_k(x) \\ &= (x_{j_1} + \dots + x_{j_s})(\sigma_{k_1}(x) + \sigma_{k_2}(x) + \dots + \sigma_{k_m}(x)) = 0, \end{aligned}$$

где $k_1 < k_2 < \dots < k_m$. Пусть M — моном симметрического полинома $g(x)$. Обозначим через $M(l(x))$ сумму тех слагаемых $l(x)$, которые входят в M , а через $M^*(l(x))$ — сумму остальных слагаемых $l(x)$. Рассмотрим теперь произведение $l(x)\sigma_{k_1}(x)$. В $\sigma_{k_1}(x)$ число слагаемых равно $C_n^{k_1}$: $M_1, \dots, M_{C_n^{k_1}}$. Тогда $l(x)\sigma_{k_1}(x)$ можно представить в виде

$$\begin{aligned} M_1(l(x))M_1 + M_1^*(l(x))M_1 + M_2(l(x))M_2 \\ + M_2^*(l(x))M_2 + \dots + M_{C_n^{k_1}}(l(x))M_{C_n^{k_1}} + M_{C_n^{k_1}}^*(l(x))M_{C_n^{k_1}}^*. \end{aligned}$$

Здесь все слагаемые в произведениях без $*$ имеют степень k_1 , а остальные — степень $k_1 + 1$. Все остальные слагаемые в произведении $l(x)g(x)$ имеют степень, большую k_1 . Чтобы $l(x)$ был аннигилятором $g(x)$, необходимо

$$M_1(l(x))M_1 + M_2(l(x))M_2 + \dots + M_{C_n^{k_1}}(l(x))M_{C_n^{k_1}} = 0.$$

Вместе с тем для любого $i = 1, \dots, C_n^{k_1}$ все слагаемые в произведении $M_i(l(x))M_i$ одинаковы и отличаются от всех слагаемых в любом произведении $M_s(l(x))M_s$ при $s \neq i$. Таким образом, любое из этих слагаемых не может аннигилироваться никаким другим мономом в произведении $l(x)g(x)$, кроме мономов произведения $M_i(l(x))M_i$. Из этого следует, что число слагаемых в произведении $M_i(l(x))M_i$ чётно. Этого не может быть, если $l(x) \neq \sigma_1(x)$, поскольку в $\sigma_{k_1}(x)$ входят все возможные мономы от n переменных степени k_1 . Если $l(x) \neq \sigma_1(x)$, то количество мономов в произведениях $M_i(l(x))M_i$, $i = 1, \dots, C_n^{k_1}$, будет обязательно разной чётности. При $l(x) = \sigma_1(x)$ число мономов в любом произведении $M_i(l(x))M_i$, $i = 1, \dots, C_n^{k_1}$, равно k_1 . Следовательно, $k_1 \equiv 0 \pmod{2}$.

Если это так, то из (13) получаем $\sigma_{k_1}(x)\sigma_1(x) = \sigma_{k_1+1}(x)$, откуда следует, что

$$M_1^*(l(x))M_1 + M_2^*(l(x))M_2 + \dots + M_{C_n^{k_1}}^*(l(x))M_{C_n^{k_1}}^* = \sigma_{k_1+1}.$$

Тогда слагаемые из $\sigma_{k_1+1}(x)$ должны аннигилироваться некоторыми слагаемыми степени $k_1 + 1$ из произведения

$$(x_{j_1} + \dots + x_{j_s})(\sigma_{k_2}(x) + \sigma_{k_3}(x) + \dots + \sigma_{k_m}(x)) = 0.$$

Так как степени элементарных симметрических полиномов в этой формуле упорядочены по возрастанию, обязательно $k_2 = k_1 + 1$. Из (14) следует, что $\sigma_{k_1+1}(x)\sigma_1(x) = \sigma_{k_1+1}(x)$. Значит,

$$l(x)(\sigma_{k_1}(x) + \sigma_{k_2}(x)) = (x_{j_1} + \dots + x_{j_s})(\sigma_{k_1}(x) + \sigma_{k_2}(x)) = 0.$$

