ОБ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ СИСТЕМ КОДИРОВАНИЯ

Леонтьев В.К.[1], Гордеев Э.Н.[2]

Булевы функции вообще и булевы полиномы, в частности, - предмет теоретических и прикладных исследований в различных областях информатики. Аннигиляторы булевых функций и алгебраическая иммунность булевых полиномов – важные предметы исследования в системах кодирования. Само определение понятия аннигилятора для булевых полиномов вводится с помощью некоторого преобразования в кольце полиномов, поэтому в работе проблематика, связанная с аннигиляторами булевых полиномов, рассматривается в рамках линейных преобразований над эти кольцом. В частности, изучаемые в работе линейные преобразования пространства булевых полиномов от n переменных позволили получить результаты, касающиеся проблемы нахождения минимальной степени аннигилятора для заданного булева полинома. Именно эта задача является наиболее актуальной в различных аналитических и алгоритмических аспектах кодирования. Цель работы – на фоне обзора важности алгебраической иммунности для конструкции «хороших» систем кодирования привести формулы и алгоритмы ее нахождения в общем случае и для определенных классов булевых полиномов. В работе приведена теорема о минимальной степени аннигилятора булева полинома в общем случае. Даны оценки минимальной степени аннигилятора. Описан класс булевых полиномов, для которых степень аннигилятора не превосходит единицы. Особое внимание уделено аннигиляторам симметрических булевых полиномов. Получены критерии наличия линейного аннигилятора для симметрического булева полинома, а также условия наличия у него квадратичного аннигилятора. Приведен ряд комбинаторных характеристик, связанных со свойствами пространства булевых полиномов. Используются методы комбинаторного анализа, алгебры и теории алгоритмов[3].

Ключевые слова: *булев полином, симметрический полином, алгебраическая иммунность, аннигилятор, линейное преобразование.*

DOI: *10.21681/2311-3456-2019-1-59-68*

Введение

Пусть B={0,1}, B^n – n-мерный булев куб, g(x) – булева функция: $B^n \to B$ 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 $F_2[x_1,...,x_n]$-кольцо полиномов над F_2. Если профакторизовать это кольцо по модулю идеала $I = (x_1 + x_1^2, x_2 + x_2^2, ..., x_n + x_n^2)$, то получится кольцо F_2/I булевых полиномов с обычными операция сложения и умножения и равенством $x_i = x_i^2, i = 1,...,n$. 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|| — называется степенью монома x^w.

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

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

Ясно, 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

$$c_w \in B, w = (w_1,..., w_n) \in B^n, x^w = x_1^{w_1},..., x_n^{w_n}, x_k^{w_k} = \begin{cases} x_k, \text{если} & w_k = 1 \\ 1, \text{если} & w_k = 0 \end{cases}.$$

Представление (1) называется булевым полиномом, полиномом Жегалкина, 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

---

1 Леонтьев Владимир Константинович, доктор физико-математических наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: vkleontiev@yandex.ru.

2 Гордеев Эдуард Николаевич, доктор физико-математических наук, профессор кафедры Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: werhorn@yandex.ru.

3 Работа выполнена в рамках Госзадания по теме №0063-2016-0003.

g(x). (Если мономы сначала упорядочены по длине, а мономы одинаковой длины – лексикографически, то получим однозначное отображение множества булевых полиномов в множество матриц мономов.)

Определение. 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)≡0 или g(x)[f(x)+1]≡0. (3)

Определение. *Алгебраической иммунностью* булевой функции $f(x) \in P_2^n[x]$ называется минимальной степень ее аннигилятора.

Задача поиска аннигиляторов булевых функций долгое время привлекала малое внимание специалистов в области дискретной математики.

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

Требование устойчивости схем шифрования к разного вида атакам приводит к тому, что в них используются булевы функции с определенными свойствами. Конечно, эти свойства зависят от принципов построения самих криптографических конструкций. В случае с потоковыми шифрами требуемые свойства булевых функции, используемых в качестве нелинейных фильтров, характеризуются ограничениями на алгебраическую иммунность и нелинейность высоких порядков.

Перечень подобных требований, их значение и взаимосвязи можно найти в любом учебнике, например, в [1]. Алгебраическая имунность задается минимальной степенью аннигилятора. Поэтому результаты, которые в дискретном анализе касались значения или оценок минимальной степени аннигилятора, в криптоанализе можно интерпретировать как исследование алгебраической имунности.

Важным прогрессом в области криптоанализа, достигнутым в 2003 году, стало введение Courtois N. и Meier W. алгебраических атак и быстрых алгебраических атак, которые являются очень мощными концепциями анализа и могут применяться практически ко всем криптографическим алгоритмам. Для изучения устойчивости к алгебраическим атакам и было тогда введено понятие алгебраической иммуннности.

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

С той поры в этой области исследований можно условно выделить три главные направления, которые, опять-таки условно, можно обозначить следующим образом.

1. Математики-дискретчики, ищущие в криптографии, обоснования постановкам задач.

2. Математики, пытающиеся найти связи между разными прикладными областями.

3. Криптографы, ищущие в полученных результатах из области дискретного анализа резервы для своих результатов.

