На правах рукописи

Коломеец Николай Александрович

БЕНТ-ФУНКЦИИ, АФФИННЫЕ НА ПОДПРОСТРАНСТВАХ, И ИХ МЕТРИЧЕСКИЕ СВОЙСТВА

Специальность 01.01.09 — Дискретная математика и математическая кибернетика

Автореферат

диссертации на соискание учёной степени

кандидата физико-математических наук

Новосибирск — 2014

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН)

Научный руководитель: **Токарева Наталья Николаевна**, кандидат физико-математических наук, с.н.с.

Официальные оппоненты: **Черёмушкин Александр Васильевич**, доктор физико-математических наук, профессор, Институт криптографии, связи и информатики;

Панкратова Ирина Анатольевна, кандидат физико-математических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет».

Ведущая организация: Институт проблем информационной безопасности Московского государственного университета им. М. В. Ломоносова.

Защита состоится 15 октября 2014 г. в 16 час. 30 мин. на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга, 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук.

Автореферат разослан "____"_____ 2014 г.

Ученый секретарь
диссертационного совета
Д 003.015.01, д.ф.-м.н. Ю. В. Шамардин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Работа посвящена исследованию важного класса булевых функций, обладающих максимальной нелинейностью. Это класс бент-функций. Бент-функции интересны не только из-за экстремального значения нелинейности, но и из-за большого числа приложений в криптографии, теории кодирования, алгебре, теории символьных последовательностей.

Приведем необходимые определения.

Функция вида $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных, $x \in \mathbb{Z}_2^n$ — *двоичным вектором* длины n, $x = (x_1, \ldots, x_n)^T$. Через $\mathcal{F}_n$ обозначим множество всех булевых функций от n переменных. Для $x, y \in \mathbb{Z}_2^n$ определим $x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)^T$, где $\oplus$ — сложение по модулю 2. Введем аналог скалярного произведения по модулю 2:

$$\langle x, y \rangle = x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_n y_n.$$

Отметим, что $\langle x, y \rangle$ не является скалярным произведением в полном смысле этого понятия, поскольку не все свойства скалярного произведения верны в двоичном случае.

Аффинной булевой функцией от n переменных называется функция вида

$$\ell_{a,c}(x) = \langle a, x \rangle \oplus c \text{ для некоторых } a \in \mathbb{Z}_2^n, c \in \mathbb{Z}_2.$$

Через $\mathcal{A}_n$ обозначается множество всех аффинных функций от n переменных. *Расстоянием Хэмминга* между двумя двоичными векторами $x, y \in \mathbb{Z}_2^n$ называется число координат, в которых x и y различаются. *Расстоянием* между двумя булевыми функциями $f, g \in \mathcal{F}_n$ называется расстояние Хэмминга между векторами их значений, оно обозначается как $\mathrm{dist}(f, g)$. Булевы функции $f, g \in \mathcal{F}_n$ называются *аффинно эквивалентными*, если существует невырожденная двоичная матрица A размера $n \times n$, вектор $b \in \mathbb{Z}_2^n$ и аффинная функция $\ell \in \mathcal{A}_n$, такие что

$$f(x) = g(Ax \oplus b) \oplus \ell(x) \text{ для всех } x \in \mathbb{Z}_2^n.$$

Нелинейностью N_f булевой функции $f \in \mathcal{F}_n$ называется расстояние от f до множества всех аффинных функций:

$$N_f = \min_{g \in \mathcal{A}_n} \mathrm{dist}(f, g).$$

Булева функция $f \in \mathcal{F}_n$ называется *максимально нелинейной*, если N_f принимает максимальное возможное значение. В случае чётного n максимальное N_f известно:

$$\max_{f \in \mathcal{F}_n} N_f = 2^{n-1} - 2^{n/2-1}.$$

Все булевы функции, обладающие такой нелинейностью, называются **бент-функциями**. Таким образом, бент-функции существуют только для чётного числа переменных, и в этом случае являются максимально нелинейными. В случае нечётного n точное значение максимальной нелинейности неизвестно.

Преобразованием Уолша—Адамара функции $f \in \mathcal{F}_n$ называется функция $W_f : \mathbb{Z}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x,y \rangle},$$

