Московский государственный университет
имени М.В. Ломоносова
Механико-математический факультет

На правах рукописи
УДК 519.1, 519.7

Лобанов Михаил Сергеевич

О соотношениях между алгебраической иммунностью и нелинейностью булевых функций

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2009

Работа выполнена на кафедре дискретной математики Механико-математического факультета Московского государственного университета имени М.В. Ломоносова.

Научный руководитель:	кандидат физико-математических наук, доцент Тарannиков Юрий Валерьевич
Официальные оппоненты:	доктор физико-математических наук, профессор Шевченко Валерий Николаевич
	кандидат физико-математических наук Логачев Олег Алексеевич
Ведущая организация:	Институт математики имени С.Л. Соболева СО РАН,

Защита диссертации состоится 20 ноября 2009 г. в 16 ч. 45 м. на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М.В. Ломоносова по адресу: Российская Федерация, 119991,Москва, ГСП-1, Ленинские горы, дом 1, МГУ им М.В.Ломоносова, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (Главное здание, 14 этаж)

Автореферат разослан 20 октября 2009 г.

Ученый секретарь
диссертационного совета
Д501.001.84 при МГУ
доктор физико-математических наук,
профессор

А.О. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы.

Диссертация посвящена изучению взаимосвязи алгебраической иммунности булевых функций и их нелинейностей различных порядков. Эти два свойства булевых функций очень важны с точки зрения криптографии.

Многие потоковые шифры состоят из линейной части, порождающей последовательность с большим периодом, обычно состоящей из одного или нескольких регистров сдвига с линейной обратной связью (linear feedback shift registers, LFSR), и нелинейной комбинирующей функции f, которая порождает выходную последовательность по данным линейным входам. Исследования криптографической устойчивости таких шифров большей частью сводятся к исследованию нелинейной функции f, в частности, к исследованию этой функции с точки зрения того, удовлетворяет или не удовлетворяет она некоторым критериям, необходимым для того, чтоб успешно противостоять различным криптографическим атакам. Часто эти критерии конфликтуют между собой.

Пусть f является булевой функцией над F_2^n. Известно, что f единственным образом представляется полиномом. Степенью булевой функции называется длина самого длинного слагаемого в ее полиноме (количество переменных в этом слагаемом), обозначение $\deg(f)$. Булева функция g над F_2^n называется *аннигилятором* булевой функции f над F_2^n, если $fg = 0$.

Алгебраической иммунностью $AI(f)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n, где g не равная тождественно нулю функция с минимальной степенью, такая что $fg = 0$ или $(f + 1)g = 0$.

Известно, что для любой f над F_2^n выполнено $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Алгебраическая иммунность – это способность противостоять разного рода алгебраическим атакам на регистры сдвига с линейной обратной связью (LFSR). Эти атаки впервые были предложены Н.Куртуа и В.Майером[1]. Они раскрывают секретный ключ путем решения системы уравнений, зависящих от многих переменных. Данные системы уравнений описывают соотношения между битами ключа/состояния и выходными битами f (комбинирующей функции для LFSR). Н.Куртуа[2] показал, что, если найдено такое соотношение низкой степени, алгебраические атаки очень эффективны.

[1]N.Courtois and W.Meier. Algebraic attacks on stream ciphers with linear feedback // Anvances in cryptology, EUROCRYPT 2003. — Berlin/Heidelberg: Springer Verl., 2003 , P. 345-359. (Lecture Notes in Computer Science; Vol. 2656).

[2]N.Courtois and W.Meier. Algebraic attacks on stream ciphers with linear feedback // Anvances in cryptology, EUROCRYPT 2003. — Berlin/Heidelberg: Springer Verl., 2003. — P. 345-359. (Lecture Notes in Computer Science; Vol. 2656).

