Бент-функции и разбиения двоичного куба*

Олег А. Логачев, Алексей А. Сальников, Валерий В. Ященко

Московский государственный университет им. М. В. Ломоносова,
119899, Россия, Москва, Воробьевы горы,
лаборатория по математическим проблемам криптографии

Аннотация. В настоящей работе предложена новая форма представления булевых функций — кусочно-аффинная. Получено выражение для коэффициентов Фурье функции, представленной в кусочно-аффинной форме. Развивается техника неполного преобразования Фурье. Предложен новый подход к описанию булевых бент-функций (максимально-нелинейных функций), основанный на кусочно-аффинном представлении функций. Предложен способ построения новых классов бент-функций. Вводится новое понятие частичной бент-функции. Для частичных бент-функций получен аналог критерия Ротхауза. Рассмотрено понятие функции, дуальной к частичной бент-функции. Рассмотрен способ сведения нерешенной на сегодняшний день проблемы описания бент-функций к комбинаторным задачам описания подмножеств двоичного куба с определенными свойствами и описания разбиений двоичного куба на такие подмножества.

1. Введение

Бент-функции выделены из множества всех булевых функций как решения некоторой экстремальной задачи о коэффициентах Фурье [14, 19, 21]. Разнообразные приложения бент-функций стимулировали многочисленные исследования их свойств, но удобного конструктивного описания бент-функций пока нет.

Понятие булевой бент-функции было введено в [14, 15, 19, 21]. В [21] исследованы некоторые их свойства и приведены два класса бент-функций. В [19] указывалась связь бент-функций и такого комбинаторного объекта, как разностные множества. Исходя из методов построения разностных множеств, в [14, 15] указаны два достаточно больших класса бент-функций: $\boldsymbol{M}$ и $\boldsymbol{PS}$. Причем последний из них состоит из подклассов функций, задаваемых неявно ($\boldsymbol{PS}^+$, $\boldsymbol{PS}^-$), и класса функций, задаваемого явно ($\boldsymbol{PS}_{\mathrm{ap}}$). Дальнейшие исследования в этом направлении привели к рассмотрению новых классов бент-функций ($\boldsymbol{D}$ и $\boldsymbol{C}$) в [7]. В той же работе введено понятие полноты класса бент-функций и показано, что классы $\boldsymbol{D}$ и $\boldsymbol{C}$ не входят в ранее известные классы $\boldsymbol{M}$ и $\boldsymbol{PS}$, а также показано, что классы $\boldsymbol{M}$ и $\boldsymbol{PS}$ не

* Работа поддержана Российским фондом фундаментальных исследований (номера проектов 99-01-00929 и 99-01-00941)

полны. Существенное продвижение в исследовании бент-функций получено в [10]. В ней рассмотрено так называемое «геометрическое представление» бент-функций и введен класс $\boldsymbol{GPS}$ бент-функций, представимых в этом виде. Получен ряд свойств бент-функций из этого класса, продемонстрирована эффективность этого подхода при построении ранее неизвестных бент-функций (см. также [9]). В заключение высказана гипотеза о возможности представления (характеризации) бент-функций в виде суммы (в поле рациональных чисел) характеристических функций подпространств специального вида. Эта гипотеза была доказана в [11].

Достаточно широкие приложения бент-функций в теории кодирования (см. [4], где бент-функции названы максимально-нелинейными функциями), в теории связи [8, 16, 18, 20, 22], в других областях, породили направления исследований, изучающие бент-функции с дополнительными условиями [12], а также функции, близкие по своим свойствам к бент-функциям [6].

Одновременно с изучением булевых бент-функций развивались различные обобщения этого понятия. Здесь следует отметить работы [13, 17]. В них введены бент-функции, определенные на прямом произведении конечного числа одинаковых циклических групп, со значениями в этой циклической группе. Иное обобщение понятия бент-функции приведено в [1]. В ней рассмотрены бент-функции, определенные на векторном пространстве над конечным полем, со значениями в этом конечном поле. Изложение ведется на языке случайных величин и характеристических функций. Более подробный обзор результатов о свойствах булевых бент-функций (максимально-нелинейных функций) содержится в [2]. Указанные обобщения вкладываются в понятие бент-функции на конечной абелевой группе, введенном в [3].