при этом сами числа $W_f(y)$ называются *коэффициентами Уолша—Адамара*. Коэффициенты Уолша—Адамара однозначно определяют функцию f. Также они тесно связаны с расстоянием от функции f до аффинных функций:

$$\mathrm{dist}(f, \ell_{y,0}) = 2^{n-1} - \frac{1}{2} W_f(y).$$

Поскольку $\mathrm{dist}(f, \ell_{y,1}) = 2^n - \mathrm{dist}(f, \ell_{y,0})$, то

$$N_f = 2^{n-1} - \frac{1}{2} \max_{y \in \mathbb{Z}_2^n} |W_f(y)|.$$

Для коэффициентов Уолша—Адамара справедливо равенство Парсеваля:

$$\sum_{y \in \mathbb{Z}_2^n} W_f^2(y) = 2^{2n}.$$

Из него следует, что $N_f \leq 2^{n-1} - 2^{n/2-1}$. Так как коэффициенты Уолша—Адамара являются удобным инструментом для подсчёта нелинейности, бент-функции часто определяют следующим образом: $g \in \mathcal{F}_{2k}$ называется бент-функцией, если $|W_g(y)| = 2^k$ для всех $y \in \mathbb{Z}_2^{2k}$. Множество всех бент-функций от $2k$ переменных обозначают через $\mathfrak{B}_{2k}$. Оба приведенных определения бент-функций являются эквивалентными.

Сдвигом $s \oplus D$ множества D, $s \in \mathbb{Z}_2^n$, $D \subseteq \mathbb{Z}_2^n$ называется множество $\{s \oplus x \mid x \in D\}$. Множество $L \subseteq \mathbb{Z}_2^n$ называется *аффинным подпространством* $\mathbb{Z}_2^n$ (или просто *подпространством*), если оно является сдвигом некоторого линейного подпространства $\mathbb{Z}_2^n$. *Размерностью* аффинного подпространства называется размерность соответствующего линейного подпространства. Функция $f \in \mathcal{F}_n$ *аффинна на подпространстве* L, $L \subseteq \mathbb{Z}_2^n$, если

$$f|_L(x) = \langle a, x \rangle \oplus c \text{ , где } a \in \mathbb{Z}_2^n,\ c \in \mathbb{Z}_2.$$

Нелинейность — одно из важнейших криптографических свойств булевых функций. В частности, алгоритм симметричного шифрования DES (Data

Encryption Standard), бывший американский стандарт блочного шифрования, был заменён на AES (Advanced Encryption Standard) в том числе из-за низкой нелинейности некоторых булевых функций его S-блоков (узлов замены), и, как следствие, уязвимости к линейному криптоанализу[1]. Помимо нелинейности, к криптографическим свойствам относится уравновешенность, критерий распространения, строгий лавинный критерий, корреляционная иммунность, алгебраическая иммунность, см., например, работу О. А. Логачёва, А. А. Сальникова, В. В. Ященко[2]. Некоторые из перечисленных свойств похожи, например, строгий лавинный критерий и критерий распространения; функции, удовлетворяющие критерию распространения максимального порядка, являются максимально нелинейными. Некоторые же свойства могут противоречить друг другу: максимально нелинейные булевы функции от чётного числа переменных не могут быть ни сбалансированными, ни корреляционно иммунными. Приведем примеры свойств и их сочетаний, востребованных в криптографии: высокая нелинейность[3], корреляционная иммунность[4], высокая нелинейность, уравновешенность и корреляционная иммунность[5], высокая нелинейность и алгебраическая иммунность[6] [7] .

Бент-функции были предложены О. Ротхаусом в 1960-х годах, хотя его работа[8] была опубликована только в 1976 г. Известно, что и в СССР в 60-х занимались исследованием бент-функций, В. А. Елисеев и О. П. Степченков называли их *минимальными*. Имея оптимальную нелинейностью, бент-функции не обладают рядом других важных криптографических свойств, например, не являются сбалансированными. Булева функция называется *сбалансированной* или *уравновешенной*, если она принимает значения 0 и 1 одинаково часто. Отсутствие сбалансированности препятствует использованию

[1] Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93. Workshop on the theory and application of cryptographic techniques (Lofthus, Norway. May 23–27, 1993). Proc. Berlin: Springer, 1994. — P. 386–397 (Lecture Notes in Computer Science. — V. 765).

[2] Логачёв О. А., Сальников А. А., Ященко В. В. Криптографические свойства дискретных функций // Материалы конференции «Московский университет и развитие криптографии в России», МГУ, 2002. М.: МЦНМО, 2003. — С. 174–199.

[3] Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken: LAP LAMBERT Academic Publishing, 2011. — 180 с.

[4] Siegentaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. — 1984. — V. 30, N 5. — P. 776–780.

[5] Tarannikov Yu. On Resilient Boolean Functions with Maximal Possible Nonlinearity // INDOCRYPT 2000 — First International Conference in Cryptology in India (Calcutta, India. December 10–13, 2000). Proc. Springer. 2000. P. 19–30 (Lecture Notes in Computer Science. — V. 1977).

[6] Лобанов М. С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. — 2006. — Т. 18, № 3. — С. 152–159.

[7] Tu Z., Deng Y. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity // Designs, Codes and Cryptography. — 2011. — V. 60, N 1. — P. 1–14.