Переходим к k_3 . Точно так же доказываем, что k_3 чётно, $k_4 = k_3 + 1$ и

$$l(x)(\sigma_{k_3}(x) + \sigma_{k_4}(x)) = (x_{j_1} + \dots + x_{j_s})(\sigma_{k_3}(x) + \sigma_{k_4}(x)) = 0,$$

и т. д. Необходимость доказана.

ДОСТАТОЧНОСТЬ. Из (13) и (14) следует, что для аннигиляции симметрического полинома $g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x)$, $\lambda_k \in F_2$, линейным симметрическим полиномом $\sigma_1(x)$ в сумме $\sum_{k=1}^n \lambda_k \sigma_k(x)$ для всех слагаемых с $\lambda_k = 1$, $k \equiv 0 \pmod{2}$ обязательно присутствовало слагаемое с $\lambda_{k+1} = 1$. Тогда из (13) и (14) сразу следует, что

$$l(x)(\sigma_k(x) + \sigma_{k+1}(x)) = \sigma_1(x)(\sigma_k(x) + \sigma_{k+1}(x)) = 0.$$

Таким образом при выполнении условий 1–4 обеспечивается равенство

$$\sigma_1(x)g(x) = \sigma_1(x) \sum_{k=1}^n \lambda_k \sigma_k(x) = 0.$$

Теорема 2 доказана.

Теорема 3. Пусть $g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x)$, $\lambda_k \in F_2$, — симметрический полином общего вида и $n > 2$. Для того чтобы $l(x) = 1 + x_{j_1} + \dots + x_{j_s}$ был его аннигилятором, необходимо и достаточно выполнения следующих условий:

- 1) $k > 0$;
- 2) $l(x) = 1 + \sigma_1(x)$;
- 3) для всех k таких, что $\lambda_k = 1$, выполняется условие $k \equiv 1 \pmod{2}$.

ДОКАЗАТЕЛЬСТВО. НЕОБХОДИМОСТЬ первого условия очевидна.

Пусть выполняется соотношение

$$l(x)g(x) = (1 + x_{j_1} + \dots + x_{j_s})g(x) = (1 + x_{j_1} + \dots + x_{j_s}) \sum_{k=1}^n \lambda_k \sigma_k(x)$$

$$= (\sigma_{k_1}(x) + \sigma_{k_2}(x) + \dots + \sigma_{k_m}(x)) \\ + (x_{j_1} + \dots + x_{j_s})(\sigma_{k_1}(x) + \sigma_{k_2}(x) + \dots + \sigma_{k_m}(x)) = 0,$$

где $k_1 < k_2 < \dots < k_m$.

Рассмотрим произведение $l(x)\sigma_{k_1}(x)$. В $\sigma_{k_1}(x)$ входят слагаемые $M_1, \dots, M_{C_n^{k_1}}$. Вновь $l(x)\sigma_{k_1}(x)$ представим в виде

$$M_1(l(x)M_1 + M_1^*(l(x))M_1 + M_2(l(x))M_2 \\ + M_2^*(l(x))M_2 + \dots + M_{C_n^{k_1}}(l(x))M_{C_n^{k_1}} + M_{C_n^{k_1}}^*(l(x))M_{C_n^{k_1}}^*).$$

В нём все слагаемые в произведениях без $*$ имеют степень k_1 , а остальные — степень $k_1 + 1$. Все остальные слагаемые в произведении $l(x)g(x)$ имеют степень, большую k_1 . Чтобы $l(x)$ был аннигилятором $g(x)$, необходимо

$$M_1(l(x)M_1 + M_2(l(x))M_2 + \dots + M_{C_n^{k_1}}(l(x))M_{C_n^{k_1}}) = \sigma_{k_1}(x).$$

