Московский государственный университет
имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

На правах рукописи

Омаров Рустам Рамазанович

Исследование криптографических параметров, близких к нелинейности, для булевых функций

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2013

Работа выполнена на кафедре математической кибернетики факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, профессор Алексеев Валерий Борисович.
Официальные оппоненты:	доктор физико-математических наук, профессор Леонтьев Владимир Константинович;
	кандидат физико-математических наук Таранников Юрий Валерьевич.
Ведущая организация:	Национальный исследовательский университет - Московский энергетический институт.

Защита диссертации состоится 12 апреля 2013 г. в 11 часов на заседании диссертационного совета Д 501.001.44 при Московском государственном университете имени М.В. Ломоносова по адресу: 119991, Москва, ГСП-1, Ленинские горы, 2-й учебный корпус, факультет ВМК, аудитория 685. Желающие присутствовать на заседании диссертационного совета должны сообщить об этом за два дня по тел. 939-30-10 (для оформления заявки на пропуск).

С диссертацией можно ознакомиться в фундаментальной библиотеке МГУ имени М. В. Ломоносова. С текстом автореферата можно ознакомиться на официальном сайте факультета ВМК МГУ http://cs.msu.ru/.

Автореферат разослан ___ марта 2013 г.

Ученый секретарь
диссертационного совета
профессор Н.П. Трифонов

Общая характеристика работы

Актуальность темы. Работа относится к теории дискретных функций. В диссертации рассматриваются булевы функции и их важный с криптографической точки зрения параметр нелинейность. Исследуется класс максимально нелинейных функций.

Дискретные функции широко исследуются в математике, так как с их помощью удается описывать широкий класс природных явлений. Традиционными задачами для теории дискретных функций является изучение параметров и свойств этих функций, важных с практической или теоретической точки зрения. Множество функций, обладающих определенным свойством, можно выделить в отдельный класс. Поэтому естественным образом возникают задачи получения явных конструкций таких функций для использования в практике, подсчета мощностей этих классов, что представляет определенный теоретический интерес. Часто важно знать, как разные параметры соотносятся друг с другом, находятся ли они в противоречии или дополняют друг друга.

Наиболее известным примером дискретных функций являются булевы функции. Они находят широкое применение в электронных вычислительных и управляющих системах, играют важную роль при передаче информации. В криптографии они используются при конструировании различных криптографических объектов (шифры, хэш-функции и т.п.). Основной целью, преследуемой разработчиком таких объектов, например, шифров, является максимальное затруднение их анализа противником. Развитие методов криптографического анализа привело к выделению ряда свойств, важных с криптографической точки зрения. Наличие этих свойств у функций необходимо, чтобы криптографические схемы, построенные с их использованием, успешно противостояли различным методам анализа, например статистическому, корреляционному, дифференциальному, линейному[1,2,3,4,5]. К таким свойствам можно отнести нелинейность и устойчивость

[1]Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В., *Основы криптографии*, М.:Гелиос, Ассоциация российских ВУЗов, 2001. 479 с.

[2]Бабаш А. В., Шанкин Г. П., *Криптография*, М.: Солон-Р, 2007. 512 с.

[3]Biham E., Shamir A., *Differential cryptanalysis of DES-like cryptosystems*// J. Cryptology, 1991. V. 4, N 1. 3–72.

[4]Courtois N., Meier. W., *Algebraic attacks on stream ciphers with linear feedback* // Advances in cryptology, EUROCRYPT 2003. - Berlin/Heidelberg: Springer Verl., 2003. 345–359. (Lecture Notes in Computer Science; V. 2656).

[5]Matsui M., *Linear cryptanalysis method for DES cipher*// Advancesin Cryptology - EUROCRYPT'93. Workshop on the theory and application of cryptographic techniques (Lofthus, Norway. May 23-27, 1993),

булевой функции, корреляционную и алгебраическую иммунности. Ежегодно публикуются десятки работ, посвященных изучению этих параметров, а также связей между ними[6,7,8,9].