[8] Rothaus O. On bent functions // J. Combin. Theory, Ser. A. — 1976. — V. 20, N 3. — P. 300–305.

бент-функций как координатных функций во взаимно однозначных S-блоках блочных шифров. Одним из путей решения проблемы является построение криптографических булевых функций путем модификации имеющейся бент-функции, поскольку во многих случаях можно гарантировать, что нелинейность функции по-прежнему останется высокой. Ещё один путь — использование различных обобщений бент-функций, например, полу-бент-функций[9].

Бент-функции в явном виде используются в S-блоках канадского блочного шифра CAST-128[10] (а также в шифре CAST-256). Поскольку данный шифр является сетью Фейстеля, он не требует взаимной однозначности от используемых S-блоков. Прямая сумма бент-функции и аффинной функции (сумма булевых функций от непересекающихся переменных) используется в хэш-функции HAVAL[11]. В качестве бент-функций для HAVAL выбраны представители четырёх различных классов аффинной эквивалентности бент-функций от 6 переменных. В поточном шифре GRAIN[12] в качестве функции обратной связи в нелинейном регистре сдвига используется прямая сумма квадратичной бент-функции и линейной функции от подмножества битов.

Помимо криптографических приложений, бент-функции связаны с такими комбинаторными объектами как матрицы Адамара, разностные множества (в частности, Р. Л. МакФарланд[13] и Дж. Диллон[14] исследовали бент-функции в терминах разностных множеств), сильно регулярные графы[15]. Последовательности, построенные по бент-функциям, обладают предельно низкой автокорреляцией и взаимной корреляцией[16].

Несмотря на большой интерес к бент-функциям, до сих пор остаётся множество открытых вопросов в этой области. Неизвестно точное число бент-функций, нет даже его приемлемых оценок. Существует множество различ-

[9] Chee S., Lee S., Kim K. Semi-bent Functions // Advances in Cryptology — ASIACRYPT'94 — 4th International Conference on the Theory and Applications of Cryptology. (Wollongong, Australia. November 28 – December 1, 1994). Proc. Berlin: Springer. 1995. P. 107–118 (Lecture Notes in Computer Science. — V. 917).

[10] Adams C. M. Constructing Symmetric Ciphers Using the CAST Design Procedure // Designs, Codes, and Cryptography. — 1997. — V. 12. — P. 283–316.

[11] Zheng Yu., Pieprzyk J., Seberry J. HAVAL — a one-way hashing algorithm with variable length of output // Advances in Cryptology — AUSCRYPT'92 (Queensland, Australia, December 13–16, 1992) Proc. Springer-Verlag, 1993. — P. 83–104 (Lecture Notes in Computer Science. — V. 718).

[12] Hell M., Johansson T., Maximov A., Meier W. A Stream Cipher Proposal: Grain-128. Режим доступа: `http://www.ecrypt.eu.org/stream/p2ciphers/grain/Grain128_p2.pdf`

[13] McFarland R. L. A family of difference sets in non-cyclic groups // J. Combin. Theory, Ser. A. — 1973. — V. 15. — P. 1–10.

[14] Dillon J. F. Elementary Hadamard Difference sets // Ph. D. Thesis, Univ. of Maryland, 1974.

[15] Bernasconi A., Codenotti B., VanderKam J. M. A characterization of bent functions in terms of strongly regular graphs // IEEE Trans. Computers. — 2001. — V. 50, N 9. — P. 984–985.

[16] Olsen J. D., Scholtz R. A., Welch L. R. Bent-function sequences // IEEE Trans. Inform. Theory. — 1982. — V. 28, N 6. — P. 858–864.

ных конструкций бент-функций. Одни из самых первых — класс Мэйорана—МакФарланда (Р. Л. МакФарланд, 1973) и частичное расщепление (Дж. Диллон, 1974). Помимо них предложены итеративные конструкции (О. Ротхаус, 1976, А. Канто, П. Шарпин, 2003), алгебраические конструкции (подход к булевым функциями через функции вида $GF(2^n) \to GF(2)$) (Дж. Диллон, 1974, Х. Доббертин, 1994, Дж. Диллон, Х. Доббертин, 2004, Г. Леандр, 2006, А. Канто, П. Шарпин, Г. Карегян, 2008). Исследуются такие подклассы класса бент-функций как нормальные и слабо нормальные бент-функции, однородные бент-функции, мономиальные бент-функции, квадратичные бент-функции. Рассматриваются алгоритмы порождения бент-функций. При этом из-за большого разрыва между известными нижними и верхними оценками числа бент-функций не ясно, насколько известные конструкции покрывают весь класс бент-функций.

Множество статей посвящено обобщениям бент-функций. Большой интерес представляют гипер-бент-функции, которые определяются как функции, находящиеся на максимальном возможном расстоянии от множества собственных мономиальных функций[17]. Ценные практические приложения имеют векторные обобщения[18].