Заметим, что для любого $i = 1, \dots, C_n^{k_1}$ все слагаемые в произведении $M_i(l(x))M_i$ одинаковы и отличаются от всех слагаемых в любом произведении $M_s(l(x))M_s$ при $s \neq i$. Таким образом, любое из этих слагаемых не может аннигилироваться никаким другим мономом в произведении $l(x)g(x)$, кроме мономов произведения $M_i(l(x))M_i$. Из этого следует, что число слагаемых в произведении $M_i(l(x))M_i$ нечётное. (Одно слагаемое оставляем для аннигиляции соответствующего слагаемого в $\sigma_{k_1}(x)$.) Этого не может быть, если $l(x) \neq \sigma_1(x)$, поскольку в $\sigma_{k_1}(x)$ входят все возможные мономы от n переменных степени k_1 . Если $l(x) \neq \sigma_1(x)$, то число мономов в произведениях $M_i(l(x))M_i$, $i = 1, \dots, C_n^{k_1}$, будет обязательно разной чётности. При $l(x) = \sigma_1(x)$ число мономов в любом произведении $M_i(l(x))M_i$, $i = 1, \dots, C_n^{k_1}$, равно k_1 . Следовательно, $k_1 \equiv 1 \pmod{2}$.

Если это так, то из (12) получаем

$$\sigma_{k_1}(x)(1 + \sigma_1(x)) = \sigma_{k_1}(x) + \sigma_{k_1}(x) = 0,$$

откуда следует, что

$$A_f = \begin{pmatrix} v_1 \\ \vdots \\ v_{2^n} \end{pmatrix}.$$

Переходим к k_2 и точно так же доказываем, что k_2 нечётное и

$$l(x)\sigma_{k_2}(x) = (1 + x_{j_1} + \dots + x_{j_s})\sigma_{k_2}(x) = 0,$$

и т. д. Необходимость доказана.

ДОСТАТОЧНОСТЬ. Для случая полинома $1 + \sigma_1(x)$ из (12) получаем, что если $p \equiv 0 \pmod{2}$, то

$$\sigma_p(x)(1 + \sigma_1(x)) = \sigma_p(x) + \sigma_{p+1}(x), \quad (15)$$

если $p \equiv 1 \pmod{2}$, то

$$\sigma_p(x)(1 + \sigma_1(x)) = \sigma_p(x) + \sigma_p(x) = 0. \quad (16)$$

Отсюда следует, что для аннигиляции симметрического полинома $g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x)$, $\lambda_k \in F_2$, линейным симметрическим полиномом $1 + \sigma_1(x)$ в сумме $\sum_{k=0}^n \lambda_k \sigma_k(x)$ для всех слагаемых с $\lambda_k = 1$ должно выполняться условие $k \equiv 1 \pmod{2}$. Тогда при выполнении условий 1–3 этой теоремы обеспечивается равенство

$$(1 + \sigma_1(x))g(x) = (1 + \sigma_1(x)) \sum_{k=1}^n \lambda_k \sigma_k(x) = 0.$$

Теорема 3 доказана.

Рассмотрим квадратичные полиномы вида

$$l(x) = x_{v_1}x_{u_1} + \dots + x_{v_s}x_{u_s} = L_{j_1} + \dots + L_{j_s},$$

т. е. все мономы второй степени.

Теорема 4. Пусть $g(x) = \sum_{k=0}^n \lambda_k \sigma_k(x)$, $\lambda_k \in F_2$, — симметрический полином и $n \equiv 0 \pmod{4}$, $n > 2$. Для того чтобы квадратичный полином $l(x) = L_{j_1} + \dots + L_{j_s}$ был аннигилятором $g(x)$, необходимо выполнение следующих четырёх условий:

- 1) $k > 0$;
- 2) $l(x) = \sigma_2(x)$;
- 3) для всех k таких, что $\lambda_k = 1$, выполняется условие $k \equiv 0 \pmod{2}$;
- 4) если k_1 — минимальная степень монома в $g(x)$, то $k_1 \equiv 0 \pmod{4}$.