2. Основные результаты

В настоящей работе развивается новый подход к описанию бент-функций, основанный на кусочно-аффинном представлении булевых функций и на понятии частичной бент-функции (см. [2, 3, 11]). Кусочно-аффинное представление булевых функций вводится впервые, как и впервые рассматривается понятие частичной бент-функции (не путать с понятием “partial bent”-функции Клода Карле [6]).

Введем следующие понятия и обозначения. V_n — множество всех двоичных векторов длины n, которое является векторным пространством размерности n над полем из двух элементов $\mathbb{F}_2$. Множество V_n называется также двоичным кубом. Функции $f : V_n \to \{0,1\}$ называют булевыми функциями, а пары $(f; D)$, где $D \subseteq V_n$, а $f : D \to \{0,1\}$ — частичными булевыми функциями с областью определения D. Скалярное произведение (x, y) двух векторов $x, y \in V_n$ определяется как двоичная сумма

$$(x, y) = x_1 y_1 + \ldots + x_n y_n \ .$$

Частичную булеву функцию $(f;D)$ будем называть частичной бент-функцией, если выполнено 2^n соотношений

$$\left|\widehat{f}_D(\alpha)\right| = \sqrt{|D|}, \quad \forall \alpha \in V_n \ ,$$

где $\widehat{f}_D(\alpha)$ — неполное преобразование Фурье функции f:

$$\widehat{f}_D(\alpha) = \sum_{x \in D} (-1)^{(\alpha,x)} (-1)^{f(x)} \ .$$

Множество всех частичных бент-функций с фиксированной областью определения D обозначим через $\mathrm{BF}(D)$. Случай $D = V_n$ соответствует стандартному понятию булевой бент-функции. Удобный критерий принадлежности функции $f(x)$ к множеству $\mathrm{BF}(V_n)$ доказан Ротхаузом еще в 1976 году (см. [21]):

> $f(x)$ принадлежит $\mathrm{BF}(D)$ тогда и только тогда, когда любая из 2^n-1 ее производных по ненулевым направлениям является уравновешенной булевой функцией, т.е.
>
> $$\frac{df}{d\sigma}(x) = f(x) + f(x+\sigma) \in \mathrm{UF}(V_n), \quad \forall \sigma \in V_n \backslash \{\mathbf{0}\} \ .$$

Здесь $\mathrm{UF}(V_n)$ — множество уравновешенных булевых функций, которое состоит из функций, принимающих значения 0 и 1 поровну, т.е. по 2^{n-1} раз.

Булеву функцию $f(y,z)$ представимую в виде

$$f(y,z) = y_1\varphi_1(z) + \ldots + y_t\varphi_t(z) + \psi(z), \quad y \in V_t, z \in V_{n-t} \ , \tag{1}$$

будем называть кусочно-аффинной. Если ввести отображение

$$\nu(z) = (\varphi_1(z), \ldots, \varphi_t(z)) : V_{n-t} \to V_t \ ,$$

то представление (1) можно записать в векторном виде:

$$f(y,z) = (y, \nu(z)) + \psi(z), \quad y \in V_t, z \in V_{n-t} \ . \tag{2}$$

Кусочно-аффинное представление является обобщением известного разложения булевой функции по одной переменной:

$$f(x_1, \ldots, x_n) = x_1\varphi_1(x_2, \ldots, x_n) + \psi_1(x_2, \ldots, x_n) \ .$$

Для данной булевой функции может быть несколько различных представлений в кусочно-аффинной форме. Важнейшее свойство кусочно-аффинной функции состоит в следующем: при любом фиксировании $z = z_0 \in V_{n-t}$ булева функция $f(y, z_0)$ аффинна. Поэтому легко вычисляются коэффициенты Фурье кусочно-аффинной булевой функции.

Лемма 1. *Пусть $f(y,z)$ представима в виде (2). Тогда*

$$\widehat{f}(\alpha,\beta) = 2^t \widehat{\psi}_{\nu^{-1}(\alpha)}(\beta), \quad \forall \alpha \in V_t, \forall \beta \in V_{n-t} \ .$$

Отметим следующее полезное наблюдение: если $\{\alpha : \nu^{-1}(\alpha) = 0\} \neq \emptyset$, то часть коэффициентов Фурье $\widehat{f}(\alpha, \beta)$ обращается в ноль:

$$\widehat{f}(\alpha_0, \beta) = 0, \ \beta \in V_{n-t}, \quad \text{если } \nu^{-1}(\alpha_0) = 0 \quad .$$

Лемма 1 и критерий Ротхауза позволяют доказать, что в определенном смысле любая бент-функция состоит из некоторого количества частичных бент-функций.