Приведем примеры из этих направлений для того, чтобы была понятна тематика этой нашей работы.

Примером из первого направления может служить работа Didier F. [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 обобщенных весов Хэмминга. Это оказывается весьма полезным для кодов Рида-Маллера, для которых известны все обобщенные веса Хемминга, тогда как полное распределение весов известно лишь частично. Для этих кодов вероятность ошибки дана в связи с криптографическим понятием алгебраической иммунности. Далее с использованием этой оценки решается уже другая задача: находится алгебраическая иммунность и ее асимптотика для случайной «сбалансированной» булевой функции.

Feng K., Liao Q., Yang J. [4] обобщают понятие алгебраической иммунности булевых функций несколькими способами на вектор-функции над произвольными конечными полями и получают верхние оценки для такой обобщенной алгебраической иммунности. Доказано, что верхние границы могут быть достигнуты с использованием свойств кодов Рида-Маллера.

Направление исследований Didier F. продолжается, например, в работе Carlet C. Merabet B. [5]. Эта статья расширяет работу Didier F. по алгебраической иммунности случайных сбалансированных булевых функций, на асимптотическую нижнюю границу алгебраической имунности специального класса функций (random balanced Boolean functions).

Примерами результатов во втором направлении служит цикл работ М.С.Лобанова (см. [6], [7], [8]). В работе [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 перемен-

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

В статье Rizomeliotisa P. [11], в определенном смысле, улучшены некоторые известные нижние оценки нелинейности r-го порядка булевой функции с заданной алгебраической имунностью. Это достигается за счет того, что там вводится понятие дополнительной алгебраической имунности, а его значение может быть вычислено как часть вычисления алгебраической имунности без изменения вычислительной сложности.

Mesnager S. в [12] доказывает новую нижнюю границу для профиля нелинейности r-го порядка булевых функций, учитывая их алгебраическую иммунность, которая значительно улучшается для одной из этих нижних оценок для всех порядков и для другой для низких порядков.

Mesnager S., Cohen G. в [13] используют параметр, введенный Лю и соавторами, называемый быстрой алгебраической иммунностью (fast algebraic immunity), в качестве инструмента для измерения устойчивости криптосистемы, построенной на основе булевых полиномов к быстрым алгебраическим атакам. Доказана верхняя оценка значения быстрой алгебраической иммунности. Используя ее установлена слабость обратных функций следа (trace inverse functions) против быстрых алгебраических атак.

Примерами работ в третьем направлении являются статьи, где строятся булевы функции максимально пригодный для «хороших» (обладающих оптимальными криптографическими зхарактеристиками) криптографических конструкций.

Работа [14] Wang Q, Johansson T. изучает понятие нелинейной эквивалентности булевых функций, при которой многие криптографические 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 криптографические свойства, в том числе алгебраическая иммунность, алгебраическая степень и нелинейность классов эквивалентности и др., Описываются классы эквивалентности с «хорошими» криптографическими характеристиками и методы построения таких классов.

Хорошо известно, что булевы функции, используемые в потоковых и блочных шифрах, должны обладать большой алгебраической иммунностью, чтобы противостоять алгебраическим атакам. Поэтому активно изучаются конструкции таких функций. Например, Peng J. и Kan H. Предлагают в [15] несколько конструкций симметричных булевых полиномов с нечетным числом переменных (rotation symmetric Boolean functions) с максимальной алгебраической имунностью. Это направление продолжается в работах Lei Sun и Fang-Wei Fu [16], [17], а также Shaojing FU, Jiao DU, Longjiang QU, Chao LI [18].

В статье Wang Q., Tan Ch.H., Stanica P. [19] строятся модификации известной HWBF функции (hidden weighted bit function) введеной Briant еще в 1991 г. Новые функции сбалансированы, с почти оптимальной алгебраической степенью и удовлетворяют строгому лавинному критерию. Исследуется их алгебраическая имунность, размер BDD и другие актуальные криптографические свойства.

Аннигиляторы симметрических полиномов в связи с алгебраической иммунностью построением «хороших» криптографических конструкций изучаются во многих работах. В качестве примеров можно привести работу Леонтьева В.К. [20] и статью Carlet C., Gao G., Liu W. [21].

Su S., Tang,X в [22] изучаются симметрические булевы полиному с четным и нечетным число неизвестных. Для построения криптографически «хороших» булевых функций используется теоретико-числовая техника. Построены классы полиномов с оптимальными, в коком-то смысле, характеристиками: алгебраической иммунностью, степенью и пр.

Все, сказанное выше объясняет актуальность и тематику данной работы.

С точки зрения приведенной классификации, кроме уже упомянутых результаты авторов, принадлежащие к первым двум направлениям приведены также в работах [23],[24],[25],[26-27].

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 областях криптографии.

Большинство теорем приведено здесь без технически громоздких доказательств. Подробные доказательства можно найти в [23] и [26].

Во второй части работы приведена краткая сводка используемых понятий и определений. Третья часть посвящена нахождению минимальной степени аннигилятора (корреляционной иммунности) в общем случае. В четвертой части рассматриваются частные случаи минимальных степеней, а в пятой – комбинаторные параметры, связанные с основной тематикой работы.