ДОКАЗАТЕЛЬСТВО. НЕОБХОДИМОСТЬ первого условия очевидна.

Пусть выполняется соотношение

$$\begin{aligned} l(x)g(x) &= (L_{j_1} + \dots + L_{j_s})g(x) = (L_{j_1} + \dots + L_{j_s}) \sum_{k=1}^n \lambda_k \sigma_k(x) \\ &= (L_{j_1} + \dots + L_{j_s})(\sigma_{k_1}(x) + \sigma_{k_2}(x) + \dots + \sigma_{k_m}(x)) = 0, \end{aligned}$$

где $k_1 < k_2 < \dots < k_m$.

Пусть M — моном симметрического полинома $g(x)$. Обозначим через $M(l(x))$ сумму тех слагаемых $l(x)$, обе переменных которых входят в M ,

а через $M^*(l(x))$ — сумму остальных слагаемых $l(x)$. Рассмотрим произведение $l(x)\sigma_{k_1}(x)$. В $\sigma_{k_1}(x)$ число слагаемых равно $C_n^{k_1}$: $M_1, \dots, M_{C_n^{k_1}}$. Тогда $l(x)\sigma_{k_1}(x)$ можно представить в виде

$$M_1(l(x))M_1 + M_1^*(l(x))M_1 + M_2(l(x))M_2 + M_2^*(l(x))M_2 + \dots + M_{C_n^{k_1}}(l(x))M_{C_n^{k_1}} + M_{C_n^{k_1}}^*(l(x))M_{C_n^{k_1}}^*.$$

Здесь все слагаемые в произведениях без $*$ имеют степень k_1 , а остальные — степени $k_1 + 1$ или $k_1 + 2$. Все остальные слагаемые в произведении $l(x)g(x)$ имеют степень, большую k_1 . Чтобы $l(x)$ был аннигилятором $g(x)$, необходимо

$$M_1(l(x))M_1 + M_2(l(x))M_2 + \dots + M_{C_n^{k_1}}(l(x))M_{C_n^{k_1}} = 0.$$

Вновь отметим, что для любого $i = 1, \dots, C_n^{k_1}$ все слагаемые в произведении $M_i(l(x))M_i$ одинаковы и отличаются от всех слагаемых в любом произведении $M_s(l(x))M_s$ при $s \neq i$. Таким образом, любое из этих слагаемых не может аннигилироваться никаким другим мономом в произведении $l(x)g(x)$, кроме мономов произведения $M_i(l(x))M_i$. Из этого следует, что число слагаемых в произведении $M_i(l(x))M_i$ чётное. Этого не может быть, если $l(x) \neq \sigma_2(x)$, поскольку в $\sigma_{k_1}(x)$ входят все возможные мономы от n переменных степени k_1 . Если $l(x) \neq \sigma_1(x)$, то число мономов в произведениях $M_i(l(x))M_i$, $i = 1, \dots, C_n^{k_1}$, будет обязательно разной чётности. При $l(x) = \sigma_1(x)$ число мономов в любом произведении $M_i(l(x))M_i$, $i = 1, \dots, C_n^{k_1}$, равно $C_{k_1}^2$. Следовательно, $C_{k_1}^2 \equiv 0 \pmod{2}$, а значит, что $k_1 \equiv 0 \pmod{4}$.

Из (11) следует, что

$$\sigma_p(x)\sigma_2(x) = \binom{p}{2}_2 \sigma_p(x) + \binom{p+2}{2}_2 \sigma_{p+2}(x).$$

Таким образом, для всех k таких, что $\lambda_k = 1$, выполняется условие $k \equiv 0 \pmod{2}$. Теорема 4 доказана.