Н.Куртуа и В.Майер[3] показали, что указанные соотношения низкой степени и, соответственно, успешные алгебраические атаки существуют для некоторых хорошо известных шифров, которые иммунны по отношению ко всем другим известным атакам. В частности, было доказано, что соотношение малой степени существует для шифров, использующих комбинирующую функцию f с малым количеством входов. Эти соотношения малой степени можно получить, получая многочлены малой степени, содержащие f в качестве делителя, т.е. умножая функцию f на подходящие функции g малой степени так, чтобы произведение $f \cdot g$ снова было малой степени. Если для функции f такая функция g существует (причем f не обязательно должна иметь малое количество входов), то алгебраическую атаку можно успешно провести. Таким образом, изучение булевых функций с точки зрения существования функций малой степени, содержащей данную в качестве делителя, имеет как теоретический, так и практический интерес.

Н.Куртуа и В.Майером было предложено три разновидности такого рода атак. Позже В.Майер, Е.Пасалич и К.Карле[4] свели эти три вида к двум и ввели новый термин – алгебраическая иммунность. Те же авторы доказали, что если алгебраическая иммунность достаточно высока, то алгебраическим атакам можно успешно противостоять.

Ранее важными критериями для комбинирующих функций в LFSR признавались высокая алгебраическая степень, высокий порядок корреляционной иммунности (устойчивости) и большое расстояние до множества аффинных функций (высокая нелинейность), чтобы успешно противостоять атакам Берлекэмпа–Мэсси и различным типам корреляционных и линейных атак[5, 6].

Требование высокой алгебраической иммунности может конфликтовать с требованиями удовлетворения остальным критериям. В.Майер, Е.Пасалич и К.Карле[7] показали, что, например, функции класса Майораны–Макфарланда, имеющие высокую устойчивость, высокую нелинейность (асимптотически

[3]N.Courtois and W.Meier. Algebraic attacks on stream ciphers with linear feedback // Anvances in cryptology, EUROCRYPT 2003. — Berlin/Heidelberg: Springer Verl., 2003. — P. 345-359. (Lecture Notes in Computer Science; Vol. 2656).

[4]W.Meier, E.Pasalic and C.Carlet. Algebraic attacks and decomposition of Boolean functions // Advances in Cryptology — EUROCRYPT 2004. — Berlin/Heidelberg: Springer Verl., 2004. — P. 474-491. (Lecture Notes in Computer Science; Vol. 3027).

[5]T.Johansson, F.Jönsson. Fast correlation attacks through reconstruction of linear polynomials // Advanced in Cryptology: Crypto 2000 (Santa Barbara, California, USA, August 20-24, 2000). — Springer-Verlag, 2000. — P. 300–315. (Lecture Notes in Computer Science; Vol. 1880)

[6]A.Canteaut, M.Trabbia. Improved fast correlation attacks using Parity-check equations of weight 4 and 5 // Eurocrypt 2000 (Bruges, Belgium, May 14–18, 2000). — Springer-Verlag, 2000. — P. 573–588. (Lecture Notes in Computer Science; Vol. 1807).

[7]W.Meier, E.Pasalic and C.Carlet. Algebraic attacks and decomposition of Boolean functions // Advances in Cryptology — EUROCRYPT 2004. — Berlin/Heidelberg: Springer Verl., 2004. — P. 474-491. (Lecture Notes in Computer Science; Vol. 3027).

порядка 2^{n-1}) и оптимальную алгебраическую степень[8, 9, 10, 11], имеют при этом достаточно низкую алгебраическую иммунность и не могут противостоять алгебраическим атакам.

Расстояние между булевыми функциями f_1 и f_2 определяется как $d(f_1, f_2) = \mid \{x \in F_2^n \mid f_1(x) \neq f_2(x)\} \mid$.

Нелинейностью r-го порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min\limits_{\deg(l) \leq r} d(f, l)$. *Нелинейностью* $nl(f)$ функции f называется расстояние между f и множеством аффинных функций, т. е. нелинейность первого порядка.

Отметим, что на языке теории кодирования нелинейность r-го порядка функции — это расстояние функции до $RM(r, n)$ кода Рида-Маллера r-го порядка.