Теорема 1. *Функция $f(y, z)$, представленная в виде (2), является бент-функцией тогда и только тогда, когда выполнены следующие условия:*

1) $\left|\nu^{-1}(\alpha)\right| = 2^{n-2t}, \quad \forall \alpha \in V_t.$
2) $\psi \in \mathrm{BF}\left(\nu^{-1}(\alpha)\right), \quad \forall \alpha \in V_t.$

Качественно Теорему 1 можно переформулировать следующим образом:

> бент-функция $f(y, z)$ представима в виде (2) тогда и только тогда, когда $V_{n-t} = \bigcup_{\alpha \in V_t} \nu^{-1}(\alpha)$ — это разбиение двоичного куба V_{n-t} на непересекающиеся равномощные блоки, и сужение функции ψ на каждый блок $\nu^{-1}(\alpha)$ этого разбиения является частичной бент-функцией.

Теперь очевидно, что можно произвольным образом переставлять блоки разбиения, оставаясь при этом в классе бент-функций.

Следствие 1. *Пусть бент-функция f представлена в виде (2), а $\pi : V_t \to V_t$ — взаимно однозначное отображение. Тогда*

$$F(y, z) = (y, \pi\nu(z)) + \psi(z) \in \mathrm{BF}(V_n) \quad .$$

Следствие 1 позволяет из одной кусочно-аффинной бент-функции получать достаточно большой класс бент-функций за счет свободы выбора произвольного взаимно однозначного отображения $\pi : V_t \to V_t$. Легко понять, что при $n = 2m$, $t = m$, $\nu(z) = (z_1, \ldots, z_m)$, $\psi(z)$ — произвольная булева функция, Следствие 1 дает хорошо известный класс $\boldsymbol{M}$ бент-функций, описанный еще Ротхаузом (см. [21]).

Теорема 1 сводит задачу описания бент-функций представленных в виде (2) к решению двух следующих задач:

1) описание частичных бент-функций с областью определения мощности 2^{n-2t} и, прежде всего, описание таких множеств D, $|D| = 2^{n-2t}$, для которых $\mathrm{BF}(D) \neq \emptyset$;
2) описание бент-разбиений двоичного куба V_{n-t}, т.е. таких разбиений $V_{n-t} = \bigcup_{\alpha \in V_t} D_\alpha$ на 2^t непересекающихся равномощных блоков, что $\mathrm{BF}(D_\alpha) \neq \emptyset$ для всех $\alpha \in V_t$.

Если эти задачи решены, то любая бент-функция вида (2) описывается следующим образом. Пусть $V_{n-t} = \bigcup_{\alpha \in V_t} D_\alpha$ — произвольное бент-разбиение двоичного куба V_{n-t}. Определим отображение $\nu : V_{n-t} \to V_t$ равенством

$$\nu(z) = \alpha, \quad \forall \alpha \in V_t, \forall z \in D_\alpha \ .$$

Для каждого $\alpha \in V_t$ выберем произвольным образом функцию $\psi_\alpha \in \mathrm{BF}(D_\alpha)$ и функцию $\psi(\alpha)$ определим равенством

$$\psi(z) = \bigvee_{\substack{\alpha \in V_t \\ z \in D_\alpha}} \psi_\alpha(z) \ .$$

Тогда в соответствии с Теоремой 1

$$f(y,z) = (y, \nu(z)) + \psi(z) \in \mathrm{BF}(V_n) \ .$$

Полностью задачи 1 и 2 пока не решены, поэтому с помощью приведенной схемы удается описать лишь некоторые классы бент-функций. Простейший из таких классов связан с разбиением двоичного куба на плоскости — линейные подпространства и смежные классы по ним. Пусть $n = 2m$ и D_α, $\forall \alpha \in V_t$ — плоскости размерности $2(m-t)$. Тогда $\mathrm{BF}(D_\alpha)$ естественным образом можно отождествить с $\mathrm{BF}\left(V_{2(m-t)}\right)$, т.е. с множеством всех бент-функций от $2(m-t)$ переменных. Если теперь $V_{n-t} = \bigcup_{\alpha \in V_t} D_\alpha$ — разбиение двоичного куба, то с помощью приведенной схемы получим следующий класс бент-функций

$$f(y,z) = (y, \nu(z)) + \bigvee_{\substack{\alpha \in V_t \\ z \in D_\alpha}} \psi_\alpha(z) \ ,$$

где $\psi_\alpha(z) \in \mathrm{BF}(D_\alpha)$ — произвольный набор 2^t бент-функций от $2(m-t)$ переменных.