Замечание 4. Если $n \not\equiv 0 \pmod{4}$, то критерий существования квадратичного аннигилятора получается аналогично, но требует громоздкой формулировки и длинного переборного доказательства, в котором рассматриваются все 14 случаев вида последних компонент вектора λ : два при $n \equiv 1 \pmod{4}$, четыре при $n \equiv 2 \pmod{4}$ и восемь при $n \equiv 3 \pmod{4}$.

3. Аннигиляторы и глубина матриц

Пусть $f = \sum_w c_w x^w$ — полином и M_f — матрица мономов полинома f . Под *глубиной* $\xi(M_f)$ матрицы M_f будем понимать минимальное натуральное число r такое, что в матрице M_f существует r столбцов, образующих подматрицу M_f' , в которой нет нулевых строк. Другими словами, это означает следующее: существует r переменных из n таких, что каждый из мономов содержит хотя бы одну из этих переменных. Если $\alpha(f)$ — минимальная степень аннигилятора для f , то справедлива

Теорема 5. *Имеет место неравенство*

$$\alpha(f) \leq \xi(M_f).$$

ДОКАЗАТЕЛЬСТВО. Пусть $x_1 x_2 \dots x_r$ — «протыкающее» множество для полинома f , т. е. $r = \xi(M_f)$. Рассмотрим полином

$$g(x_1, \dots, x_n) = (1 + x_1)(1 + x_2) \dots (1 + x_r).$$

Покажем, что g — аннигилятор для f , т. е. $f \cdot g \equiv 0$.

Если $x = (x_1, \dots, x_n)$ — произвольный вектор из B^n , то какая-то из переменных x_1, x_2, \dots, x_r равна 1, и тогда $g(x) = 0$. Заметим также, что $x_1 = x_2 = \dots = x_r = 0$, так как каждый из мономов f содержит переменные из $\{x_1, x_2, \dots, x_r\}$.

Таким образом, полином $g(x_1, \dots, x_n) = (1 + x_1)(1 + x_2) \dots (1 + x_r)$ имеет степень $\xi(M_f)$ и является аннигилятором для f . Отсюда следует требуемое неравенство. Теорема 5 доказана.

Пример 4. Пусть $n = 2$ и $f_1 = x_1 + x_2$, $f_2 = x_1 + x_1 x_2$, $f_3 = 1 + x_1 + x_2$. Тогда $\alpha(f_1) = 2$, $\alpha(f_2) = 1$, $\alpha(f_3) = 1$ и $g_1 = x_1 x_2$, $g_2 = x_2$, $g_3 = x_1 + x_2$ — аннигиляторы для f_1 , f_2 и f_3 соответственно.

4. Заключение

В работе предложен новый подход к анализу комбинаторных характеристик булевых полиномов и связанных с ними объектов.

Описаны специальные типы линейных преобразований пространства булевых полиномов. С помощью этих преобразований предложены формулы и алгоритмы для нахождения минимальной степени аннигилятора заданного булева полинома. Рассмотрены условия, при которых аннигилятор может быть линейным. Приведены оценки минимальной степени аннигилятора.

Полученные в работе результаты могут представлять интерес для прикладных разработок в области криптографии и криптоанализа.

