(n,m)	Функции с $\mathrm{AI}_{\mathrm{comp}}(F)=\lceil n/2\rceil$	Все функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$	Доля функций
(2,2)	168	256	0,65625
(3,2)	1344	65536	0,02051
(3,3)	10752	16777216	0,00064
(4,2)	$\approx 10^8$	4294967296	$\approx 0{,}02$

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt'2003. LNCS. 2003. V. 2656. P. 345–359.
2. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt'2004. LNCS. 2004. V. 3027. P. 474–491.
3. *Armknecht F. and Krause M.* Constructing single- and multi-output Boolean functions with maximal immunity // ICALP'2006. LNCS. 2006. V. 4052. P. 180–191.
4. *Ars G. and Faugère J.-C.* Algebraic immunities of functions over finite fields // Proc. Conf. BFCA. 2005. P. 21–38.
5. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009. P. 104–116.

УДК 519.7 DOI 10.17223/2226308X/8/16

СВОЙСТВА p-ИЧНЫХ БЕНТ-ФУНКЦИЙ, НАХОДЯЩИХСЯ НА МИНИМАЛЬНОМ РАССТОЯНИИ ДРУГ ОТ ДРУГА[1]

В. Н. Потапов

Доказано, что минимальное расстояние Хэмминга между двумя p-ичными бент-функциями от $2n$ переменных равно p^n в случае, когда число p простое. Число p-ичных бент-функций на минимальном расстоянии от квадратичной бент-функции равно $p^n(p^{n-1}+1)\cdots(p+1)(p-1)$ при $p>2$.

Ключевые слова: *бент-функция, расстояние Хэмминга, квадратичная форма.*

Введение

Рассмотрим конечную абелеву группу G и векторное пространство $V(G)$, состоящее из функций $f: G \to \mathbb{C}$, со скалярным произведением

$$(f,g)=\sum_{x\in G} f(x)\overline{g(x)}.$$

Характерами называются гомоморфизмы группы G в мультипликативную группу поля $\mathbb{C}$, т. е. такие $\phi \in V(G)$, что $\phi(x+y)=\phi(x)\phi(y)$, для любых $x,y\in G$. Характеры абелевой группы G образуют ортогональный базис в $V(G)$. Если $G=\mathbb{Z}_q^n$, то для любого $z\in\mathbb{Z}_q^n$ характер группы G определяется равенством $\phi_z(x)=\xi^{\langle x,z\rangle}$, где $\xi=e^{2\pi i/q}$ и $\langle x,y\rangle = x_1y_1+\ldots+x_ny_n \bmod q$. Характерами прямой суммы двух групп являются всевозможные попарные произведения характеров первой и второй группы. Поскольку любая конечная абелева группа представляется в виде прямой суммы циклических групп, характеры произвольной конечной абелевой группы являются произведениями функций определённого выше вида.

Преобразованием Фурье функции из $V(G)$ называется вектор коэффициентов в разложении по базису характеров. Нам будет удобнее определить преобразование Фурье

[1]Работа поддержана грантом РФФИ № 13-01-00463.

изометричным образом: $\widehat{f}(z) = (f, \phi_z)/|G|^{1/2}$. Тогда равенство Парсеваля принимает вид $\|f\| = \|\widehat{f}\|$ и справедлива формула обращения $\widehat{(\widehat{f}(x))} = f(-x)$. *Носителем* функции называется множество аргументов, на которых функция принимает ненулевые значения $\mathrm{supp}(f) = \{x \in G : f(x) \neq 0\}$. Доказательство следующего утверждения имеется, например, в [1].

Утверждение 1 (принцип неопределённости). Пусть G — конечная абелева группа, тогда

$$|\mathrm{supp}(f)||\mathrm{supp}(\widehat{f})| \geqslant |G|. \tag{1}$$

Причём равенство в формуле (1) достигается только для характеристических функций подгрупп с точностью до естественных преобразований, сохраняющих мощности носителей функции и её фурье-образа.

Если p — простое число, то группу $\mathbb{Z}_p^n$ можно рассматривать как n-мерное векторное пространство над полем $\mathrm{GF}(p)$.