2. Необходимые понятия и определения

Исходя из (1) и (2) сопоставим каждому полиному g(x) из $P_2^n[x]$ двоичное слово длины 2^n, которое представляет вектор коэффициентов $\overline{c_w}$. 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 этого пространства, задаваемые матрицами размеров $2^n \times 2^n$, элементы которых мы будем нумеровать мономами из R_n.

Таким образом, задается преобразование

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

Мы рассмотрим специальные виды преобразований из T_n, связанные с задачей поиска для заданного полинома f(x) ненулевого аннигилятора минимальной степени, которую мы обозначим через α(f).

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

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

Утверждение. Если d - минимальная степень аннигилятора, то

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

В работах [24], [25], [27] подробно изучается вопрос нахождения Z_f и его оценок.

В общем случае условие (3) можно выразить в виде:

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

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

Пример 1.

1) Так как $f(1+f) \equiv 0$, то $\alpha \le degf$. Это следует из (4) с учетом $\overline{f} = 1 + f$.

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)≡0. Отсюда следует неравенство

α(f)≤2.

Заметим теперь, что если L_f — множество всех аннигиляторов f, то L_f — подпространство $P_2^n[x]$.

Задача о вычислении α(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 . (5)

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

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

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

$$A_{x_1x_2} = \begin{array}{c|cccc} . & 1 & x_1 & x_2 & x_1x_2 \\ 1 & 0 & 0 & 0 & 1 \\ x_1 & 0 & 0 & 0 & 1 \\ x_2 & 0 & 0 & 0 & 1 \\ x_1x_2 & 0 & 0 & 0 & 1 \end{array} . \quad (7)$$

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=$x_1 x_2$, то получаем матрицу преобразования $A(x_1 x_2)$.

2). Если n=2, f =1+$x_1 x_2$, то нужно рассматривать матрицу следующего вида: $A_{1+x1x2}=A_1+A_{x1\,x2}$.

$$A_1 = \begin{array}{c|cccc} . & 1 & x_1 & x_2 & x_1x_2 \\ 1 & 1 & 0 & 0 & 0 \\ x_1 & 0 & 1 & 0 & 0 \\ x_2 & 0 & 0 & 1 & 0 \\ x_1x_2 & 0 & 0 & 0 & 1 \end{array}$$

$$A_{x_1x_2} = \begin{array}{c|cccccc|c} . & . & 1 & x_1 & x_2 & x_1x_2 & . \\ 1 & \| & 0 & 0 & 0 & 1 & \| \\ x_1 & \| & 0 & 0 & 0 & 1 & \| \\ x_2 & \| & 0 & 0 & 0 & 1 & \| \\ x_1x_2 & \| & 0 & 0 & 0 & 1 & \| \end{array}$$

$$A_{1+x_1x_2} = \begin{array}{c|cccccc|c} . & . & 1 & x_1 & x_2 & x_1x_2 & . \\ 1 & \| & 1 & 0 & 0 & 1 & \| \\ x_1 & \| & 0 & 1 & 0 & 1 & \| \\ x_2 & \| & 0 & 0 & 1 & 1 & \| \\ x_1x_2 & \| & 0 & 0 & 0 & 0 & \| \end{array}. \quad (8)$$

3). Если n=2, f = x_1, то нужно рассматривать матрицу следующего вида:

$$A_{x_1} = \begin{array}{c|cccccc|c} . & . & 1 & x_1 & x_2 & x_1x_2 & . \\ 1 & \| & 0 & 1 & 0 & 0 & \| \\ x_1 & \| & 0 & 1 & 0 & 0 & \| \\ x_2 & \| & 0 & 0 & 0 & 1 & \| \\ x_1x_2 & \| & 0 & 0 & 0 & 1 & \| \end{array}$$

Заметим, что в общем случае комбинаторное строения матрицы описывается следующими свойствами:

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

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

Кольцо симметрических полиномов является подкольцом кольца $P_2^n[x]$ и порождается множеством элементарных симметрических полиномов $\{\sigma_0(x),\ldots,\sigma_n(x)\}$, где $\sigma_k(x) = \sum_{1\le i_1<\ldots<i_k\le n} x_{i_1}\ldots x_{i_k}$

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

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

Рассмотрим ещё одно линейное преобразование пространства полиномов $P_2^n[x]$. Здесь мы будем отождествлять 2^n-мерное линейное пространство $P_2^n[x]$ с пространством двоичных векторов длины 2^n, а линейные преобразования $P_2^n[x]$] — с квадратными ($2^n\times 2^n$)-матрицами, элементы которых нумеруются мономами из R^n.

Определение. Пусть $g(x) \in P_2^n[x]$ и

$$g^*(x) = \sum_{v\in B^n} g(v)x^v$$

Тогда линейное преобразование (*) называется 1-преобразованием.

Пусть f — полином: $f=\sum_w c_w x^w$,и M_f — матрица мономов полинома f.

Определение. 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.

3. О минимальной степени аннигилятора

В терминах линейных преобразований нахождение числа α(f) – минимальной степени аннигилятора полинома f(x) - выглядит следующим образом.