ЛИТЕРАТУРА

1. **Панкратова И. А.** Булевы функции в криптографии: учебное пособие. Томск: Томск. ун-т, 2014. 88 с.
2. **Courtois N., Meier W.** Algebraic attacks on stream ciphers with linear feedback // *Advances in Cryptology – EUROCRYPT 2003* (Proc. Int. Conf. Theory Appl. Cryptogr. Tech., Warsaw, Poland, May 4–8, 2003). Heidelberg: Springer, 2003. P. 345–359. (Lect. Notes Comput. Sci.; Vol. 2656).
3. **Didier F.** A new upper bound of the block error probability after decoding over the erasure channel // *IEEE Trans. Inform. Theory*. 2006. Vol. 52, No. 10. P. 4496–4503.
4. **Feng K., Liao Q., Yang J.** Maximal values of generalized algebraic immunity // *Des. Codes Cryptogr.* 2009. Vol. 50. P. 243–252.
5. **Carlet C., Merabet B.** Asymptotic lower bound on the algebraic immunity of random balanced multi-output Boolean functions // *Adv. Math. Commun.* 2013. Vol. 7, No. 2. P. 197–217.
6. **Лобанов М. С.** Точные соотношения между нелинейностью и алгебраической иммунностью // *Дискрет. анализ и исслед. операций*. 2008. Т. 15, № 6. С. 34–47.
7. **Лобанов М. С.** Об одном методе получения нижних оценок на нелинейность булевой функции // *Мат. заметки*. 2013. Т. 93, № 5. С. 741–745.
8. **Лобанов М. С.** Точное соотношение между нелинейностью и алгебраической иммунностью // *Дискрет. математика* 2006. Т. 18, № 3. С. 152–159.
9. **Леонтьев В. К.** Булевы полиномы и линейные преобразования // *Докл. РАН*. 2009. Т. 425, № 3. С. 320–322.
10. **Тужилин М. Э.** Алгебраический иммунитет булевых функций // *Прикл. дискрет. математика*. 2008. № 2. С. 18–22.
11. **Rizomiliotis P.** Improving the high order nonlinearity of Boolean functions with prescribed algebraic immunity // *Discrete Appl. Math.* 2010. Vol. 158, No. 18. P. 2049–2055.
12. **Mesnager S.** Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // *IEEE Trans. Inf. Theory*. 2008. Vol. 54, No. 8. P. 3656–3662.
13. **Mesnager S., Gohen G.** Fast algebraic immunity of Boolean functions // *Adv. Math. Commun.* 2017. Vol. 11, No. 2. P. 373–377.
14. **Wang Q., Johansson T.** On equivalence classes of Boolean functions // *Information Security and Cryptology* (Rev. Sel. Pap. 13th Int. Conf., Seoul, Korea, Dec. 1–3, 2010). Heidelberg: Springer, 2011. P. 311–324. (Lect. Notes Comput. Sci.; Vol. 6829).
15. **Peng J., Kan H.** Constructing rotation symmetric Boolean functions with maximum algebraic immunity on an odd number of variables // *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* 2012. Vol. E95-A, No. 6. P. 1056–1064.

16. **Sun L., Fu F.-W.** Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Theor. Comput. Sci. 2018. Vol. 738. P. 13–24.
17. **Sun L., Fu F.-W.** Constructions of even-variable RSBFs with optimal algebraic immunity and high nonlinearity // J. Appl. Math. Comput. 2018. Vol. 56, No. 1–2. P. 593–610.
18. **Shaojing F. U., Jiao D. U., Longjiang Q. U., Chao L. I.** Construction of odd-variable rotation symmetric Boolean functions with maximum algebraic immunity // IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 2016. Vol. E99-A, No. 4. P. 853–855.
19. **Wang Q., Tan C. H., Stanica P.** Concatenations of the hidden weighted bit function and their cryptographic properties // Adv. Math. Commun. 2014. Vol. 8, No. 2. P. 153–165.
20. **Леонтьев В. К.** Симметрические булевы полиномы // Журн. вычисл. математики и мат. физики. 2010. Т. 50, № 8. С. 1520–1531.
21. **Carlet C., Gao G., Liu W.** A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions // J. Comb. Theory, A. 2014. Vol. 127. P. 161–175.
22. **Su S., Tang X.** Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Des. Codes Cryptogr. 2014. Vol. 71. P. 1567–1580.
23. **Леонтьев В. К.** Комбинаторика и информация. Ч. 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.
24. **Леонтьев В. К., Морено О.** О нулях булевых полиномов // Журн. вычисл. математики и мат. физики. 1998. Т. 38, № 9. С. 1608–1615.
25. **Леонтьев В. К., Гордеев Э. Н.** О числе нулей булевых полиномов // Журн. вычисл. математики и мат. физики. 2018. Т. 68, № 7. С. 1235–1245.
26. **Гордеев Э. Н., Леонтьев В. К., Медведев Н. В.** О свойствах булевых полиномов, актуальных для криптосистем // Вопросы кибербезопасности. 2017. № 3. С. 63–69.