Нелинейность булевых функций является важным свойством с точки зрения многих разделов дискретной математики. Именно поэтому к нему уже в течение нескольких десятилетий привлечено внимание исследователей. За это время появилось большое число работ, посвященных изучению нелинейности функций, а также взаимосвязи значения нелинейности с другими важными свойствами.

С точки зрения криптоанализа от булевой функции, используемой в качестве фильтра в потоковом шифре, надо требовать не только достаточно высокой нелинейности первого порядка, но и высокой нелинейности других порядков. В этом можно убедиться по работам Н.Куртуа[12], Ж.Голича[13], Т.Иваты и К.Куросавы[14], Л.Кнудсена и М.Робшау[15], У.Маурера[16], В.Миллана[17].

Настоящая работа посвящена проблеме оценки снизу нелинейности r-го порядка функции через значение ее алгебраической иммунности.

---

[8] J.F.Dillon. Elementary Hadamard Difference Sets // Ph. D. thesis, University of Maryland, USA, 1974.

[9] P.Camion, C.Carlet, P.Charpin, N.Sendrier. On correlation-immune functions // Eurocrypt'91 (Brighton, UK, April 8–11, 1991). — Springer-Verlag, 1991. — P. 86–100.

[10] C.Carlet. A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland Construction // Crypto 2002 (Santa Barbara, California, USA, August 18–22, 2002). — Springer-Verlag, 2002. — P. 549–564. (Lecture Notes in Computer Science; Vol. 2442).

[11] E.Pasalic. Degree optimized resilient Boolean functions from Maiorana–McFarland class // in 9-th IMA Conference on Cryptography and Coding, 2003.

[12] N.Courtois. Higher order corralation attacks, XL algorithm and cryptanalysis of Toyocrypt // Proceedings of ICISC 2002. — LNCS 2587. — P. 182-199.

[13] J.Golic. Fast low order approximation of cryptographic funtions // Proceedings of EUROCRYPT'96. — LNCS 1070, 1996. — P.268-282.

[14] T.Iwata, K.Kurosawa. Probabilistic higher order differential attack and higher order bent function // Proceedings of ASIACRYPT'99. — LNCS 1716, 1999. — P.62-74.

[15] L.R.Knudsen, M.J.B.Robshaw. Non-linear approximations in linear cryptanalysis // Proceedings of EUROCRYPT'96. — LNCS 1070, 1996. — P. 224-236.

[16] U.M.Maurer. New approaches to the design of self-synchronizing stream ciphers // Proceedings of EUROCRYPT'91. — LNCS 547, 1991. — P. 458-471.

[17] W.Millan. Low order approximation of cipher functions // Cryptographic Policy and Algorithms. — LNCS 1029, 1996. — P. 144-155.

Получение таких оценок дает не только информацию о взаимосвязи этих двух свойств, но важно еще и по следующей причине. Если вопросы связанные с нелинейностью $nl(f) = nl_1(f)$ достаточно хорошо изучены, и существует аппарат коэффициентов Уолша, который позволяет ее вычислять, то с нелинейностью более высоких порядков все обстоит заметно хуже. Про $nl_r(f)$ при $r \geq 2$ мало что известно. Стоит упомянуть наилучшую, как нам известно, на этот момент верхнюю асимптотическую оценку из работы К.Карле и С.Менаже[18].

В работе Ж.Коэна, И.Хонкалы, С.Лицына и А.Лобстейна[19] доказана также достаточно сильная нижняя оценка, которая, правда, тоже носит асимптотический характер и поэтому ничего не дает для оценки нелинейности r-го порядка при $r > 1$ для конкретных функций.

Эффективных алгоритмов подсчета нелинейности порядков выше первого тоже, насколько нам известно, пока не предложено. Алгоритм Г.Кабатянского и К.Тавернье[20] и его модификации[21, 22] работают только при $r = 2$ и $n \leq 13$.