Задача нахождения метрической структуры ставилась для различных классов булевых функций, например, для кодов Рида—Маллера[19] [20] , симметрических булевых функций[21]. В данной работе исследуется расположение двух бент-функций на минимальном расстоянии друг от друга. Отметим, что более широко метрические свойства класса бент-функций, например, спектр возможных расстояний между двумя бент-функциями, связаны с гипотезой, высказанной Н. Н. Токаревой[22], о том, что любую булеву функцию от $2k$ переменных степени не больше k можно представить как сумму двух бент-функций от $2k$ переменных. Данная гипотеза, в частности, связана с асимпто-

[17] Youssef A., Gong G. Hyper-bent functions // Advances in cryptology — EUROCRYPT'2001. Int. conference on the theory and application of cryptographic techniques (Innsbruk, Austria. May 6–10, 2001). Proc. Berlin: Springer, 2001. — P. 406–419 (Lecture Notes in Computer Science. — V. 2045).

[18] Nyberg K. Perfect nonlinear S-boxes // Advances in cryptology — EUROCRYPT'1991. Int. conference on the theory and application of cryptographic techniques (Brighton, UK. April 8–11, 1991). Proc. Berlin: Springer, 1991. — P. 378–386 (Lecture Notes in Computer Science. — V. 547).

[19] Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки: Пер. с англ. / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М.: Радио и связь, 1979. — 744 с.

[20] Kasami T., Tokura N. On the Weight Structure of Reed–Muller Codes // IEEE Trans. Inform. Theory. — 1970. — V. 16, N 6. — P. 752–759.

[21] Ивченко Г. И., Медведев Ю. И., Миронова В. А. Симметрические булевы функции и их метрические свойства // Математические вопросы криптографии. — 2013. — Т. 4, № 4. — С. 49—63.

[22] Tokareva N. On the number of bent functions from iterative constructions: lower bounds and hypothesis // Adv. Math. Commun. — 2011. — V. 5, N 4. — P. 609–621.

тикой мощности класса бент-функций. В. Н. Потапов[23] доказал, что расстояния между двумя бент-функциями от $2k$ переменных в интервале от 2^k до $2^{k+1}-1$ (от минимального до удвоенного минимального) имеют вид $2^{k+1}-2^t$, где $1 \leq t \leq k$.

Целью данной работы является исследование метрических свойств класса бент-функций, связанных с аффинностью бент-функции на аффинном подпространстве, а именно, исследование расположения двух бент-функций на минимальном возможном расстоянии друг от друга. В работе доказывается критерий расположения двух бент-функций на минимальном возможном расстоянии друг от друга, предлагаются оценки числа бент-функций на минимальном возможном расстоянии от заданной бент-функции: доказана точная верхняя оценка для произвольной бент-функции и нижняя оценка для бент-функций из класса Мэйорана—Мак-Фарланда. Точная верхняя оценка достигается только для квадратичных бент-функций.

Методика исследований. В диссертации используются традиционные комбинаторные методы, аппарат алгебры и дискретного анализа.

Научная новизна и значимость. Работа носит теоретический характер. Все результаты диссертации являются новыми и снабжены полными доказательствами. В работе предложен поход к исследованию метрических свойств класса бент-функций с помощью аффинности бент-функции на подпространстве. Полученные результаты могут быть использованы в дальнейших исследованиях метрических свойств класса бент-функций, верхних оценок числа бент-функций, а также в исследованиях, связанных с аффинностью ограничения булевой функции на аффинное подпространство.

Публикации. Основные результаты по теме диссертации изложены в 12 печатных изданиях, 5 из которых изданы в журналах, рекомендованных ВАК, 7 — в тезисах докладов. Статья [1] опубликована в соавторстве с А. В. Павловым, совместно с которым проводились численные эксперименты, теоретические результаты работы [1] получены автором лично.

Апробация работы. Основные результаты работы докладывались на следующих конференциях: Международный симпозиум по теории информации ISIT'2011 (Россия, г. Санкт-Петербург, 2011 г.), Современные тенденции в криптографии CTCrypt 2013 (Россия, г. Екатеринбург, 2013 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» SIBECRYPT (2009 — 2013 гг.), Молодежная научная школа по дискретной математике и её приложениям (Россия, г. Москва, 2009 и 2013 гг.), Мальцевские чтения (Россия, г. Новосибирск,

[23] Потапов В. Н. Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Проблемы передачи информации. — 2012. — Т. 48, № 1. — С. 54–63.

2013 г.). Результаты представлялись на семинарах «Дискретный анализ» и «Криптография и криптоанализ» Института математики им. С. Л. Соболева и кафедры теоретической кибернетики НГУ, семинаре отдела теоретической кибернетики ИМ СО РАН и семинаре «Модели и методы дискретной математики» кафедры дискретной математики МГУ.