Перейдем теперь к более глубокому исследованию свойств частичных бент-функций. Вначале приведем два технических утверждения о свойствах неполного преобразования Фурье, которые аналогичны известным свойствам полного преобразования Фурье. Они доказываются с помощью стандартной техники изменения порядка суммирования и использования соотношений ортогональности для характеров $(-1)^{(\alpha,x)}$.

Теорема 2. *Функциональное уравнение*

$$\widehat{f}_D(\alpha) = c(\alpha), \quad \forall \alpha \in V_n \ ,$$

относительно неизвестной частичной булевой функции $(f; D)$ разрешимо тогда и только тогда, когда правая часть уравнения $c(\alpha)$ удовлетворяет одному из двух эквивалентных условий:

$$\sum_{\alpha \in V_n} c(\alpha) c(\alpha + \beta) = 2^n \sum_{y \in D} (-1)^{(\beta,y)}, \quad \forall \beta \in V_n \ ,$$

$$\left(\widehat{c}(x)\right)^2 = \begin{cases} 2^{2n}, & \text{если } x \in D \\ 0, & \text{если } x \notin D \end{cases} .$$

При этом решение уравнения $(f;D)$ *имеет вид:*

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{\alpha \in V_n} c(\alpha)(-1)^{(\alpha,x)}, \quad \forall x \in D \ .$$

Лемма 2. *Для любой частичной булевой функции* $(f;D)$ *выполнено тождество*

$$\sum_{\sigma \in V_n \setminus \{\mathbf{0}\}} \left| \widehat{\frac{df}{d\sigma}}(\mathbf{0}) \right|_D^2 = \frac{1}{2^n} \sum_{\alpha \in V_n} \left(\left| \widehat{f}_D(\alpha) \right|^2 - |D| \right)^2 \ .$$

Используя Лемму 2, легко получить аналог критерия Ротхауза для частичных бент-функций.

Теорема 3. *Частичная булева функция* $(f;D)$ *принадлежит* $\mathrm{BF}(D)$ *тогда и только тогда, когда выполнено условие*

$$\widehat{\frac{df}{d\sigma}}(\mathbf{0})\Big|_D = \sum_{\substack{x \in D \\ x+\sigma \in D}} (-1)^{f(x)+f(x+\sigma)} = 0, \quad \forall \sigma \in V_n \setminus \{\mathbf{0}\} \ .$$

Для частичной бент-функции можно стандартным образом ввести понятие дуальной функции, причем дуальная булева функция оказывается полностью определенной. Если $f(x) \in \mathrm{BF}(D)$, то дуальная функция $\widetilde{f}(\alpha)$ задается равенством

$$\widehat{f}_D = (-1)^{\widetilde{f}(\alpha)} \sqrt{|D|}, \quad \forall \alpha \in V_n \ .$$

Через $\mathrm{TF}(D)$ обозначим множество булевых функций, коэффициенты Фурье которых удовлетворяют условию

$$\widehat{\varphi}^2(\alpha) = \begin{cases} \frac{2^{2n}}{|D|}, & \text{если } \alpha \in D \\ 0, & \text{если } \alpha \notin D \end{cases} .$$

Заметим, что, в частности, $\mathrm{TF}(V_n) = \mathrm{BF}(V_n)$. Тогда, применяя Теорему 2 в случае $c(\alpha) = (-1)^{\widetilde{f}(\alpha)} \sqrt{|D|}$, получаем, что дуальная функция $\widetilde{f}(\alpha)$ принадлежит $\mathrm{TF}(D)$. Более того, дуальная функция удовлетворяет условию

$$\widetilde{\widetilde{f}}(x) = (-1)^{f(x)} \frac{2^n}{\sqrt{|D|}}, \quad \forall x \in D \ .$$

Это означает справедливость следующего утверждения.

Теорема 4. *Переход к дуальной функции устанавливает взаимно однозначное соответствие между множествами* $\mathrm{TF}(D)$ *и* $\mathrm{BF}(D)$.

Следствие 2. *Если* $\mathrm{BF}(D) \neq \emptyset$, *то* $|D| = 2^{2l}$, *где* $l < n$.