В ряде методов криптографического анализа существенно используется „близость“ криптографических функций к функциям, обладающим простой структурой с хорошо изученными свойствами. Примером таких „плохих“ функций служат аффинные функции (в дискретной математике их обычно называют линейными). Мерой удаленности булевой функции от класса аффинных функций является ее нелинейность. Множество функций, для которых нелинейность принимает максимально возможное значение, называется множеством максимально-нелинейных функций. Известно, что при четных n нелинейность булевой функции от n переменных ограничена величиной $N_f \leq 2^{n-1} - 2^{n/2-1}$, причем для максимально-нелинейных функций это неравенство обращается в равенство.

Наличие у булевой функции свойств, близких к линейным, говорит об определенной „простоте“ этой функции, что облегчает исследование других ее параметров и свойств. Поэтому возникает практическая необходимость в построении функций, обладающих высокой или даже максимально возможной нелинейностью[10,11,12,13]. Несмотря на то, что уже построено довольно много классов максимально-нелинейных функций, не удается описать класс всех максимально-нелинейных функций. Более того, не получено близких верхних и нижних оценок на мощность этого класса. Однако,

---

Proc. Berlin: Springer, 1994. 386–397 (Lecture Notes in Comput. Sci. V. 765).

[6]Лобанов М. С., *Точное соотношение между нелинейностью и алгебраической иммунностью*// Дискретная математика, Изд-во Наука, Москва, 2006, Т. 18, вып. 3. 152–159.

[7]Тарасников Ю. В., *О корреляционно-иммунных и устойчивых булевых функциях*// Математические вопросы кибернетики. Вып. 11, М.: Физматлит, 2002. 91–148.

[8]Dalai D. K., Gupta K. C., Maitra S., *Results on algebraic immunity for cryptographically significant Boolean functions*// Progress in Cryptology: INDOCRYPT'04, LNCS V. 1880, Springer-Verlag, 2004. 92–106.

[9]Sarkar P., Maitra S., *Nonlinearity bounds and constructions of resilient Boolean functions*// CRYPTO'2000, LNCS V. 1880, Springer-Verlag, 2000. 515–532.

[10]Халявин А. В., *Построение 4-корреляционно-иммунных булевых функций от 9 переменных с нелинейностью 240*// Материалы X Международного семинара «Дискретная математика и ее приложения», Изд-во мех.-мат. факультета МГУ, Москва, 2010. 534–537.

[11]Carlet C., *Two new classes of bent functions*// Workshop on the theory and application of cryptographic techniques on Advances in cryptology, January 1994, Lofthus, Norway. 77–101.

[12]Rodier F., *Asymptotic nonlinearity of Boolean functions* // Designs, Codes and Cryptography, V. 40, N. 1, 2006. 59–70.

[13]Tarannikov Y., *New Constructions of Resilient Boolean Functions with Maximal Nonlinearity*// Revised Papers from the 8th International Workshop on Fast Software Encryption, April 02-04, 2001., 66–77.

имеется большое число результатов в этом направлении[14,15,16].

Вместе с нелинейностью можно рассматривать и нелинейность порядка r, которая определяется как минимальное расстояние между данной функцией и всеми функциями степени не более r. Если для подсчета нелинейности разработан эффективный аппарат коэффициентов Уолша, то подсчет нелинейности произвольного порядка представляет более сложную задачу. Эту проблему удается частично разрешить. Например, имеются результаты по рекурсивным оценкам на нелинейность порядка r[17], а также оценки на нелинейность через другие параметры функции[18,19].

Высокая нелинейность булевой функции означает, что она плохо приближается аффинными функциями. Однако в принципе может оказаться, что данную функцию удастся хорошо приблизить „почти аффинной“ булевой функцией. Например, наряду с нелинейностью, исследуется расстояние до множества функций, обладающих нетривиальными линейными структурами[20] (булева функция обладает нетривиальной линейной структурой, если существует ненулевой вектор a, такой что $f(x) \oplus f(x \oplus a) = const$). Также исследовалось расстояние до множества k-аффинных функций[21] (при $k \neq 0$ это множество состоит из некоторого числа аффинных и квадратичных функций). В качестве „плохих“ функций можно рассматривать и другие классы функций, например алгебраически вырожденные функции[22] (функция f называется алгебраически вырожденной, если ее можно представить в виде $f(x) = g(Ax)$, где A — некоторая матрица, а g — функция от меньшего числа переменных).