Основные результаты диссертации заключаются в следующем.

1. Введено понятие полной аффинной расщепляемости булевой функции. Доказано, что все полностью аффинно расщепляемые булевы функции являются либо аффинными, либо квадратичными.

2. Доказано, что две бент-функции от $2k$ переменных находятся на минимальном возможном расстоянии 2^k тогда и только тогда, когда они различаются на аффинном подпространстве размерности k и обе функции на нём аффинны.

3. Получена классификация всех бент-функций на минимальном расстоянии от квадратичной бент-функции. Подсчитано число таких бент-функций.

4. Получена точная верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных. Доказано, что оценка достигается только для квадратичных бент-функций.

5. Получена нижняя оценка числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана—МакФарланда.

Объём и структура работы. Диссертация состоит из введения, пяти глав, заключения, списка литературы и приложения. Объём диссертации 81 страница. Список литературы содержит 97 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель работы.

В **первой главе** даны необходимые определения. Приводится обзор понятий и известных результатов, связанных с аффинностью булевой функции на подпространстве. В частности, рассматриваются k-аффинные булевы функции, уровень аффинности булевой функции, обобщенный уровень аффинности булевой функции (М. Л. Буряков, О. А. Логачёв, А. А. Сальников,

В. В. Ященко), нормальные, k-нормальные, слабо нормальные и k-слабо нормальные булевы функции (Х. Доббертин, П. Шарпин), представление булевой функции в виде линейного разветвления (О. А. Логачёв, А. А. Сальников, В. В. Ященко).

Во **второй главе** предлагается усиление аффинных свойств булевой функции, вводится понятие полной аффинной расщепляемости.

Определение 1. Булева функция f от n переменных называется *полностью аффинно расщепляемой* порядка k, $2 \leq k \leq n$, если

- для любого аффинного подпространства $\mathbb{Z}_2^n$ размерности k верно, что f либо аффинна на каждом сдвиге этого подпространства, либо не аффинна ни на одном из сдвигов;
- f аффинна хотя бы на одном подпространстве размерности k.

Доказывается

Теорема 1. *Пусть f — булева функция от n переменных. Справедливы следующие утверждения.*

(i) Функция f полностью аффинно расщепляема порядка k, $2 \leq k \leq \lceil n/2 \rceil$ тогда и только тогда, когда f либо аффинная, либо квадратичная;

(ii) Функция f является полностью аффинно расщепляемой порядка k, $\lceil n/2 \rceil \leq k < n$ и не является полностью аффинно расщепляемой порядка $k+1$ тогда и только тогда, когда f аффинно эквивалентна функции $g(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2n-2k-1}x_{2n-2k}$.

Таким образом, аффинно расщепляемыми могут быть только аффинные и квадратичные булевы функции.

Отметим, что именно полностью аффинно расщепляемые бент-функции от $2k$ переменных имеют наибольшее число бент-функций на расстоянии 2^k (см. пятую главу). Из теоремы 1 также следует, что бент-функция от $2k$ переменных является полностью аффинно расщепляемой порядка t, $2 \leq t \leq k$ тогда и только тогда, когда она квадратичная, при этом полностью аффинно расщепляемых бент-функций других порядков не существует.

В **третьей главе** рассматриваются бент-функции на минимальном возможном расстоянии друг от друга. Минимальное возможное расстояние между двумя бент-функциями от $2k$ переменных равно 2^k. Доказывается следующая теорема.

Теорема 2. *Пусть f и g — бент-функции от $2k$ переменных. Тогда $dist(f, g) = 2^k$ тогда и только тогда, когда $f \oplus g = Ind_L$, где L — аффинное подпространство размерности k и обе функции аффинны на L.*

К. Карле[24] предложил следующую конструкцию бент-функций: пусть f — бент-функция от $2k$ переменных, L — аффинное подпространство $\mathbb{Z}_2^{2k}$ размерности k и f аффинна на L. Тогда $f \oplus Ind_L$ также является бент-функцией, где Ind_L — характеристическая функция множества L. Таким образом, по теореме 2 все бент-функции на расстоянии 2^k от f описываются с помощью приведенной выше конструкции, т.е. имеется прямая связь между бент-функциями на минимальном возможном расстоянии и аффинностью бент-функции на подпространстве.

Отметим симметрию расстояний между функциями в классе бент-функций $\mathfrak{B}_{2k}$: $\mathrm{dist}(f, g \oplus 1) = 2^{2k} - \mathrm{dist}(f, g)$, при этом если $g \in \mathfrak{B}_{2k}$, то и $g \oplus 1 \in \mathfrak{B}_{2k}$, т.е. расстояния симметричны относительно 2^{2k-1}. Следовательно, результаты для расстояния 2^k естественным образом обобщаются на расстояние $2^{2k} - 2^k$.