В свете выше изложенного, получение как можно более сильных нижних оценок нелинейности r-го порядка через значение алгебраической иммунности приобретает особую важность. Отметим, что в работах Ф.Дидье, Ж.Тиллича[23] и В.Баева[24, 25] был предложен ряд алгоритмов подсчета алгебраической иммунности, а в работах Ф.Армкнехта, М.Краузе[26], А.Брэкена, Б.Пренеля[27], К.Карле[28], Д.Далаи и Ш.Майтры[29] построено несколько семейств функций, имеющих максимально возможную алгебраическую иммунность $\lceil \frac{n}{2} \rceil$.

---

[18]C.Carlet, S.Mesnager. Improving the upper bounds on the covering radii of binary Reed-Muller codes // IEEE Transactions on Information Theory, 2006.

[19]G.Cohen, I.Honkala, S.Litsyn, A.Lobstein. Covering codes. North-Holland, 1997.

[20]G.Kabatiansky, C.Tavernier. List decoding of second order Reed-Muller codes // In Proc. 8^{th} Intern. Simp. Comm. Theory and Applications (Ambelside, UK, july 2005).

[21]I.Dumer, G.Kabatiansky, C.Tavernier. List decoding of Reed-Muller codes up to the Johnson bound with almost linear complexity // Proceedings of ISIT 2006. Seattle, USA.

[22]R.Fourquet. Une FFT adaptee au decodage par liste dans les codes de Reed-Muller d'ordres 1 et 2 // Master-thesis of the University of Paris VIII, Thales communication, Bois Colombes, 2006.

[23]F.Didier, J.P.Tillich. Computing the algebraic immunity efficiently // Fast softwware encryption 2006, LNCS 4047, 2006. — P. 359-374.

[24]В.В Баев. Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими след-формами // Пробл. передачи информ. — 2008. — Т. 44, вып. 3. — С. 81–104.

[25]В.В Баев. Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина // Дискретная математика. — 2007. — Т. 19, вып. 4. — С. 132-138.

[26]F.Armknecht, M.Krause. Constructing single- and multi-output boolean functions with maximal algebraic immunity // International conference on automata, language and programing 2006. — LNCS 4052, Springer, 2006.— Part II. — P. 180-191.

[27]A.Braeken, B.Preneel. On the algebraic immunity of symmetric boolean functions // Indocrypt 2005. — LNCS 3797, Springer, 2005. — P. 35-48.

[28]C.Carle. A method of construction of balanced functions with optimum algebraic immunity // Cryptology ePrint archive, http://eprint.iacr.org/2006/149.

[29]D.K.Dalai, S.Maitra. Balanced Boolean functions with (more than) maximum algebraic immunity // Cryptology ePrint archive, http://eprint.iacr.org/2006/434.

Цель работы.

Получение нижних оценок нелинейностей различных порядков через значение алгебраической иммунности функции.

Научная новизна.

В диссертации получены следующие новые результаты:

1. Проблема получения нижних оценок нелинейности r-го порядка через значение алгебраической иммунности функции сводится к нахождению размерности определенных подпространств в пространстве булевых функций.
2. Доказана точная нижняя оценка нелинейности ($r = 1$) через значение алгебраической иммунности. Для всех допустимых значений параметров построены функции, на которых эта оценка достигается.
3. Получена точная нижняя оценка нелинейности второго порядка ($r = 2$) через значение алгебраической иммунности.
4. Получена новая нижняя оценка нелинейности r-го порядка через значение алгебраической иммунности при всех r.

Основные методы исследования.

В работе используются методы комбинаторики, теории множеств, теории булевых функций и линейной алгебры.

Теоретическая и практическая ценность работы.

Диссертация носит теоретический характер. Изложенные в диссертации подходы и полученные результаты представляют интерес для специалистов по криптографии и теории кодирования. Результаты диссертации могут быть использованы для дальнейшего развития теории булевых функций, а также при разработке и криптографическом анализе потоковых шифров.

Апробация работы.