Анализ конкретных криптографических объектов часто приводит к ре-

[14]Agievich S. V., *On the representation of bent functions by bent rectangles* // Fifth Int. Petrozavodsk conf. on probabilistic methods in discrete mathematics. Proc. Boston: VSP, 2000. 121–135.

[15]Carlet C., Klapper A., *Upper bounds on the numbers of resilient functions and of bent functions* // 23rd Symposium on Information Theory (Benelux, Belgium. May, 2002). Proc. 2002. 307–314.

[16]Tokareva N. N., *On the number of bent functions from iterative constructions: lower bounds and hypotheses* // Advances in Mathematics of Communications (AMC), 2011, V. 5, N 4. 609–621.

[17]Carlet C., *Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications*// IEEE Transactions on Information Theory, V. 54, N. 3, 2008. 1262–1272.

[18]Лобанов М. С., *Точные соотношения между нелинейностью и алгебраической иммунностью*// Дискретная математика и исследование операций, Изд-во Наука, Москва, 2008, Т. 15, вып. 6. 34–47.

[19]Лобанов М. С., *Получение нижних оценок на нелинейность булевой функции через размерность некоторых подпространств*, Материалы X Международного семинара «Дискретная математика и ее приложения», Изд-во мех.-мат. факультета МГУ, Москва, 2010. 416–419.

[20]Meier W., Staffelbach O. *Nonlinearity criteria for cryptographic functions* // LNCS. 1990. V. 434. 549–562.

[21]Токарева Н. Н. *Сильно нелинейные булевы функции: бент-функции и их обобщения.* Диссертация на соискание ученой степени кандидата физико-математических наук, Новосибирск, 2008.

[22]Алексеев Е. К., *Аппроксимация дискретных функций алгебраически вырожденными функциями в анализе систем защиты информации.* Диссертация на соискание ученой степени кандидата физико-математических наук, Москва, 2011.

шению систем булевых уравнений вида

$$\begin{cases} f(\tilde{a}_1, \tilde{x}) = c_1, \\ \qquad \dots \\ f(\tilde{a}_m, \tilde{x}) = c_m; \end{cases}$$

для некоторого неизвестного вектора $\tilde{x}$. Для произвольной булевой функции f такие системы плохо решаются. Предположим, что для некоторой булевой функции $g(\tilde{a}, \tilde{x})$ с достаточно большой вероятностью выполняется равенство $f(\tilde{a}, \tilde{x}) = g(\tilde{a}, \tilde{x})$, тогда с определенной вероятностью будет выполняться система равенств

$$\begin{cases} g(\tilde{a}_1, \tilde{x}) = c_1, \\ \qquad \dots \\ g(\tilde{a}_m, \tilde{x}) = c_m. \end{cases}$$

Если функция g – аффинная относительно $\tilde{x}$, то получим линейную систему, которая быстро решается, и мы с определенной вероятностью находим решение исходной системы. Однако решение можно быстро найти и в тех случаях, когда функция g в своем полиноме Жегалкина содержит не более k нелинейных слагаемых. Заменяя каждый моном вида $x_{i_1} \dots x_{i_s}$ на соответствующую переменную $u_{i_1,\dots,i_s}$, мы придем к некоторой линейной системе. Если исходная нелинейная система содержала n неизвестных, то полученная линейная система будет содержать не более $n+k$ неизвестных. При фиксированном k сложность решения такой линейной системы будет $O(n^3)$. Находя решения этой линейной системы и проверяя их на необходимую связь между переменными, мы с некоторой вероятностью можем быстро получить решение исходной системы.

Таким образом, для криптографических целей нужно, чтобы функция f плохо приближалась не только аффинными, но и „почти аффинными“ функциями. В диссертации в качестве „почти аффинных“ функций рассматриваются функции с небольшим числом нелинейных слагаемых в их полиноме Жегалкина.

Целью диссертационной работы является исследование расстояния от класса максимально-нелинейных функций до класса функций, у которых в полиноме Жегалкина присутствует не более фиксированного числа k нелинейных слагаемых.

Методы исследования. При выполнении диссертационного исследования использовались методы дискретной математики и алгебры.