В работе[25] были найдены примеры не слабо нормальных бент-функций, это такие бент-функции от $2k$ переменных, которые не аффинны ни на одном аффинном подпространстве размерности k. Из этого следует, что не от любой бент-функции имеются бент-функции на расстоянии 2^k.

В главе рассматриваются бент-функции от 2, 4 и 6 переменных, а также от 8 переменных степени не больше 3. От любой из этих бент-функций существуют бент-функции на расстоянии 2^1, 2^2, 2^3 и 2^4 соответственно. Используя аффинную классификацию этих бент-функций, экспериментально найдено число бент-функций на минимальном расстоянии от каждой из них.

От любой бент-функции от 2 и 4 переменных имеется 6 и 60 соответственно бент-функций на минимальном расстоянии (следует из того, что все бент-функции от 2 и 4 переменных являются квадратичными, число бент-функций на минимальном расстоянии от любой из этих бент-функций можно получить из теоремы 4).

Любая бент-функция от 6 переменных аффинно эквивалентна одной из четырёх бент-функций (аффинной классификацией занимались О. Ротхауса, 1976 г., Дж. Диллон 1974 г, Б. Пренель, 1993 г.). Число бент-функций на расстоянии 2^3 от любой такой бент-функции равно одному из следующих значений: 376, 440, 568, 1080.

[24] Carlet C. Two new classes of bent functions // Advances in Cryptology — EUROCRYPT'93 Workshop on the Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993). Proc. Berlin: Springer, 1993. — P. 77–101 (Lecture Notes in Computer Science. — V. 765).

[25] Canteaut A., Daum M., Dobbertin H., Leander G. Finding nonnormal bent functions // Discrete Applied Mathematics. — 2006. — V. 154, N 2. — P. 202–218.

Любая бент-функция от 8 переменных степени не больше 3 аффинно эквивалентна одной из десяти бент-функций[26] [27]. Число бент-функций на расстоянии 2^4 от любой из них равно одному из следующих значений: 1392, 2928, 4464, 6000, 12144, 36720. Значение 2928 повторяется для четырёх аффинно неэквивалентных функций, значение 6000 — для двух.

В **четвёртой главе** рассматриваются квадратичные бент-функции и бент-функции на минимальном возможном расстоянии от них. Ближайшая бент-функция от любой квадратичной бент-функции от $2k$ переменных находится на расстоянии 2^k. Поскольку известно, что все квадратичные бент-функции от $2k$ переменных аффинно эквивалентны бент-функции вида $f_0^{2k}(x) = x_1x_{k+1} \oplus x_2x_{k+2} \oplus \ldots \oplus x_kx_{2k}$, то достаточно найти все бент-функции на минимальном расстоянии от f_0^{2k}, и тогда от любой квадратичной бент-функции все бент-функции на минимальном расстоянии можно построить с помощью аффинных преобразований.

Далее будем представлять базисы линейных подпространств в виде базисных матриц Гаусса—Жордана (сокращенно GJB-матриц). Матрица G называется *GJB-матрцей*, если матрица G^T является редуцированной ступенчатой матрицей, а сама матрица G не содержит нулевых столбцов (отметим, что базисными векторами являются *столбцы* матрицы G). Через $\ell(G)$ обозначим множество номеров ведущих элементов строк матрицы G^T. Использование GJB-матриц удобно тем, что любое линейное подпространство имеет ровно одну базисную матрицу такого вида.

Введем определение допустимой GJB-матрицы. GJB-матрица G размера $2k \times k$ называется *допустимой* порядка t, $t \in \{0, \ldots, k\}$, если она имеет вид

$$G = \left(\begin{array}{c|c} \mathrm{A} & 0 \\ \hline \mathrm{Z} & \mathrm{Y} \end{array}\right), \text{ где}$$

- A — произвольная GJB-матрица размера $k \times t$,
- Y — GJB-матрица ортогонального подпространства к линейному подпространству с базисом A.
- Все строки матрицы Z с номерами из $\ell(Y)$ — нулевые.
- Пусть матрицы A' и Z' получены из матриц A и Z соответственно с помощью удаления строк с номерами из $\ell(Y)$. Если $t > 1$, все элементы матрицы Z' являются решениями следующей системы линейных уравнений (через $a'^{(i)}$ и $z'^{(i)}$ обозначены i-е столбцы матриц A' и Z' соответственно)

[26] Hou X. D. Cubic bent functions // Discrete Mathematics. — 1998. — V. 189. — P. 149–161.

