В качестве обратной к f по модулю $UT_3^2(\mathbb{Z}_3)$ возьмём функцию, индуцированную полиномом $p(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x$. Степень p_1 равна 2, значит, $m = 2$ и обратная перестановка к f получается как $g(x) = p(x)(x^{-1}f(p(x)))^{-2}$:

$$g : (1, 26, 6)(2, 9, 22)(3, 16, 14)(4, 20, 18, 13, 11, 27)(5, 12, 7, 23, 21, 25)(8, 24, 10, 17, 15, 19).$$

Таким образом, при фиксированных нормальном ряде в группе и способе выбора представителей в факторах этого ряда определён класс ВКП-функций над группой. Функции класса задаются набором полиномов и получаются как произведение их координатных функций. Класс ВКП-функций над $UT_n(\mathbb{Z}_p)$ не совпадает с классом полиномиальных функций над $UT_n(\mathbb{Z}_p)$ (теорема 1). К ВКП-функциям применимы критерий биективности и формулы обращения дифференцируемых функций, которые в случае $\mathbb{G} = UT_n(\mathbb{Z}_p)$ принимают вид теорем 2 и 3 соответственно.

ЛИТЕРАТУРА

1. *Заец М. В.* О классе вариационно-координатно-полиномиальных функций над примарным кольцом вычетов // Прикладная дискретная математика. 2014. № 3. С. 12–27.
2. *Карпов А. В.* Обращение дифференцируемых перестановок над группой // Прикладная дискретная математика. Приложение. 2015. № 8. С. 30–33.
3. *Anashin V. S.* Solvable groups with operators and commutative rings having transitive polynomials // Algebra. Logika. 1982. No. 21(6). С. 627–646.
4. *Меньшов А. В.* Асимптотические свойства рациональных множеств и систем уравнений в свободных абелевых группах и разрешимость регулярных уравнений в классе нильпотентных групп: дис. ... канд. физ.-мат. наук. Омск, 2014.

УДК 519.7 DOI 10.17223/2226308X/9/10

О РАССТОЯНИИ ХЭММИНГА МЕЖДУ ДВУМЯ БЕНТ-ФУНКЦИЯМИ[1]

Н. А. Коломеец

Рассматривается расстояние Хэмминга между двумя бент-функциями. С использованием конструкции бент-функций на минимальном расстоянии друг от друга получен ряд возможных значений расстояния. Найдены всевозможные значения расстояния между бент-функциями из класса Мэйорана — МакФарланда.

Ключевые слова: *булевы функции, бент-функции, расстояние Хэмминга.*

Булевой функцией от n переменных называется отображение вида $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Расстоянием Хэмминга* $\mathrm{dist}(f, g)$ между двумя булевыми функциями f и g от n переменных называется количество значений аргументов, на которых значения функций различаются. Функция вида $\langle a, x\rangle \oplus c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$ и $\langle a, x\rangle = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$, называется *аффинной* булевой функцией. *Бент-функциями* называются булевы функции от чётного числа переменных, находящиеся на максимально возможном расстоянии от множества всех аффинных функций. Они предложены О. Ротхаусом [1]. Бент-функции имеют приложения в алгебре, комбинаторике, теории кодирования, криптографии [2]. Обозначим через $\mathcal{B}_{2k}$ множество всех бент-функций от $2k$ переменных.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.

В данной работе рассматривается расстояние Хэмминга между двумя бент-функциями и носитель их суммы. Исследование возможных носителей связано с гипотезой Н. Н. Токаревой [3] о том, что любую булеву функцию степени не больше k от $2k$ переменных можно представить в виде суммы двух бент-функций из $\mathcal{B}_{2k}$. Следующая лемма даёт общий критерий принадлежности функции на расстоянии $|D|$ от бент-функции f к классу бент-функций.

Лемма 1. Пусть $f \in \mathcal{B}_{2k}$. Тогда $f \oplus \mathrm{Ind}_D \in \mathcal{B}_{2k}$, где $D \subseteq \mathbb{F}_2^{2k}$, тогда и только тогда, когда для всех $y \in \mathbb{F}_2^{2k}$ справедливо

$$\sum_{x \in D} (-1)^{f(x) \oplus \langle x,y \rangle} \in \{0, \pm 2^k\}.$$

Опишем всевозможные значения расстояния между бент-функциями из класса Мэйорана — МакФарланда M_{2k} [4], который содержит функции вида

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y),$$

где $x, y \in \mathbb{F}_2^k$; π — подстановка на множестве $\mathbb{F}_2^k$; φ — произвольная булева функция от k переменных.

Утверждение 1. Расстояние Хэмминга между двумя бент-функциями $f, g \in M_{2k}$ имеет вид $(n+2m)2^{k-1}$, где $0 \leqslant n \leqslant 2^k$, $n \neq 1$ и $0 \leqslant m \leqslant 2^k - n$, причём для любой бент-функции из M_{2k} существует бент-функция на данном расстоянии от неё. Носитель $f \oplus g$ представим в виде объединения аффинных подпространств размерностей $k-1$ и k.

Особый интерес представляют расстояния в $\mathcal{B}_{2k}$ в интервале от минимального возможного до удвоенного минимального, поскольку в [5] получены всевозможные носители суммы с точностью до аффинной эквивалентности. В [6] доказано, что между двумя бент-функциями достижимы расстояния вида $2^{k+1} - 2^t$, где $1 \leqslant t \leqslant k$.

С использованием конструкции бент-функций на минимальном возможном расстоянии 2^k (см., например, [7]) получены следующие расстояния между двумя бент-функциями.

Теорема 1. Для всех d вида $\ell 2^k - 2^t$, где $1 \leqslant t \leqslant k$ и $2 \leqslant \ell \leqslant 2^k - 2^{k-t+1} + 2$, существуют бент-функции $f, g \in \mathcal{B}_{2k}$, такие, что $\mathrm{dist}(f, g) = d$ и $\mathrm{dist}(f \oplus 1, g) = 2^{2k} - d$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N. N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
3. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds and hypothesis // Adv. Math. Commun. 2011. V. 5. No. 4. P. 609–621.
4. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.
5. *Kasami T. and Tokura N.* On the weight structure of Reed — Muller codes // IEEE Trans. Inform. Theory. 1970. V. 16. No 6. P. 752–759.
6. *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.
7. *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.