Научная новизна. Все результаты диссертации являются новыми. А именно, изучен новый параметр – расстояние от максимально-нелинейных булевых функций до класса всех функций, у которых в полиноме Жегалкина присутствует не более фиксированного числа k нелинейных слагаемых. Для минимума этого расстояния по множеству всех максимально-нелинейных булевых функций от $2n$ переменных при произвольном k получены близкие нижние и верхние оценки. При $k = 1$ получена точная формула. Для функций из класса Мэйорана–Мак-Фарланда при $k = 1$ получены точные границы, в которых изменяется это расстояние. При $k = 2$ получена точная формула для минимума этого расстояния по множеству всех максимально-нелинейных булевых функций от $2n$ переменных из класса Мэйорана–Мак-Фарланда.

Достоверность полученных в диссертации результатов обусловлена строгостью математических доказательств, использованием апробированных научных методов и средств.

Теоретическая и практическая значимость работы. Результаты диссертации имеют теоретический характер и состоят в получении новых оценок важных криптографических параметров. Полученные результаты дают дополнительные аргументы в пользу применения максимально-нелинейных булевых функций в практических системах защиты информации.

Соответствие диссертации паспорту научной специальности. Диссертация соответствует паспорту специальности 01.01.09, поскольку исследования в ней относятся к научному направлению «Дискретная математика».

Апробация результатов. Результаты, полученные в диссертации, докладывались и обсуждались на международных конференциях: X международном семинаре «Дискретная математика и её приложения» (Москва, 2010), VIII международной конференции «Колмогоровские чтения» (Ярославль, 2010), XVI международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 2011), XI международном семинаре «Дискретная математика и её приложения» (Москва, 2012).

Кроме того, результаты обсуждались на научном семинаре «Дискретная математика и математическая кибернетика» кафедры математической кибернетики факультета ВМК МГУ.

Публикации. Результаты автора по теме диссертации опубликованы в 6 работах, список которых приводится в конце автореферата; 2 из них опубликованы в журналах из списка ВАК.

Личный вклад автора. Основные результаты диссертации получены автором. В работах, опубликованных в соавторстве с В.Б. Алексеевым, В.Б. Алексееву принадлежит постановка задач, общее руководство исследованиями и обсуждение новых подходов.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения и библиографии, включающей 29 наименований. Общий объем диссертации составляет 75 страниц.

Краткое содержание работы

Во введении содержится история вопроса, обосновывается актуальность темы исследования. В нём сформулирована цель диссертации, описана структура диссертации и перечислены основные результаты.

В первой главе приводятся основые определения и вспомогательные утверждения.

Пусть n - произвольное натуральное число. Через V_n будем обозначать векторное пространство наборов длины n с компонентами из $\{0,1\}$ с операцией $\oplus$ покоординатного сложения векторов по модулю 2. Под *булевой функцией* от n переменных будем понимать отображение $f : V_n \to \{0,1\}$. Ее *весом* $wt(f)$ будем называть количество наборов, на которых она равна 1. *Расстоянием* от булевой функции f до булевой функции g называется величина $dist(f,g) = wt(f \oplus g)$, т.е. число наборов, на которых значения функций f и g различаются. *Расстоянием от f до множества M булевых функций от n переменных* называется величина $dist(f,M) = \min\limits_{g \in M} dist(f,g)$. Под *расстоянием между двумя множествами булевых функций M и N* будем понимать $dist(M,N) = \min\limits_{\substack{g \in M \\ h \in N}} dist(g,h)$.

Пусть x и y – два произвольных вектора из V_n. Через $\langle x,y \rangle$ будем обозначать их *скалярное произведение* над полем $GF(2)$ с двумя элементами 0 и 1: $\langle x,y \rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$ (здесь $\oplus$ – это сложение по модулю 2). Булева функция f от n переменных называется *аффинной*, если существуют $a = (a_1,\ldots,a_n) \in V_n$ и $c \in \{0,1\}$ такие, что $f(x) = \langle a,x \rangle \oplus c$. Множество всех аффинных булевых функций от n переменных будем обозначать A_n. Расстояние $dist(f,A_n)$ от булевой функции $f(x)$ от n переменных до множества A_n аффинных булевых функций называется *нелинейностью* функции $f(x)$ и обозначается через N_f.