Леонтьев Владимир Константинович
Гордеев Эдуард Николаевич

Статья поступила
24 января 2019 г.
После доработки —
10 сентября 2019 г.
Принята к публикации
25 сентября 2019 г.

ON THE ANNIHILATORS OF BOOLEAN POLYNOMIALS

V. K. Leontiev^{1,2,a} and *E. N. Gordeev*^{2,b}¹Dorodnitsyn Computing Center,
42 Vavilov Street, 119991 Moscow, Russia²Bauman Moscow State Technical University,
5 Vtoraya Baumanskaya Street, 105005 Moscow, RussiaE-mail: ^a*vkleontiev@yandex.ru*, ^b*werhorn@yandex.ru*

Abstract. Boolean functions in general and Boolean polynomials (Zhegalkin polynomials or algebraic normal forms (ANF)) in particular are the subject of theoretical and applied studies in various fields of computer science. This article addresses the linear operators of the space of Boolean polynomials in n variables, which leads to the results on the problem of finding the minimum annihilator degree for a given Boolean polynomial. This problem is topical in various analytical and algorithmic aspects of cryptography. Boolean polynomials and their combinatorial properties are under study in discrete analysis. The theoretical foundations of information security include the study of the properties of Boolean polynomials in connection with cryptography. In this article, we prove a theorem on the minimum annihilator degree. The class of Boolean polynomials is described for which the degree of an annihilator is at most 1. We give a few combinatorial characteristics related to the properties of the space of Boolean polynomials. Some estimates of the minimum degree of an annihilator are given. We also consider the case of symmetric polynomials. Bibliogr. 26.

Keywords: Boolean polynomial, symmetric polynomial, annihilator, linear operator, cryptosystem.

This research is supported by Ministry of Science and Higher Education of Russian Federation (State Assignment 0063–2016–0003) and Russian Foundation for Basic Research (Project 19–07–00895).

English version: Journal of Applied and Industrial Mathematics **14** (1), 162–175 (2020), DOI 10.1134/S1990478920010159.