Следствие 1. Пусть $G = \mathbb{Z}_p^n$ и p — простое число. Равенство в формуле (1) достигается, если и только если $f = c\phi_z\chi^\Gamma$, где $z \in G$; $c \in \mathbb{C}$ — константа и χ^Γ — характеристическая функция аффинного подпространства Γ в G.

Известно (см., например, [2, с. 33, лемма 1.1.26]) следующее равенство.

Утверждение 2 (тождество Саркара). Пусть p — простое число и Γ — линейное подпространство в $\mathbb{Z}_p^n$. Тогда

$$\sum_{y\in\Gamma} \widehat{f}(y) = p^{\dim\Gamma - n/2} \sum_{x\in\Gamma^\perp} f(x).$$

Определим *свёртку* двух функций $f, g \in V(G)$ равенством $f*g(z) = \sum\limits_{x\in G} f(x)g(z-x)$. Из определения свёртки нетрудно получить известное равенство

$$\widehat{f * g} = |G|^{1/2}\widehat{f}\cdot\widehat{g}. \tag{2}$$

1. Бент-функции

Для функций $g : \mathbb{Z}_q^n \to \mathbb{Z}_q$ определим *преобразование Уолша — Адамара* следующим образом: $W_g(z) = \widehat{\xi^g}(z)$. Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *бент-функцией* (q-ичной), если $|W_f(y)| = 1$ для любых $y \in Z_q^n$, или (что то же самое) $\widehat{\xi^f}\cdot\overline{\widehat{\xi^f}} = I$, I — функция, всюду равная 1 [3 – 5]. Из (2) следует, что определение бент-функции эквивалентно равенству $\xi^f * \overline{\xi^f} = |G|\chi^{\{0\}}$. Отсюда непосредственно вытекает, что матрица $A = (a_{z,y})$, где $a_{z,y} = \xi^{f(z+y)}$, является обобщённой матрицей Адамара, как и матрица $H = (h_{z,y})$, где $h_{z,y} = \xi^{\langle z,y\rangle}$. Нетрудно видеть, что невырожденные аффинные преобразования аргументов бент-функции и прибавление аффинной функции не выводят из класса бент-функций.

Бент-функция b называется *регулярной*, если найдётся функция $b' : \mathbb{Z}_q^n \to \mathbb{Z}_q$, удовлетворяющая равенству $\xi^{b'} = \widehat{\xi^b}$. Из формулы обращения следует, что b' также является бент-функцией. Известно следующее

Утверждение 3.

1) $\sum\limits_{j=0}^{q-1} \xi^{kj} = 0$ при $k \neq 0 \pmod q$;

2) если q — простое, то ξ не является корнем многочлена степени меньше $q-1$;
3) если q — степень простого числа, то алгебраическая система, полученная присоединением элемента ξ к полю рациональных чисел, является полем.

Из свойства 3 непосредственно получаем

Следствие 2. Если q — степень простого числа и n чётно, то все бент-функции регулярны.

Для доказательства следствия нужно использовать то, что число $|G|^{n/2}$ — целое и линейная комбинация элементов поля содержится в поле.

В дальнейшем полагаем p простым, а n чётным. Из свойства 2 утверждения 3 можно получить

Следствие 3. Для любых двух p-ичных бент-функций b и b' справедливо равенство $|\mathrm{supp}(\xi^b - \xi^{b'})| = |\mathrm{supp}(\widehat{\xi^b} - \widehat{\xi^{b'}})|$.

Для доказательства следствия достаточно проверить, что имеется $(p-1)/2$ различных чисел вида $|\xi^i - \xi^j|^2$, $i \neq j$, которые независимы над полем рациональных чисел.

Отсюда и из утверждения 1, а также следствия 1 имеем

Следствие 4. Расстояние Хэмминга между двумя бент-функциями, т. е. число аргументов из $\mathbb{Z}_p^n$, на которых они различаются, не меньше $p^{n/2}$. Если это расстояние равно $p^{n/2}$, то разность между ними равна $c\chi^\Gamma$, где $c \in \mathbb{Z}_p$; Γ — аффинное подпространство размерности $n/2$.