Если A_f –матрица линейного преобразования (5), а множество всех аннигиляторов полинома f(x) – это ее нуль-пространство, то для нахождения минимальной степени полинома в этом нуль-пространстве введем следующее определение.

Определение. 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. Пусть α-ранг матрицы A_f равен d, тогда 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.

Замечание 1. Очевидно, что «обычный» ранг r(A) матрицы A и ее α-ранг rα(A) связаны неравенством:

rα(A)≤ r(A).

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

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

Пример 3.

1). Если $f=x_1 x_2$, то матрица A_f была построена выше (5).

Ясно, что α-ранг A_f равен двум и $1<2<\binom{2}{0}+2$ и потому α(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 (6).

Ясно, что α-ранг A_f равен четырем и $4 = \binom{2}{0}+\binom{2}{1}+\binom{2}{2}$ и потому α(f)=2. В частности, полином $g(x)=x_1x_2$ является аннигилятором для f.

4. Линейные и квадратичные аннигиляторы

Рассмотрим сначала некоторые следствия из теоремы 1.

Первое следствие касается полиномов, аннигиляторы которых имеют степень не выше единицы.

Пусть f – полином от n переменных, но существенно зависящий от k переменных, состоящий из m мономов.

Определение. Линейным представлением полинома называется представление множества {1,...,k} в виде объединения s его подмножеств $U_1,...,U_s$ (мощности которых: $k_1,...,k_s$) такое, что выполняется одно из двух условий:

$$f(x_1,...,x_n)=\sum_{i=1}^{s}F(x_1,...,x_n)\sum_{p=1}^{k_i}x_{j_p} \qquad (11)$$

или

$$f(x_1,...,x_n)=\sum_{i=1}^{s}F(x_1,...,x_n)\left(1+\sum_{p=1}^{k_i}x_{j_p}\right). \qquad (12)$$

Теорема 2. Если существует линейное представление полинома $f(x_1,...,x_n)$, то его аннигилятор имеет степень не более единицы.

Доказательство. Если существует линейное представление полинома $f(x_1,...,x_n)$, то соотношения (11) или (12) задают отношения линейной зависимости среди первых n+1 строк матрицы A_f линейного преобразования, связанного с f(x). Но это означает, что α(f)=1,так как

или $d=\sum_{i=0}^{1}\binom{n}{i}$, или

$$\sum_{i=0}^{0}\binom{n}{i}<d<\sum_{i=0}^{1}\binom{n}{i}.$$

Теорема доказана.

Пример 4. Пусть $f(x)=x_3+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4$. Для него существует линейное разбиение $f(x)=x_1(x_3+x_4)+x_2(x_3+x_4)+x_3(x_3+x_4)$поэтому степень его аннигилятора, например, $g(x)=x_1+x_2+x_3$ равна единице.

Пусть f(x)=l(x)+q(x)+u(x), где l(x) - линейный, q(x) - квадратичный, u(x) -полином степени выше двух.

Пусть задано подмножество I индексов из {1,...,n}, через x(I) обозначим полином $x(I)=\sum_{i\in I}x_i$.

Можно сформулировать простое необходимое условие существования аннигилятора степени единица.

Теорема 3. Для того чтобы полином f(x) имел аннигилятор степени единица необходимо чтобы существовало подмножество I индексов из {1,...,n} такое что либо ни один из мономов l(x) не содержит переменной с индексом из I и l(x)x(I)=q(x), либо в l(x) присутствуют все мономы с индексами из I, а полином x(I)q(x)+x(I)l(x) имел степень больше двух.

Доказывается непосредственной проверкой. Если выполняется первое условие, то может существовать линейный полином со свободным членом 1, в противном случае такого аннигилятора не будет. Аналогично, во втором случае может существовать линейный полином –аннигилятор без свободного члена. В противном случае его не будет.

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 мы имеем оптимизационную задачу с размером входа $O(2^n)$. Поэтому поиск минимальной степени аннигилятора формально имеет сложность полиномиальную 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 сложность полиномиальную по длине входа и позволяет решить задачу. Однако, эта сложность экспоненциальная по n. Заметим, однако, что для криптографических моделей такая ситуация типична и не выглядит неестественной.

Перейдем теперь к рассмотрению интересного и важного подкласса полиномов: симметрическим полиномам.

Условие того, что симметрический полином имеет аннигилятор степени не выше единицы, следует из результатов работы [7], 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 $p>q,\ x=(x_1,\ldots,x_n),\ \binom{n}{k}_2=\begin{cases}1, \binom{n}{k}\equiv 1 \pmod 2\\ 0, \binom{n}{k}\equiv 0 \pmod 2\end{cases}$.

По этой формулы непосредственно строится алгоритм поиска аннигиляторов для симметрических полиномов.