Результаты диссертации докладывались на следующих научно-исследовательских семинарах и конференциях:

- Семинар "Булевы функции в криптологии"под руководством к.ф.-м.н. О.А.Логачева и к.ф.-м.н., доцента Ю.В.Таранникова (2005-2009).
- Семинар "Математические вопросы кибернетики"под руководством д.ф.-м.н., профессора О.М.Касим-Заде (21 марта 2008).
- Вторая международная конференция по проблемам безопасности и противодействия терроризму (МГУ, 25-26 октября 2006).
- VI молодежная научная школа по дискретной математике и ее приложениям (Москва, 16-21 апреля, 2007).
- IX международный семинар "Дискретная математика и ее приложения" (Москва, 18-23 июня, 2007).
- Ежегодная научная конференция "Ломоносовские чтения"(МГУ, апрель 2007)
- Международная конференция "NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security"(Звенигород, сентябрь 2007).
- XVII международная школа-семинар "Синтез и сложность управляющих систем"(Новосибирск, 27 октября - 1 ноября, 2008).
- Международная конференция "Современные проблемы математики, механики и их приложений"(Москва, 30 марта - 02 апреля, 2009).

Публикации.

Основное содержание диссертации было опубликовано в 8 работах, список которых приведен в конце автореферата [1]—[8].

Структура и объем диссертации.

Диссертация состоит из введения, 6 глав и списка литературы. Объем диссертации — 64 страницы, библиография включает 47 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** содержится обзор результатов, связанных с темой диссертации, приводится постановка задачи, дается краткое изложение основных результатов диссертации.

В **первой главе** мы обсуждаем предварительные сведения и формулируем основные определения.

Определение 1. Алгебраической иммунностью $AI(f)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n, где g не равная тождественно нулю функция с минимальной степенью, такая что $fg = 0$ или $(f + 1)g = 0$.

Определение 2. Нелинейностью r-го порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min\limits_{\deg(l)\leq r} d(f, l)$. Нелинейностью $nl(f)$ функции f называется расстояние между f и множеством аффинных функций, т. е. нелинейность первого порядка.

Вводится определение коэффициентов Уолша и раскрывается их связь с нелинейностью функции. Формулируется теорема об аффинной классификации квадратичных булевых функций.

Во **второй главе** проблема получения как можно более сильных нижних оценок нелинейности r-го порядка через значение алгебраической иммунности функции полностью сводится к задаче определения размерности некоторых подпространств $B_k(h) = \{g(x_1, \ldots, x_n) | \deg(g) \leq k, \deg(gh) \leq k\}$.

Теорема 1 *Пусть $f(x_1, \ldots, x_n)$ имеет $AI(f) = k$, тогда*

$$nl_r(f) \geq \min_{deg(g)\leq r} dim(B_{k-1}(g)).$$

Кроме того, при $k \leq \lceil \frac{n}{2} \rceil$ существует функция f_0, $AI(f_0) = k$, для которой

$$nl_r(f_0) = \min_{deg(g)\leq r} dim(B_{k-1}(g)).$$

Теорема 1 позволяет получить в качестве простых следствий некоторые оценки других авторов. Например, оценку

$$nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i}$$

из работы группы индийских исследователей[30], а также оценку

$$nl_r(f) \geq 2 \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}$$

из работы К.Карле[31] и оценку, полученную независимо автором [3] и С.Менаже[32]:

$$nl_r(g) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i} + \sum_{i=AI(f)-2r}^{AI(f)-r-1} \binom{n-r}{i}. \quad (1)$$

Но вместе с тем главное значение теоремы 1 в том, что она дает довольно хороший общий подход к проблеме, изучению которой посвящена диссертация. Этот подход будет неоднократно успешно использован в следующих главах.

Третья глава посвящена случаю обычной нелинейности $nl(f)$. В главе доказана оценка

$$nl(f) = nl_1(f) = \min_{\deg(l)\leq 1} d(f,l) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n}{i}, \quad (2)$$

и построено семейство функций

$$f_{n,k}(x_1,\ldots,x_n) = \begin{cases} 0, & \text{если} \quad wt(x_1,\ldots,x_n) < k, \\ 1, & \text{если} \quad wt(x_1,\ldots,x_n) > n-k, \\ x_1, & \text{если} \quad k \leq wt(x_1,\ldots,x_n) \leq n-k, \end{cases}$$

на которых оценка достигается при всех допустимых значениях параметров n и $AI(f)$. А именно, доказано, что

$$AI(f_{n,k}) = k$$

и

$$nl(f_{n,k}) = 2\sum_{i=0}^{k-2} \binom{n-1}{i}.$$

Также в третьей главе мы доказываем следующее утверждение:

[30]D.K.Dalai, K.C.Gupta and S.Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions // Indocrypt 2004 (Chennai, India, December 20-22, 2004) — Berlin/Heidelberg: Springer Verl., 2004. — P. 92-106.