REFERENCES

1. **I. A. Pankratova**, *Boolean Functions in Cryptography* (Tomsk. Gos. Univ., Tomsk, 2014).
2. **N. Courtois** and **W. Meier**, Algebraic attacks on stream ciphers with linear feedback, in *Advances in Cryptology – EUROCRYPT 2003 (Proc. Int. Conf. Theory and Applications of Cryptography Techniques, Warsaw, Poland, May 4–8, 2003)* (Springer, Heidelberg, 2003), pp. 345–359.
3. **F. Didier**, A new upper bound of the block error probability after decoding over the erasure channel, *IEEE Trans. Inform. Theory*. **52** (10), 4496–4503 (2006).
4. **K. Feng**, **Q. Liao**, and **J. Yang**, Maximal values of generalized algebraic immunity, *Des. Codes Cryptogr.* **50**, 243–252 (2009).
5. **C. Carlet** and **B. Merabet**, Asymptotic lower bound on the algebraic immunity of random balanced multi-output Boolean functions, *Adv. Math. Commun.* **7** (2), 197–217 (2013).
6. **M. S. Lobanov**, Exact ratios between nonlinearity and algebraic immunity, *Diskretn. Anal. Issled. Oper.* **15** (6), 34–47 (2008).
7. **M. S. Lobanov**, About a method for obtaining some lower estimates of nonlinearity of a Boolean function, *Mat. Zametki* **93** (5), 741–745 (2013).
8. **M. S. Lobanov**, An exact ratio between nonlinearity and algebraic immunity, *Diskretn. Mat.* **18** (3), 152–159 (2006).
9. **V. K. Leont'ev**, Boolean polynomials and linear transformations, *Dokl. Ross. Akad. Nauk* **425** (3), 320–322 (2009).
10. **M. E. Tuzhilin**, Algebraic immunity of Boolean functions, *Prikl. Diskretn. Mat.*, No. 2, 18–22 (2008).
11. **P. Rizomiliotis**, Improving the high order nonlinearity of Boolean functions with prescribed algebraic immunity, *Discrete Appl. Math.* **158** (18), 2049–2055 (2010).
12. **S. Mesnager**, Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity, *IEEE Trans. Inform. Theory* **54** (8), 3656–3662 (2008).
13. **S. Mesnager** and **G. Gohen**, Fast algebraic immunity of Boolean functions, *Adv. Math. Commun.* **11** (2), 373–377 (2017).
14. **Q. Wang** and **T. Johansson**, On equivalence classes of Boolean functions, in *Information Security and Cryptology (Rev. Sel. Pap. 13th Int. Conf., Seoul, Korea, Dec. 1–3, 2010)* (Springer, Heidelberg, 2011), pp. 311–324.
15. **J. Peng** and **H. Kan**, Constructing rotation symmetric Boolean functions with maximum algebraic immunity on an odd number of variables, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E95-A** (6), 1056–1064 (2012).
16. **L. Sun** and **F.-W. Fu**, Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, *Theor. Comput. Sci.* **738**, 13–24 (2018).

17. **L. Sun** and **F.-W. Fu**, Constructions of even-variable RSBFs with Optimal algebraic immunity and high nonlinearity, *J. Appl. Math. Comput.* **56** (1–2), 593–610 (2018).
18. **F. U. Shaojing**, **D. U. Jiao**, **Q. U. Longjiang**, and **L. I. Chao**, Construction of odd-variable rotation symmetric Boolean functions with maximum algebraic immunity, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E99-A** (4), 853–855 (2016).
19. **Q. Wang**, **C. H. Tan**, and **P. Stănică**, Concatenations of the hidden weighted bit function and their cryptographic properties, *Adv. Math. Commun.* **8** (2), 153–165 (2014).
20. **V. K. Leont'ev**, Symmetrical Boolean polynomials, *Zh. Vychisl. Mat. Mat. Fiz.* **50** (8), 1520–1531 (2010).
21. **C. Carlet**, **G. Gao**, and **W. Liu**, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions, *J. Comb. Theory, Ser. A*, **127**, 161–175 (2014).
22. **S. Su** and **X. Tang**, Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, *Des. Codes Cryptogr.* **71**, 1567–1580 (2014).
23. **V. K. Leont'ev**, *Combinatorics and Information*, Vol. 1: *Combinatorial Analysis* (MFTI, Moscow, 2015).
24. **V. K. Leont'ev** and **O. Moreno**, About zeros of Boolean polynomials, *Zh. Vychisl. Mat. Mat. Fiz.* **38** (9), 1608–1615 (1998).
25. **V. K. Leont'ev** and **E. N. Gordeev**, On number of zeros of Boolean polynomials, *Zh. Vychisl. Mat. Mat. Fiz.* **68** (7), 1235–1245 (2018).
26. **E. N. Gordeev**, **V. K. Leont'ev**, and **N. V. Medvedev**, On properties of Boolean polynomials important for cryptosystems, *Vopr. Kiberbezopasnosti*, No. 3, 63–69 (2017).

Vladimir K. Leontiev

Eduard N. Gordeev

Received January 24, 2019

Revised September 10, 2019

Accepted September 25, 2019