Булевы функции $f(x)$, для которых N_f равно максимально возможному

значению среди всех функций от n переменных, называют *максимально-нелинейными* функциями (в случае четного n это расстояние равно $N_f = 2^{n-1} - 2^{n/2-1}$). Множество таких функций будем обозначать через B_n.

Далее рассматривается множество приближающих функций, у которых в полиноме Жегалкина присутствует не более k нелинейных слагаемых.

Определение. Через AE_n^k будем обозначать класс всех почти аффинных функций от n переменных, а именно, функций вида $X_{I_1} \oplus \ldots \oplus X_{I_k} \oplus l(x)$, где $X_{I_t} = \prod\limits_{j \in I_t} x_j$, I_t – произвольные подмножества (возможно, пустые: $X_\varnothing = 0$) множества $\{1, \ldots, n\}$, $t = \overline{1,k}$ и $l(x) \in A_n$. При $k = 1$ будем писать AE_n.

Введем следующую функцию $\rho_k(U) = dist(U, AE_{2n}^k)$, где U — некоторое множество функций от $2n$ переменных. В следующей теореме получена нижняя оценка для расстояния между классом максимально-нелинейных функций от $2n$ переменных и множеством приближающих функций AE_{2n}^k.

Теорема 1. *Пусть B_{2n} — множество всех максимально-нелинейных функций от $2n$ переменных, тогда*

$$\rho_k(B_{2n}) \geq 2^{2n-1} - 3^k \cdot 2^{n-1}.$$

Возникает вопрос, насколько оценка из теоремы 1 точна. Оказывается для некоторого известного класса максимально-нелинейных функций удается ответить на этот вопрос.

Определение. Пусть $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$. Класс Мэйорана–Мак-Фарланда определяется как класс всех булевых функций $f(x, y)$ от $2n$ переменных вида $f(x, y) = \langle \pi(y), x \rangle \oplus \Phi(y)$, где π – произвольная подстановка на множестве V_n, а $\Phi(y)$ – произвольная булева функция от n переменных. Будем обозначать его через M_{2n}.

Для класса Мэйорана–Мак-Фарланда удается доказать следующие два утверждения.

Теорема 2. *При любом $k > 0$ и $n = pk + t, 0 \leq t < k$ выполняется:*

$$\rho_k(M_{2n}) \leq 2^{2n-1} - 3^k \cdot \left(1 - \frac{4}{3 \cdot 2^p}\right)^k \cdot 2^{n-1}.$$

Следствие 1. *При любом фиксированном k и $n \to \infty$ выполняется:*

$$\rho_k(M_{2n}) \leq 2^{2n-1} - 3^k \cdot 2^{n-1} + o(2^{n-1}).$$

С учетом того, что $\rho_k(B_{2n}) \leq \rho_k(M_{2n})$, из теоремы 1 и следствия 1 получаем.

Теорема 3. *При любом фиксированном k и $n \to \infty$ выполняется:*

$$\rho_k(B_{2n}) = 2^{2n-1} - 3^k \cdot 2^{n-1} + o(2^{n-1}).$$

Теорема 4. *При любом фиксированном k и $n \to \infty$ выполняется:*

$$\rho_k(M_{2n}) = 2^{2n-1} - 3^k \cdot 2^{n-1} + o(2^{n-1}).$$

Легко заметить, что, в отличие от класса A_n, класс AE_n^k не является замкнутым относительно невырожденных афинных преобразований. Поэтому интерес также представляет исследование расстояния до класса, содержащего все функции из AE_n^k, а также все функции, аффинно эквивалентные им. В частности, интересно, сохранятся ли полученные для AE_n^k оценки?

Определение. Через $\widetilde{AE}_n^k$ будем обозначать класс всех функций, аффинно эквивалентных функциям из класса AE_n^k, а именно, функций вида $g(Ax \oplus d)$, где $g \in AE_n^k$, A — произвольная невырожденная над полем $GF(2)$ матрица размера $n \times n$, а $d \in V_n$ — произвольный вектор и вычисление $Ax \oplus d$ производится в поле $GF(2)$. При $k = 1$ будем писать $\widetilde{AE}_n^1 = \widetilde{AE}_n$.

Определим функцию $\widetilde{\rho}_k(U)$ как $\widetilde{\rho}_k(U) = dist(U, \widetilde{AE}_{2n}^k)$, где U — некоторое множество функций от $2n$ переменных.