[27] Braeken A. Cryptographic properties of Boolean functions and S-boxes // Ph. D. thesis, Katholieke Universiteit Leuven, Leuven, Belgium. 2006.

$$\begin{pmatrix} {a'^{(2)}}^T & {a'^{(1)}}^T & 0 & 0 & \dots & 0 \\ \dots & & & & & \\ {a'^{(t)}}^T & 0 & 0 & \dots & 0 & {a'^{(1)}}^T \\ \dots & & & & & \\ 0 & {a'^{(3)}}^T & {a'^{(2)}}^T & 0 & \dots & 0 \\ \dots & & & & & \\ 0 & {a'^{(t)}}^T & 0 & \dots & 0 & {a'^{(2)}}^T \\ \dots & & & & & \\ 0 & 0 & 0 & \dots & {a'^{(t)}}^T & {a'^{(t-1)}}^T \end{pmatrix} \cdot \begin{pmatrix} z'^{(1)} \\ z'^{(2)} \\ \\ \\ \vdots \\ \\ \\ z'^{(t)} \end{pmatrix} = 0,$$

где матрица системы имеет размер $(t(t-1)/2) \times t^2$, отметим также, что все её строки являются линейно независимыми.

Теорема 3. *Пусть L — аффинное подпространство $\mathbb{Z}_2^{2k}$ размерности k. Бент-функция f_0^{2k} аффинна на L тогда и только тогда, когда L является линейным подпространством с допустимой GJB-матрицей или сдвигом такого подпространства.*

Например, при $k = 2$ бент-функция f_0^{2k} аффинна на линейных подпространствах со следующими базисными матрицами и всех сдвигах таких подпространств (на месте каждой $*$ может находиться любой элемент $\mathbb{Z}_2$).

$$\left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \\ \hline \mathbf{1} & 0 \\ 0 & \mathbf{1} \end{array}\right), \left(\begin{array}{cc} \mathbf{1} & 0 \\ 0 & 0 \\ \hline * & 0 \\ 0 & \mathbf{1} \end{array}\right), \left(\begin{array}{cc} \mathbf{1} & 0 \\ 1 & 0 \\ \hline 0 & \mathbf{1} \\ * & 1 \end{array}\right), \left(\begin{array}{cc} 0 & 0 \\ \mathbf{1} & 0 \\ \hline 0 & \mathbf{1} \\ * & 0 \end{array}\right) \left(\begin{array}{cc} \mathbf{1} & 0 \\ 0 & \mathbf{1} \\ \hline * & a \\ a & * \end{array}\right),$$

где a — некоторый элемент $\mathbb{Z}_2$.

Число бент-функций на минимальном расстоянии от квадратичной бент-функции даёт следующая теорема.

Теорема 4. *Любая квадратичная бент-функция от $2k$ переменных имеет ровно $2^k \cdot (2^1+1) \cdot \ldots \cdot (2^k+1)$ бент-функций на расстоянии 2^k.*

Это число можно оценить как

$$2^{k(k+1)/2+k} < 2^k \cdot (2^1+1) \cdot \ldots \cdot (2^k+1) < 3 \cdot 2^{k(k+1)/2+k}.$$

Более чем треть базисных матриц линейных подпространств $\mathbb{Z}_2^{2k}$, на которых f_0^{2k} аффинна, строятся очень просто, а именно, следующим образом:

$$G = \left(\frac{E}{T}\right),$$

где T — произвольная симметричная матрица размера $k \times k$, а E — единичная матрица того же размера. Это допустимые GJB-матрицы порядка k.

Заметим также, что любая бент-функция на минимальном расстоянии от квадратичной бент-функции аффинно эквивалентна некоторой бент-функции из класса Мэйорана—МакФарланда.

В **пятой главе** рассматриваются оценки числа функций на расстоянии 2^k от заданной бент-функции. Доказана точная оценка сверху.

Теорема 5. *Пусть f — бент-функция от $2k$ переменных. Тогда число бент-функций на расстоянии 2^k не превосходит $2^k(2^1+1)\cdot\ldots\cdot(2^k+1)$. При этом данная оценка достигается только на квадратичных бент-функциях.*

Достижимость оценки только на квадратичных бент-функциях следует из теоремы 1, т.е. из того, что только квадратичные бент-функции являются полностью аффинно расщепляемыми бент-функциями.

Отметим, что тривиальная оценка сверху числа бент-функций на расстоянии 2^k от бент-функции от $2k$ переменных — это число всех аффинных подпространств $\mathbb{Z}_2^{2k}$. Их число можно оценить как

$$2^{k^2+k} < 2^k \frac{(2^{2k}-1)\cdot\ldots\cdot(2^{k+1}-1)}{(2^k-1)\cdot\ldots\cdot(2^1-1)} < 2^{k^2+2k}.$$

Таким образом, доказанная верхняя оценка близка к квадратному корню из тривиальной оценки.