Литература

1. Амбросимов, А.С.: Свойства бент-функций q-значной логики над конечными полями. Дискретная математика. **6** Вып. 3 (1994) 50–60
2. Кузнецов, Ю.В., Шкарин, С.А.: Коды Рида-Маллера (обзор публикаций). Математические вопросы кибернетики. Вып. 6 (1996) 5–50
3. Логачев, О.А., Сальников, А.А., Ященко, В.В.: Бент-функции на конечной абелевой группе. Дискретная математика. **9** Вып. 4 (1997) 3–20
4. Мак-Вильямс, Ф.Дж., Слоэн, Н.Дж.: Теория кодов, исправляющих ошибки. «Связь», Москва (1979)
5. Ященко, В.В.: О критерии распространения для булевых функций и бент-функциях. Проблемы передачи информации. **33** Вып.1 (1997) 52–63
6. Carlet, C.: Partially-bent Functions. In: Brickell, E.F. (ed.): Advances in Cryptology — CRYPTO'92. Proceedings. Lecture Notes in Computer Science, **740** Springer-Verlag, Berlin Heidelberg New York (1993) 280–291 and Designs Codes and Cryptography. **3** (1993) 135–145
7. Carlet, C.: Two New Classes of Bent Functions. In: Helleseth, T. (ed.): Advances in Cryptology — EUROCRYPT'93. Proceedings. Lecture Notes in Computer Science, **765** Springer-Verlag, Berlin Heidelberg New York (1994) 77–101
8. Carlet, C., Seberry, J., Zhang, X.M.: Comments on "Generating and Counting Binary Bent Sequences". IEEE Transactions on Information Theory. **40** № 2 (1994) 600
9. Carlet, C.: A Constraction of Bent Functions. In: Proceedings of the Seventh Joint Swedish-Russian International Workshop on Information Theory, St.-Petersburg Russia June, 17–22 (1995) 57–59 and Finite Fields and Applications. London Mathematical Society. Lecture Series, **233**. Cambridge University Press (1996) 47–58
10. Carlet, C.: Generalized Partial Spreads. IEEE Transactions on Information Theory. **41** № 5 Sept. (1995) 1482–1487
11. Carlet, C., Guillot, Ph.: A Characterization of Binary Bent Functions. In: Proceedings of the Fifth Intern. Workshop., Sozopol Bulgaria (1996) 86–92 and Journal of Combinatorial Theory, Ser. **A**. **76** № 2 (1996) 328–335
12. Carlet C. Hyper-bent Functions. In: Proceedings of the International Conference on the Theory and Applications of Cryptology PRAGOCRYPT'96, Czech Technical University Publishing House GC UCMP 145–155
13. Chung, H., Kumar, P.V.: A new General Construction for Generalized Bent Functions. IEEE Transactions on Information Theory. **35** № 1 (1989) 206–209
14. Dillon, J.F.: A Survey of Bent Functions. The NSA Techical Journal (unclassified). (1972) 191–215
15. Dillon, J.F.: Elementary Hadamard Difference Sets. Ph.D. dissertation. University of Maryland (1974) and In: Proceedings of the Sixth Southeastern Conference on Combinatorics Graph Theory and Computing, Florida Atlantic University. (1975) 237–249
16. Gold, R.: Optimal Binary Sequences for Spread-Spectrum Multiplexing. IEEE Transactions on Information Theory. **13** № 4 (1967) 619–621
17. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized Bent Functions and Their Properties. Journal of Combinatorial Theory, Ser. **A**. **40** (1985) 90–107
18. Lempel, A., Cohn, M.: Maximal Families of Bent Sequences. IEEE Transactions on Information Theory. **IT-28** № 6 Nov. (1982) 65–68
19. MacFarland, R.A.: A Family of Difference Sets in Noncyclic Groups. Journal of Combinatorial Theory, Ser. **A**. **15** № 1 (1973) 1–10

20. Olsen, J.D., Scholtz, R.A., Welch, L.R.: Bent-Function Sequences. IEEE Transactions on Information Theory. **IT-28** № 6 Nov. (1982) 858–864
21. Rothaus, O.S.: On "Bent" Functions. Journal of Combinatorial Theory, Ser. **A**. **20** № 3 (1976) 300–305
22. Yarlagadda, R., Hershey, J.E. Analysis and Syntesis of Bent Sequences. IEE Proc. Pt.E. **136** № 2 (1989)