Следующая теорема говорит о том, что добавление к функциям класса AE_{2n}^k всех функций, аффинно эквивалентных им, не сокращает расстояние от класса B_{2n} до приближающего класса $\widetilde{AE}_{2n}^k$ по сравнению с $\rho_k(B_{2n})$.

Теорема 5. *Для множества максимально-нелинейных функций B_n верно*

$$\widetilde{\rho}_k(B_n) = \rho_k(B_n)$$

и, следовательно, при любом фиксированном k и $n \to \infty$

$$\widetilde{\rho}_k(B_{2n}) = 2^{2n-1} - 3^k \cdot 2^{n-1} + o(2^{n-1}).$$

В первой главе мы попытались ответить на вопрос: Как изменится расстояние между классами B_{2n} и A_{2n}, если перейти от последнего к AE_{2n}^k или

$\widetilde{AE}^k_{2n}$. К сожалению, класс B_{2n} полностью не описан, что затрудняет получение точного значения. Но для малого значения параметра k и класса максимально-нелинейных функций M_{2n} удается получить точный ответ.

Во второй главе получена точная формула для расстояния от классов B_{2n} и M_{2n} до классов AE_{2n} и $\widetilde{AE}_{2n}$ при всех n.

Теорема 6. *Для класса всех максимально-нелинейных функций B_{2n} при всех $n \geq 2$ выполняется равенство:*

$$\rho_1(B_{2n}) = 2^{2n-1} - 3 \cdot 2^{n-1} + 2.$$

(При $n = 1$ $\rho_1(B_{2n}) = 0$.)

Примером максимально-нелинейной функции, для которой $dist(f, AE_{2n}) = 2^{2n-1} - 3 \cdot 2^{n-1} + 2$ служит $f(x, y) = \langle x, y \rangle \oplus y_1 \oplus \ldots \oplus y_n \oplus sg(y_1, \ldots, y_n)$, где $sg(0, \ldots, 0) = 0$ и $sg(y_1, \ldots, y_n) = 1$, если $(y_1, \ldots, y_n) \neq (0, \ldots, 0)$.

Следствие 2. *Для класса максимально-нелинейных функций M_{2n} при всех $n \geq 2$ выполняется равенство:*

$$\rho_1(M_{2n}) = 2^{2n-1} - 3 \cdot 2^{n-1} + 2.$$

(При $n = 1$ $\rho_1(M_{2n}) = 0$.)

Доказательство следует из того факта, что указанная выше $f(x, y) \in M_{2n}$.

Класс M_{2n} не является инвариантным относительно невырожденных аффинных преобразований.

Определение. Обозначим через H^k_{2n} — множество функций от n переменных вида:

$$h(x) = f(l_1(x), \ldots, l_{2n}(x)),$$

где $l_i \in A_{2n}, i = \overline{1, 2n}$, $f(x) \in AE^k_{2n}$.

Заметим, что $\widetilde{AE}^k_{2n} \subset H^k_{2n}$ и $dist(M_{2n}, H^k_{2n}) \leq \widetilde{\rho}_k(M_{2n})$.

Следствие 3. *Для класса максимально-нелинейных функций M_{2n} при всех $n \geq 2$ выполняется равенство:*

$$dist(M_{2n}, H^1_{2n}) = 2^{2n-1} - 3 \cdot 2^{n-1} + 2.$$

При $n = 1$ $dist(M_{2n}, H^1_{2n}) = 0$.

Также удается показать, что не все максимально-нелинейные функции одинаково хорошо приближаются функциями из AE_{2n}.

Теорема 7. *Для любой максимально-нелинейной функции $f(x) \in B_{2n}$ верно неравенство:*

$$dist(f, AE_{2n}) \leq 2^{2n-1} - 2 \cdot 2^{n-1},$$

причем при всех $n \geq 2$ существуют максимально-нелинейные функции от $2n$ переменных, для которых это неравенство обращается в равенство.

Более того, теорема 7 останется верной, если от AE_{2n} перейти к $\widetilde{AE}_{2n}$.