В качестве следствия из нее можно получить следующее соотношение:

$$\sigma_p(x)\sigma_q(x) = \sum_{s=0}^{q} \binom{p+s}{r}_2 \binom{p}{q-s}_2 \sigma_{p+q}(x). \quad (13)$$

Из (13) с использованием теоремы Куммера при q=1 в [20] получается выражение

$$\sigma_p(x)\sigma_1(x) = (p)_2\sigma_p(x) + (p+1)_2\sigma_{p+1}(x). \quad (14)$$

Теорема 4. Пусть $g(x) = \sum_{k=0}^{n} \lambda_k \sigma_k(x), \lambda_k \in F_2$ – симметрический полином и n>2. Для того, чтобы линейный полином $l(x) = x_{j_1} + \ldots + x_{j_s}$ – был аннигилятором необходимо и достаточно выполнения четырех условий:

1. k>0.

2. $l(x) = \sigma_1(x)$.

3. Для всех k таких, что λ_k=1, если k=0 (mod2), λ_{k+1}=1.

4. А если k=1 (mod2), то λ_{k-1}=1.

Теорема 5. Пусть $g(x) = \sum_{k=0}^{n} \lambda_k \sigma_k(x), \lambda_k \in F_2$ – симметрический полином и n>2. Для того, чтобы $l(x) = 1 + x_{j_1} + \ldots + x_{j_s}$ – был его аннигилятором необходимо и достаточно выполнения условий:

1. k>0.

2. $l(x) = \sigma_1(x)$

3. Для всех k таких, что λ_k=1 выполняется условие k=1 (mod2).

Рассмотрим теперь квадратичные полиномы вида

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

т.е. все мономы этого полинома имеют вторую степень.

Теорема 6. Пусть $g(x) = \sum_{k=0}^{n} \lambda_k \sigma_k(x), \lambda_k \in F_2$ – симметрический полином и n>2. Для того, чтобы квадратичный полином $l(x) = L_{j_1} + \ldots + L_{j_s}$ был аннигилятором *g(x)* необходимо и достаточно выполнение условий:

1. $l(x) = \sigma_2(x)$.

2. Для всех k таких, что λ_k=1и k=0 (mod4) выполняется условие: λ_{k+2}=1.

3. Для всех k таких, что λ_k=1и k=1 (mod4) выполняется условие: λ_{k+2}=1.

4. Для всех k таких, что λ_k=1и k=2 (mod4) выполняется условие: λ_{k-2}=1.

5. Для всех k таких, что λ_k=1и k=3 (mod4) выполняется условие: λ_{k-2}=1.

5. Аннигиляторы и связанные с ними комбинаторные характеристики линейных преобразований

5.1. Аннигиляторы и глубина матриц

Если α(f) — минимальная степень аннигилятора для f, то справедливо следующее предложение.

Теорема 5. Имеет место неравенство

α(f)≤ξ(M_f).

Доказательство. Пусть x_1 x_2...x_r —«протыкающее» множество для полинома f, то есть r=ξ(M_f).

Рассмотрим полином g(x_1...x_n)=(1+x_1)(1+x_2)... (1+x_r). Покажем, что g — аннигилятор для f, то есть f • g≡0.

Если x=(x_1...x_n) — произвольная точка из B^n, то какая-то из переменных x_1,x_2,...,x_r равна 1 и тогда g(x)=0. Если же x_1=x_2= • • • =x_r=0, то f(x)=0, так как каждый из мономов f содержит переменные из {x_1 x_2...x_r}.

Таким образом, данный полином g(x_1...x_n)=(1+x_1)(1+x_2)... (1+x_r) – имеет степень ξ(M_f) и является аннигилятором для f. Отсюда и следует требуемое неравенство.

Теорема доказана.

Пример 5.

1). 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 α(f_1)=2, α(f_2)=1, α(f_3)=1 и g_1=x_1 x_2, g_2=x_2, g_3=x_1+x_2 — аннигиляторы соответственно для f_1, f_2 и f_3.

5.2. Булевы полиномы и 1-преобразования

Рассмотрим теперь второе из определенных выше линейных преобразований – преобразование (*).

Теорема 6. Преобразование (*) обладает следующими свойствами:

1. Инволютивность: (g*)* =g.

2. Число единиц g(x) равно числу мономов g*(x).

Пример 6.

1). (x_1 x_2...x_n)* =x_1 x_2...x_n.

2). (x_1 v x_2 v ... v x_n)* =x_1 v x_2 v ... v x_n.

3). Если e_n=x_1+x_2+ • • • +x_n, то

$$e_n^* = \begin{cases} e_n & \text{прин}\equiv 0(\text{mod}2) \\ e_n + x_1x_2\ldots x_n & \text{прин}\equiv 1(\text{mod}2) \end{cases}$$

Пусть A_n^* — матрица введённого выше линейного преобразования (*). Для описания A_n^* рассмотрим «стандартный» частичный порядок на множестве мономов $R_n = \{1, x_1, \ldots, x_n, \ldots, x_1x_2\ldots x_n\}$, положив для мономов v_i и v_j

$$v_i \le v_j,$$

если множество переменных, входящих в моном v_i, является подмножеством множества переменных, входящих в моном v_j.