[31]C.Carlet. On the higher order nonlinearities of algebraic immune functions // CRYPTO 2006. — Berlin/Heidelberg: Springer, 2006. — P. 584-601. (Lecture Notes in Computer Science; Vol.4117).

[32]S.Mesnager. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. Cryptology ePrint archive(http://eprint.iacr.org/), Report 2007/117.

Следствие 8. Пусть $f(x_1, \ldots, x_n)$ булева функция над F_2^n и $AI(f) = k$, $k \leq \frac{n}{2}$, тогда равенство в неравенстве (2) может достигаться не более чем на одной линейной функции l.

Там же показываем, что для функции $f_{2k+1,\,k+1}$ равенство в неравенстве (2) достигается сразу на нескольких линейных функциях l.

Четвертая глава посвящена получению оценки на нелинейность второго порядка.

В начале вводятся определения множества $S_{a_1,\ldots,a_q}(k)$ и $(a_1, \ldots, a_q)$-бесповторного полинома:

Определение 6. Пусть есть набор целых чисел $a_1 \geq a_2 \geq \ldots \geq a_q > 0$, таких что $\sum_{i=1}^{q} a_i \leq n$, тогда двоичному набору $\bar{x} = (x_1, \ldots, x_n)$ длины n можно сопоставить набор из целых чисел: $(s_1(\bar{x}), \ldots, s_q(\bar{x})) = (\sum_{i=1}^{a_1} x_i, \sum_{i=a_1+1}^{a_1+a_2} x_i, \ldots, \sum_{i=a_1+\ldots+a_{q-1}+1}^{a_1+\ldots+a_q} x_i)$. Обозначим через $S_{a_1,\ldots,a_q}(k)$ множество двоичных наборов $\bar{x}$ длины n, таких что $s_t(\bar{x}) = 0$ при некотором $t_{\bar{x}} \leq q$, $0 < s_i(\bar{x}) < a_i$ при $i < t_{\bar{x}}$ и также $k - a_{t_{\bar{x}}} < wt(\bar{x}) \leq k$.

Определение 7. Полином, в котором каждая переменная входит не более чем в один моном, будем называть бесповторным. Если полином имеет вид

$$x_1 x_2 \cdots x_{a_1} + x_{a_1+1} \cdots x_{a_1+a_2} + \cdots + x_{a_1+\ldots+a_{q-1}+1} \cdots x_{a_1+\ldots+a_q},$$

где $a_1 \geq a_2 \geq \ldots \geq a_q$, то будем его называть $(a_1, \ldots, a_q)$-бесповторным.

Для бесповторного полинома доказана теорема, которая для довольно широкого класса функций сводит проблему вычисления размерности пространства $B_k(f)$ к несложному комбинаторному подсчету:

Теорема 2 *Пусть $f(x_1, \ldots, x_n)$ — это $(a_1, \ldots, a_q)$-бесповторный полином. Тогда*

$$dim(B_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - |S_{a_1,\ldots,a_q}(k)|.$$

Известно[33, 34], что любую квадратичную булеву функцию можно аффинным преобразованием перевести в функцию с бесповторным полиномом. Благодаря этому факту и теоремам 1 и 2, доказывается точная нижняя оценка на нелинейность второго порядка:

---

[33] О.А.Логачев, А.А.Сальников, В.В.Ященко. Булевы функции в теории кодирования и криптологии // М: МЦНМО, 2004.