Теорема 8. *При всех $n \geq 2$ существуют максимально-нелинейные функции от $2n$ переменных, для которых*

$$dist(f, \widetilde{AE}_{2n}) = 2^{2n-1} - 2 \cdot 2^{n-1}.$$

В третьей главе исследуется расстояние между классом максимально-нелинейных функций M_{2n} и классом „почти“ линейных функций AE^2_{2n}. Получена точная формула для этого расстояния при всех n. Показано, что существуют функции, расстояние от которых до класса AE^2_{2n} заведомо не достигает этой величины.

Теорема 9. *Верно равенство:*

$$\rho_2(M_{2n}) = 2^{2n-1} - 9 \cdot 2^{n-1} + 6\left(2^{\lfloor \frac{n}{2} \rfloor} + 2^{\lceil \frac{n}{2} \rceil}\right) - 8$$

при $n \geq 6$. При $n = 1, 2, 3, 4, 5$ величина $\rho_2(M_{2n})$ равна $0, 0, 16, 88, 416$ соответственно.

Теорема 10. *При всех $n \geq 2$ существуют максимально-нелинейные функции от $2n$ переменных, для которых*

$$dist(f, AE^2_{2n}) = 2^{2n-1} - 4 \cdot 2^{n-1}.$$

Основные результаты, выносимые на защиту

1. Получены нижние и верхние оценки для расстояния от класса всех максимально-нелинейных функций от $2n$ переменных до класса функций, у которых в полиноме Жегалкина присутствует не более фиксированного числа k нелинейных слагаемых. Показано также, что это

расстояние не меняется, если в класс приближающих функций добавить все функции аффинно эквивалентные функциям из этого класса. Установлено, что это расстояние уменьшается по сравнению с нелинейностью рассматриваемых функций на величину, асимптотически равную $(3^k - 1) \cdot 2^{n-1}$ при n, стремящемся к бесконечности.

2. Получена точная формула для расстояния от класса всех максимально-нелинейных функций от $2n$ переменных до класса функций, у которых в полиноме Жегалкина присутствует не более одного нелинейного слагаемого. Показано, что для различных максимально-нелинейных функций расстояние до класса функций, у которых в полиноме Жегалкина присутствует не более одного нелинейного слагаемого, может быть различным. Для функций из класса Мэйорана–Мак-Фарланда получены точные границы, в которых изменяется это расстояние.

3. Получена точная формула для расстояния от класса максимально-нелинейных функций Мэйорана–Мак-Фарланда от $2n$ переменных до класса функций, у которых в полиноме Жегалкина присутствует не более двух нелинейных слагаемых.

Благодарности

Автор выражает благодарность своему научному руководителю, доктору физико-математических наук, профессору Алексееву Валерию Борисовичу за постановку задачи и постоянное внимание к работе.

Публикации автора по теме диссертации

[1] Алексеев В. Б., Омаров Р. Р., *"О приближении максимально-нелинейных булевых функций почти линейными функциями"*, Дискретная математика, Изд-во Наука, Москва, 2012, Т. 24, вып. 3, 73–81

[2] Алексеев В. Б., Омаров Р. Р., *"Исследование одного параметра булевых функций, близкого к нелинейности"*, Научные ведомости Белгородского государственного университета, 2009, Т. 15(70), № 12/1, 81–87

[3] Омаров Р. Р., *"О расстояниях от максимально-нелинейных функций до некоторого класса булевых функций"*, Материалы XI Международ-

ного семинара «Дискретная математика и ее приложения», Изд-во мех.-мат. факультета МГУ, Москва, 2012, 425–428

[4] Алексеев В. Б., Омаров Р. Р., *"О приближении булевых функций почти линейными функциями"*, Материалы X Международного семинара «Дискретная математика и ее приложения», Изд-во мех.-мат. факультета МГУ, Москва, 2010, 514–516

[5] Алексеев В. Б., Омаров Р. Р., *"О приближении одного класса максимально-нелинейных булевых функций почти аффинными функциями"*, Труды VIII Международных Колмогоровских чтений, Изд-во ЯГПУ, Ярославль, 2010, 98–104

[6] Алексеев В. Б., Омаров Р. Р., *"О расстояниях от максимально-нелинейных булевых функций до почти аффинных функций"*, Материалы XVI Международной конференции «Проблемы теоретической кибернетики», Нижегородский университет, Нижний Новгород, 2011, 24–28