Из утверждения 2 можно получить

Следствие 5. Если бент-функция $b : \mathbb{Z}_p^n \to \mathbb{Z}_p$ аффинна на аффинном подпространстве Γ, то $\dim \Gamma \leqslant n/2$.

Следствие 6. Если бент-функция $b : \mathbb{Z}_p^n \to \mathbb{Z}_p$ аффинна на аффинном подпространстве размерности $n/2$, то найдётся ровно $p-1$ бент-функций, отличающихся от b только на этом подпространстве.

Поскольку аффинные преобразования не выводят из класса бент-функций, при доказательстве следствия 6 достаточно рассматривать содержащие нулевой вектор грани Γ размерности $n/2$ и бент-функции, постоянные на этой грани. Из утверждения 2 видно, что если ξ^b постоянна на Γ, то и $\widehat{\xi^b}$ постоянна на $\Gamma^\perp$ и принимает это же значение ξ^k, $k \in \mathbb{Z}_p$. Нетрудно видеть, что $\chi^{\Gamma^\perp} = \widehat{\chi^\Gamma}$. Тогда сумма $\xi^b + (\xi^m - \xi^k)\chi^\Gamma$, $m \in \mathbb{Z}_p$, также является бент-функцией.

Следствия 4–6 при $p = 2$ доказаны в [6] (следствия 5 и 6 имеются в [7]). В двоичном случае исследованы также возможные (не превышающие двух минимальных) расстояния между двумя бент-функциями [8].

2. Число бент-функций на минимальном расстоянии от квадратичной

Квадратичная форма $Q : (\mathrm{GF}(q))^n \to \mathrm{GF}(q)$ называется *невырожденной*, если её ядро $\{x \in (\mathrm{GF}(q))^n : \forall y \in (\mathrm{GF}(q))^n\,(Q(y+x) = Q(y))\}$ состоит из нуля. Линейное подпространство U в $(\mathrm{GF}(q))^n$ называется *тотально изотропным*, если $Q(U) = 0$. Максимальная размерность тотально изотропного подпространства называется *индексом Витта* формы Q. При $n = 2d$ максимальный индекс Витта невырожденной квадратичной формы равен d. Все квадратичные формы максимального индекса Витта эквива-

лентны (переводятся друг в друга невырожденным линейным преобразованием). Одним из представлений такой формы является $Q_0(v_1, \ldots, v_d, u_1, \ldots, u_d) = v_1u_1 + \ldots + v_du_d$.

Нетрудно показать, что Q_0 является бент-функцией (частным примером конструкции Майорана — МакФарланда [5]). Известно (см., например, [9, p. 274, Lemma 9.4.1]) следующее

Утверждение 4. Число тотально изотропных подпространств максимального индекса $d = n/2$ у квадратичной формы Q_0 равно $\prod_{i=1}^{d}(q^{d-i} + 1)$.

Нетрудно видеть, что если форма Q_0 аффинна на некотором аффинном подпространстве, то она аффинна и на любом его смежном классе. При $q > 2$ если форма Q_0 аффинна на некотором линейном подпространстве индекса d, то это подпространство тотально изотропно. Таким образом, форма Q_0 аффинна на всех смежных классах тотально изотропных подпространств индекса d и не аффинна на других аффинных подпространствах той же размерности.

Из утверждения 4 и следствия 6 имеем

Следствие 7. Пусть p — простое, $p > 2$. Тогда количество p-ичных бент-функций от $2d$ переменных, находящихся на расстоянии p^d от квадратичной формы Q_0, равно $p^d(p^{d-1} + 1) \cdots (p + 1)(p - 1)$.

В двоичном случае аналогичное утверждение доказано в [10]. В [11] доказано, что максимальное количество близких соседних бент-функций имеется только у квадратичной бент-функции. Можно предположить, что последнее свойство, характеризующее квадратичные функции, остаётся верным для всех простых $p > 2$.