Теорема 7. Пусть $A_n^* = \left\| \alpha_{v_i,v_j} \right\|$, тогда

$$\alpha_{v_i,v_j} = \begin{cases} 1, & \text{если} v_i \le v_j \\ 0, & \text{если} v_i > v_j \end{cases}.$$

Пример 7.

$$A_{x_1x_2} = \begin{array}{ccccccc} . & . & 1 & x_1 & x_2 & x_1x_2 & . \\ 1 & \| & 1 & 1 & 1 & 1 & \| \\ x_1 & \| & 0 & 1 & 0 & 1 & \| \\ x_2 & \| & 0 & 0 & 1 & 1 & \| \\ x_1x_2 & \| & 0 & 0 & 0 & 1 & \| \end{array}$$

Отметим следующие свойства матрицы A_n^*:

1) $\alpha_{v_i,v_j} = \overline{\alpha}_{v_i,v_j}$ при $i \ne j$,

2) $\alpha_{v_i,v_j} = 1$ при $i = 1, 2^n$,

3) A_n^* — треугольная матрица и $rang\left(A_n^*\right) = 2^n$,

4) ${A_n^*}^2$ или $A_n^* = {A_n^*}^{-1}$,

5) если $A_n^* = H_n + E$, то $H_n^2 = 0$.

Все эти свойства могут быть выведены из приведённой выше теоремы и инволютивности преобразования (*).

Определение. Полином f(x) называется 1-инвариантным, если выполняется соотношение f*(x)=f(x).

Теорема 8. Полином f(x) является 1-инвариантным тогда и только тогда, когда выполняется соотношение: fHn=0.

Замечание 4. В терминах функциональных уравнений формулировка этой теоремы выглядит следующим образом.

Теорема 9. Полином f(x) является 1-инвариантным тогда и только тогда, когда выполняется соотношение:

$$f(x) = \sum_{y \le x} f(y).$$

Замечание 5. Важна с прикладной, в частности, криптографической точки зрения проблема нахождения числа нулей булевого полинома. Она подробно рассматривается, в частности, в работах ([24], [25], [27]). Также ей посвящена и следующая теорема.

Теорема 10. Пусть f(x) является 1-инвариантным полином и m(f) –число его мономов, тогда справедливо соотношение:

$$Z_f = 2^n - m(f).$$

Доказательство непосредственно следует из определений и утверждений, приведенных выше.

6. Заключение

В работе предложен новый подход к анализу комбинаторных характеристик булевых полином и связанных с ними объектов. Он позволил получить новые формулы, оценки и алгоритмы нахождения такой важной для систем защиты информации характеристики криптосистем, ка их корреляционная иммунность.

Описаны специальные типы линейных преобразований пространства булевых полиномов. С помощью этих преобразований предложены формулы и алгоритмы для нахождения минимальной степени аннигилятора заданного булевы полинома. Приведены формулы и оценки минимальной степени аннигилятора. Теорема 1 позволяет построить алгоритм нахождения минимальной степени аннигилятора произвольно булева полинома. Рассмотрены условия, при которых аннигилятор может быть линейным.

Для симметрических булевых полиномов приведены критерии, при которых аннигилятор может быть линейным. Дано необходимое условие наличия квадратичного аннигилятора специального виде (все мономы второй степени).

Приведена связь задач нахождения минимальной степени аннигилятора и глубины матрицы.

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

Достоверность полученных результатов основывается на доказательствах и рассмотрениях, приведенных в настоящей статье и цитируемых работах авторов, на которой базируется эта работа.