В главе также предложена нижняя оценка числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана — МакФарланда.

Теорема 6. *Пусть f — бент-функция от $2k$ переменных, аффинно эквивалентная бент-функции из класса Мэйорана-МакФарланда. Тогда число бент-функций на расстоянии 2^k от нее не меньше, чем $2^{2k+1}-2^k$.*

В **приложении А** описано разработанное программное обеспечение для проведения численных экспериментов. С его помощью можно работать с булевыми функциями в различных представлениях (вектор значений, алгебраическая нормальная форма, трейс-представление), двоичными векторами, подпространствами $\mathbb{Z}_2^n$, полями Галуа $GF(2^n)$. Для булевых функций можно подсчитать такие параметры, как степень, коэффициенты Уолша—Адамара, нелинейность, алгебраическую иммунность, а также перебрать все аффинные подпространства, на которых она аффинна. В частности, с его помощью получено число бент-функций на минимальном расстоянии для бент-функций от малого числа переменных (третья глава).

В **заключении** приведены основные результаты работы.

Благодарности. Автор выражает глубокую признательность своему научному руководителю Н. Н. Токаревой за постоянное внимание к работе и предложенные интересные направления исследований. Также автор благодарит коллектив комнаты 142 ИМ СО РАН — А. А. Городилову, В. А. Виткуп,

Е. П. Корсакову, С. Ю. Филюзина и Г. И. Шушуева — за дружескую атмосферу и отзывчивость, С. В. Августиновича и В. Н. Потапова за интерес к рассматриваемой теме и ценные советы, Д. С. Кротова, взявшего на себя труд прочитать текст диссертации, своего первого научного руководителя А. А. Левина, а также А. А. Евдокимова и других сотрудников лаборатории дискретного анализа Института математики им. С. Л. Соболева СО РАН за поддержку.

Публикации автора по теме диссертации

Статьи в рецензируемых журналах из списка ВАК

1. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. — 2009. — № 4. — С. 5–20.

2. Коломеец Н. А. Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 1. — С. 41—58 (Перевод: Kolomeets N. A. Enumeration of the bent functions of least deviation from a quadratic bent function // Journal of Applied and Industrial Mathematics. — 2012. — V. 6, N 3. — P. 306–317.).

3. Коломеец Н. А. Пороговое свойство квадратичных булевых функций // Дискретный анализ и исследование операций. — 2014. — Т. 21, № 2. — С. 52–58.

4. Kolomeec N. A. On a property of quadratic Boolean functions // Математические вопросы криптографии. — 2014. — Т. 5, № 2. — С. 79–85.

5. Коломеец Н. А. Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. — 2014. — № 3. — С. 12–23.

Тезисы и труды конференций

6. Kolomeec N. A., Pavlov A. V. Bent functions on the minimal distance // Proc. of IEEE Region 8 International Conference on Computational Technologies in Electrical and Electronics Engineering (Irkutsk, Russia. July, 11–15, 2010). — Irkutsk. — 2010. P. 145–149.

7. Kolomeec N. A. Constructions of bent functions on the minimal distance from the quadratic bent function // Proc. of IEEE International Symposium on

Information Theory (Saint-Petersburg, Russia. July, 31 – August, 5, 2011). — Saint-Petersburg. — 2011. — P. 647–651.

8. Коломеец Н. А. Количество бент-функций на минимальном расстоянии от квадратичной бент-функции // Прикладная дискретная математика. Приложение. — 2011. — № 4. — С. 9–11.

9. Коломеец Н. А., Павлов А. В. Boolean Functions – система для работы с булевыми функциями // Прикладная дискретная математика. Приложение. — 2011. — № 4. — С. 67–68.

10. Коломеец Н. А. Об аффинности булевых функций на подпространствах и их сдвигах // Прикладная дискретная математика. Приложение. — 2013. — № 6. — С. 15–16.

11. Kolomeec N. A. On a property of quadratic Boolean functions // Мальцевские чтения (Новосибирск, Россия. 11–15 ноября, 2013). [Электронный ресурс]. Режим доступа: `http://www.math.nsc.ru/conference/malmeet/13/maltsev13.pdf`. P. 42.

12. Коломеец Н. А. Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. Приложение. — 2014. — № 7. — С. 22–24.

Коломеец Николай Александрович

Бент-функции, аффинные на подпространствах, и их метрические свойства

Автореферат диссертации
на соискание учёной степени
кандидата физико-математических наук

Подписано в печать .08.2014 г. Формат 60×84 1/16.
Усл. печ. л. 1,2. Уч.-изд. л. 1,0. Тираж 100 экз. Заказ №

Отпечатано в ООО "Омега Принт"
пр. Ак. Лаврентьева, 6, Новосибирск 630090