[34] F.J.McWilliams, N.J.A.Sloane. The Theory of Error Correcring Codes. New York: North-Holland, 1977. — 760 p.

Теорема 3 *Пусть* $f(x_1, \ldots, x_n)$ *имеет* $AI(f) = k$, *тогда*

$$nl_2(f) \geq \sum_{i=0}^{k-1} \binom{n}{i} - \sum_{i=0}^{k-1} 2^i \binom{n-2i-1}{k-1-i}. \tag{3}$$

Кроме того, при $k \leq \lceil \frac{n}{2} \rceil$ *существует функция* f_0, $AI(f_0) = k$, *для которой*

$$nl_2(f_0) = \sum_{i=0}^{k-1} \binom{n}{i} - \sum_{i=0}^{k-1} 2^i \binom{n-2i-1}{k-1-i}.$$

В **пятой главе** доказана оценка, которая является на настоящий момент рекордной для нелинейностей третьего и выше порядков:

Теорема 4 *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i} + 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}. \tag{4}$$

Доказательство этой теоремы опирается на доказанное нами утверждение:

Утверждение 17. Пусть $f(x_1, \ldots, x_n)$ булева функция, $deg(f) = k > 1$. Тогда аффинными преобразованиями ее можно привести к многочлену, который будет содержать моном $x_1 x_2 \ldots x_k$ и любой другой моном которого будет содержать не более чем $k-2$ из переменных $x_1, x_2, \ldots, x_k$.

В **шестой главе** для конкретных значений n, $AI(f)$ и $r = 2$ сравниваются оценки (1), (4) и (3). Из преведенных сравнений видно, что в случае нелинейности второго порядка оценка (3) заметно сильнее.

Также для конкретных значений n, $AI(f)$ и $r \geq 3$ сравниваются оценки (1) и (4). Оказывается, что вторая оценка существенно лучше.

Благодарности.

Автор выражает искреннюю благодарность своему научному руководителю кандидату физико-математических наук, доценту Юрию Валерьевичу Таранникову за постановку задач, постоянное внимание, многочисленные плодотворные обсуждения и помощь в работе.

Список публикаций по теме диссертации.

[1] М.С.Лобанов. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. — 2006. — Т. 18, вып. 3. — С. 152-159.

[2] М.С.Лобанов. Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций. — 2008. — Т. 15, вып. 5. — С. 47-60.

[3] М.С.Лобанов. Оценка нелинейности высоких порядков булевой функции через значение ее алгебраической иммунности // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16-21 апреля, 2007). Часть 2. — М.: Институт прикладной математики РАН, 2007. — С. 11–16.

[4] М.С.Лобанов. Новый подход к оценке нелинейности высоких порядков булевой функции через значение ее алгебраической иммунности // Материалы IX международного семинара "Дискретная математика и ее приложения"(Москва, 18-23 июня, 2007). — М.: Издательство механико-математического факультета МГУ, 2007. — С. 434-437.

[5] М.С.Лобанов. Новая нижняя оценка нелинейности высокого порядка через алгебраическую иммунность // Материалы XVII международной школы-семинара "Синтез и сложность управляющих систем"(Новосибирск, 27 октября - 1 ноября, 2008). — Новосибирск: Издательство института математики, 2008. — С. 95-98.

[6] М.С.Лобанов. Об оценках нелинейности высоких порядков через алгебраическую иммунность // Материалы международной конференции "Современные проблемы математики, механики и их приложений"(Москва, 30 марта - 02 апреля, 2009). — М: Издательство "Университетская книга", 2009. — С. 395.

[7] М.С.Лобанов. Неулучшаемая оценка нелинейности функции через значение алгебраической иммунности // Материалы II международной конференции по проблемам безопасности и противодействия терроризму (МГУ, 25-26 октября 2006). — М.: МЦНМО, 2007. — С. 210-217.

[8] M.Lobanov. Tight bounds between nonlinearity and algebraic immunity of high orders // Boolean functions in cryptology and information security. — 2008. — IOS Press. — P. 296-305. (NATO Science for Peace and Security Series D: Information and Communication Security - Vol. 18)