Литература:
1. Панкратова И.А. Булевы функции в криптографии: учебное пособие. Томск.: Томский Университет, 2014. 88 с.
2. Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback // Advances in cryptology, EUROCRYPT 2003. Berlin, Heidelberg: Springer Verl., 2003. P. 345–359. (Lect. Notes in Comp. Sci.; V. 2656).
3. Didier F. A new upper bound of the block error probability after decoding over the erasure channel // IEEE Transactions On Information Theory. 2006. V. 52. No. 10. P. 4496 – 4503.
4. Feng K., Liao Q., Yang J. Maximal values of generalized algebraic immunity // Des. Codes Cryptogr. 2009. V. 50. P. 243–252.
5. Carlet C, Merabet B. Asymptotic lower bound on the algebraic immunity of random balanced multi-output Boolean functions // Advances in Mathematics of Communications. 2013, V.7. №2. P. 197-217. DOI: 10.3934/amc.2013.7.197.
6. Лобанов М.С. Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций. 2008. Том 15, № 6 С. 34–47.
7. Лобанов М.С. Об одном методе получения нижних оценок на нелинейность булевой функции // Матем. Заметки 2013. Т.93. №5. С. 741–745. DOI:10.4213/mzm10233.
8. Лобанов М.С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика / 2006. Т.18. №3. С. 152-159.
9. Леонтьев В.К. Булевы полиномы и линейные преобразования // ДАН. 2009. Т.425. №3. С. 320-322.
10. Тужилин М.Э. Алгебраический Иммунитет булевых функций // Прикладная Дискретная Математика. 2008. № 2(2). С.18-22.
11. Rizomiliotis P., Improving the high order nonlinearity lower bound for Boolean functions with given algebraic immunity // Discrete Appl. Math. 2010. V.158. Is.18 , P. 2049–2055. DOI: 10.1016 / j.dam.2010.08.023.
12. Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // IEEE Trans. Inf. Theory. 2008. V.54. № 8. P. 3656-3662. Zbl 1247.94028.
13. Mesnager S., Cohen G. Fast algebraic immunity of Boolean functions// Advances in Mathematics of Communications / 2017. V. 11. №2. P. 373-377. DOI: 10.3934/amc.2017031.
14. Wang Q., Johansson T. On Equivalence Classes of Boolean Functions. In Proceedings of “Information Security and Cryptology - Icisc 2010” / Lecture Notes in Computer Science, 6829, eds. Rhee KH., Nyang D., Springer-Verlag Berlin. 2011. P. 311–324.
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. V. E95A. №6. P.1056–1064. DOI: 10.1587/transfun.E95.A.1056.
16. Lei Sun, Fang-Wei Fu. Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Theoretical Computer Science. 2018. Vol.738. P.13-24. DOI: 10.1016/j.tcs.2018.04.040.
17. Lei Sun, Fang-Wei Fu. Constructions of even-variable RSBFs with optimal algebraic immunity and high nonlinearity // Journal of Applied Mathematics and Computing. 2018, Vol.56. №1-2. P.593-610. DOI: 10.1007/s12190-017-1088-1.
18. Shaojing FU, Jiao DU, Longjiang QU, Chao LI. Construction of odd-Variable Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2016. V. E99.A. №4. P.853-855. DOI: 10.1587/transfun.E99.A.853.
19. Wang Q., Tan Ch.H., Stanica P.Concatenations of the Hidden Weighted BIT Function and their Cryptographic Properties // Adv. Math. Commun. 2014. V.8. №2. P.153–165. DOI: 10.3934/amc.2014.8.153.
20. Леонтьев В.К. Симметрические булевы полиномы // Ж. вычисл. матем. и матем. физ. 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. V. 127. P. 161–175. DOI: 10.1016/j.jcta.2014.05.00.16.
22. Su S., Tang X. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Des. Codes Cryptogr. 2014. V. 71. P. 1567–1580. DOI: 10.1007/s10623-012-9727-x.
23. Леонтьев В.К. Комбинаторика и информация. Часть 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.
24. Леонтьев В.К., Морено О. О нулях булевых полиномов // Ж. вычисл. матем. и матем. физ. 1998. Т. 38. № 9. С. 1608–1615.
25. Леонтьев В.К., Гордеев Э.Н. О числе нулей булевых полиномов // Ж. вычисл. матем. и матем. физ. 2018. Т. 68. №7. С.1235-1245.
26. Леонтьев В.К., Гордеев Э.Н. Об аннигиляторах булевых полиномов // Дискретный анализ и исследование операций. 2019. Т. 26. В печати.
27. Гордеев Э.Н., Леонтьев В.К., Медведев Н.В. О свойствах булевых полиномов, актуальных для криптосистем // Вопросы кибербезопасности, 2017, №3. С. 63-69. DOI: 10.21681/2311-3456-2017-3-63-69

Рецензент: *Басараб Михаил Алексеевич, доктор физико-математических наук, профессор и заведующий кафедрой «Информационная безопасность» МГТУ им. Н.Э. Баумана. E-mail: bmic@mail.ru*

ON THE ALGEBRAIC IMMUNITY OF CODING SYSTEMS

Leontiev V. K.[4], Gordeev E. N.[5]

Boolean functions in General and Boolean polynomials in particular are the subject of theoretical and applied research in various fields of computer science. Annihilators of Boolean functions and algebraic immunity of Boolean polynomials are important subjects of research in theoretical cryptography. The very definition of the annihilator concept for Boolean polynomials is introduced by means of some transformation in the ring of Boolean polynomials, so in the paper the problem related to the annihilators of Boolean polynomials is considered within the framework of linear transformations over these ring. In particular, the linear transformations of the space of Boolean polynomials in n variables studied in the

4 Vladimir K. Leontiev, Dr.Sc., Professor, BMSTU, Moscow, Russia. E-mail: vkleontiev@yandex.ru The state assignment topic No. 0063-2016-0003
5 Eduard N. Gordeev, Dr.Sc., Professor, BMSTU, Moscow, Russia. E-mail: werhorn@yandex.ru

paper allowed us to obtain results concerning the problem of finding the minimum annihilator degree for a given Boolean polynomial. This task is the most relevant in various analytical and algorithmic aspects of cryptography. The aim of the work is to give formulas and algorithms for its finding in the General case and for certain classes of Boolean polynomials on the background of the review of the importance of algebraic immunity for the construction of «good» cryptosystems. The paper presents a theorem on the minimum degree of the annihilator of a Boolean polynomial. Estimates of the minimum degree of the annihilator are given. The described class of Boolean polynomials, where the degree of the annihilator does not exceed unity. Special attention is paid to annihilators of symmetric Boolean polynomials. The criteria for the presence of a linear annihilator for a symmetric Boolean polynomial and the conditions for the presence of a quadratic annihilator are obtained. A number of combinatorial characteristics related to the properties of the space of Boolean polynomials are given. Methods of combinatorial analysis, algebra and algorithm theory are used.