ЛИТЕРАТУРА

1. *Tao T.* An uncertainty principle for cyclic groups of prime order // Math. Res. Lett. 2005. V. 12. No. 1. P. 121–127.
2. *Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003. 504 с.
3. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Comb. Theory. Ser. A. 1985. V. 40. No. 1. P. 90–107.
4. *Токарева Н. Н.* Бент-функции и их обобщения // Прикладная дискретная математика. Приложение. 2009. № 2. С. 5–17.
5. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 1. С. 34–64.
6. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
7. *Carlet C.* Two new classes of bent functions // Advances in Cryptology — EUROCRYPT'93. LNCS. 1994. No. 765. P. 77–101.
8. *Потапов В. Н.* Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информ. 2012. Т. 48. № 1. С. 54–63.
9. *Brouwer A. E., Cohen A. M., and Neumaier A.* Distance-Regular Graphs. N. Y.: Springer Verlag, 1989. 485 p.
10. *Коломеец Н. А.* Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. опер. 2012. Т. 19. № 1. С. 41–58.

11. *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. 28–39.

УДК 519.719.1 DOI 10.17223/2226308X/8/17

ПЕРЕЧИСЛЕНИЕ ДВОИЧНЫХ ФУНКЦИЙ, ИМЕЮЩИХ ЗАДАННОЕ ЧИСЛО АФФИННЫХ СОМНОЖИТЕЛЕЙ

А. В. Черемушкин

Предлагается рекурсивный способ вычисления числа двоичных функций от n переменных, имеющих заданное число аффинных сомножителей, допускающий введение ограничений на вес или степень нелинейности функций.

Ключевые слова: *двоичные функции, аффинная классификация, формула обращения Мёбиуса.*

1. Случай обычных функций

Пусть $n \geqslant 0$. Подсчитаем число двоичных функций от n переменных заданного веса, имеющих аффинные сомножители. Функция $f : V_n(2) \to \{0, 1\}$ *имеет аффинные сомножители*, если найдутся такие функция $l(x) = (x, a^*) \oplus b$, $x \in V_n(2)$, $0 \neq a^* \in \in V_n(2)^*$ ($V_n(2)^*$ — сопряжённое пространство), $b \in \{0, 1\}$ и функция h, что $f = l \cdot h$.

Пусть $k \in \{0, \ldots, n\}$. Обозначим через $\mathcal{F}_n(k)$ множество всех двоичных функций от n переменных, имеющих ровно k аффинных сомножителей. Функцию $f \equiv 0$ не включаем ни в одно из множеств $\mathcal{F}_n(k)$. Легко видеть, что выполняется равенство

$$\mathcal{F}_n = \bigcup_{k=0}^{n} \mathcal{F}_n(k) \cup \{0\}. \tag{1}$$

Справедливы следующие свойства:

1. Множества $\mathcal{F}_n(k)$ при разных k не пересекаются, $k = 0, \ldots, n$.
2. Множества $\mathcal{F}_n(k)$, $k = 0, \ldots, n$, инвариантны относительно действия полной аффинной группы $\mathbf{AGL}\,(n, 2)$ (и, следовательно, разбиваются на классы эквивалентности относительно этой группы).
3. Каждую функцию $f \in \mathcal{F}_n(k)$ можно привести с помощью некоторого аффинного преобразования к виду

$$h(x) = f(xQ \oplus b) = \overline{x}_1 \ldots \overline{x}_k g(x_{k+1}, \ldots, x_n), \tag{2}$$

   где $g \in F_{n-k}(0)$.
4. Если $k \in \{0, \ldots, n\}$ и $f \in \mathcal{F}_n(k)$, то $1 \leqslant \|f\| \leqslant 2^{n-k}$, где $\|f\|$ — вес функции f.
5. Множество векторов, входящих в область истинности $\{a \in V_n(2) : f(a) = 1\}$ функции f вида (2), порождает смежный класс по подпространству размерности $n - k$.

Теорема 1. Пусть $1 \leqslant k \leqslant n$ и функции $f, h \in \mathcal{F}_n(k)$ и $g \in \mathcal{F}_{n-k}(0)$ удовлетворяют равенству (2). Тогда порядки групп инерции функций f, h и g в группе аффинных преобразований связаны равенством

$$|\mathbf{AGL}\,(n, 2)_f| = |\mathbf{AGL}\,(n, 2)_h| = 2^{k(n-k)} |\mathbf{GL}\,(k, 2)| \cdot |\mathbf{AGL}\,(n-k, 2)_g|. \tag{3}$$