Keywords: *Boolean polynomial, symmetric polynomial, algebraic immunity, annihilator, linear transformation, cryptosystem.*

References:

1. Pankratova I.A. Boolean functions in cryptology. Tomsk: Tomskiy Universitet. 2014. 88 p.
2. Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback // Advances in cryptology, EUROCRYPT 2003. Berlin, Heidelberg: Springer Verl., 2003. P. 345–359. (Lect. Notes in Comp. Sci.; V. 2656).
3. Didier F. A new upper bound of the block error probability after decoding over the erasure channel // IEEE Transactions On Information Theory. 2006. V. 52. No. 10. P. 4496 – 4503.
4. Feng K., Liao Q., Yang J. Maximal values of generalized algebraic immunity // Des. Codes Cryptogr. 2009. V. 50. P. 243–252.
5. Carlet C, Merabet B. Asymptotic lower bound on the algebraic immunity of random balanced multi-output Boolean functions // Advances in Mathematics of Communications. 2013, V.7. №2. P. 197-217. DOI: 10.3934/amc.2013.7.197.
6. Lobanov M.S. Exact relations between nonlinearity and algebraic immunity // Journal of Applied and Industrial Mathematics. 2009. V. 3. № 3. P. 367-376.
7. Lobanov M.S. On a Method of Derivation of Lower Bounds for the Nonlinearity of Boolean Functions // Math. Notes. 2013. V. 93. №5. P. 727–731. DOI: 10.1134/S000143461305009X.
8. Lobanov M.S. Exact relation between nonlinearity and algebraic immunity // Discrete mathematics. 2006. V. 18. No. 3. P. 152-159.
9. Leontiev V. K. Boolean polynomials and linear transformations // DAN. 2009. Vol. 425. № 3. P. 320-322.
10. Tuzhilin M. E. Algebraic Immunity of Boolean functions // Applied Discrete Mathematics. 2008. Is. 2 (2). 18-22.
11. Rizomiliotis P., Improving the high order nonlinearity lower bound for Boolean functions with given algebraic immunity // Discrete Appl. Math. 2010. V.158. Is.18, P. 2049–2055. DOI: 10.1016/j.dam.2010.08.023.
12. Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // IEEE Trans. Inf. Theory. 2008. V.54. № 8. P. 3656-3662. Zbl 1247.94028.
13. Mesnager S., Cohen G. Fast algebraic immunity of Boolean functions // Advances in Mathematics of Communications / 2017. V. 11. №2. P. 373-377. DOI: 10.3934/amc.2017031.
14. Wang Q., Johansson T. On Equivalence Classes of Boolean Functions. In Proceedings of “Information Security and Cryptology - Icisc 2010” / Lecture Notes in Computer Science, 6829, eds. Rhee KH., Nyang D., Springer-Verlag Berlin. 2011. P. 311–324.
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. V. E95A. №6. P.1056–1064. DOI: 10.1587/transfun.E95.A.1056.
16. Lei Sun, Fang-Wei Fu. Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Theoretical Computer Science. 2018. Vol.738. P.13-24. DOI: 10.1016/j.tcs.2018.04.040.
17. Lei Sun, Fang-Wei Fu. Constructions of even-variable RSBFs with optimal algebraic immunity and high nonlinearity // Journal of Applied Mathematics and Computing. 2018, Vol.56. №1-2. P.593-610. DOI: 10.1007/s12190-017-1088-1.
18. Shaojing FU, Jiao DU, Longjiang QU, Chao LI. Construction of odd-Variable Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2016. V. E99.A. №4. P.853-855. DOI: 10.1587/transfun.E99.A.853.
19. Wang Q., Tan Ch.H., Stanica P.Concatenations of the Hidden Weighted BIT Function and their Cryptographic Properties // Adv. Math. Commun. 2014. V.8. №2. P.153–165. DOI: 10.3934/amc.2014.8.153.
20. Leont’ev V. K. Symmetric Boolean polynomials // Zh. Vychisl. matem. and matem. Fiz. 2010. V. 50. № 8. P. 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. V. 127. P. 161–175. DOI: 10.1016/j.jcta.2014.05.00.16.
22. Su S., Tang,X. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Des. Codes Cryptogr. 2014. V. 71. P. 1567–1580. DOI: 10.1007/s10623-012-9727-x.
23. Leont’ev V. K. Combinatorics, and information. Part 1. Combinatorial analysis. Moscow: MIPT, 2015. 174 p.
24. Leont’ev V. K., Moreno O. On the zeros of Boolean polynomials // Zh. Vychisl. matem. and matem. Fiz.. Vol. 38. № 9. P. 1608-1615.
25. Leont’ev V. K., Gordeev E.N. Number of zeroes of Boolean polynomials // Zh. Vychisl. matem. and matem. Fiz. 2018. V.68. № 7. P. 1235-1245.
26. Leont’ev V. K., Gordeev E.N. On the Annigilators of Boolean polynomials // Journal of Applied and Industrial Mathematics. 2019. V. 26. In preparation.
27. Gordeev E. N., Leont’ev V. K., Medvedev N. In. The properties of Boolean polynomials that are relevant to public key cryptosystems // Voprosy kiberbezopasnosti, 2017, № 3. P. 63-69. DOI: 10.21681/2311-3456-2017-3-63-69