

УДК 519.7

НОВАЯ КОМБИНАТОРНАЯ КОНСТРУКЦИЯ БЕНТ-ФУНКЦИЙ¹

Н. Н. Токарева

Бент-функции впервые были введены О. Ротхаусом [1]. В настоящее время они активно изучаются и имеют много приложений в теории кодирования, криптографии, цифровой сотовой связи и других областях (см. подробнее обзоры [2, 3]). Тем не менее в области бент-функций много открытых вопросов. Одними из основных являются вопросы о конструкциях бент-функций и оценках их числа.

В работе предложена новая итеративная конструкция бент-функций от $n + 2$ переменных на основе бент-функций от n переменных. В дальнейшем представляется интересным исследовать те нижние оценки числа бент-функций, которые следуют из этой конструкции.

Напомним, что *преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle + f(x)}$. Булева

функция от n переменных (n четно), такая, что модуль каждого коэффициента Уолша — Адамара этой функции равен $2^{n/2}$, называется *бент-функцией*. С бент-функцией f часто связывают *дуальную* булеву функцию, которая определяется равенством $2^{n/2}(-1)^{\tilde{f}(y)} = W_f(y)$. Функция $\tilde{f}$ также является бент-функцией, $\tilde{\tilde{f}} = f$.

Пусть булева функция g от $n + 2$ переменных определяется равенством

$$g(a_1, a_2, x) = f_i(x), \text{ где } i = a_1 + 2a_2,$$

и f_0, f_1, f_2 и f_3 — булевы функции от n переменных.

Теорема 1. Пусть f_0, f_1, f_2 — бент-функции. Тогда g является бент-функцией от $n + 2$ переменных тогда и только тогда, когда функция $\tilde{f}_0 + \tilde{f}_1 + \tilde{f}_2$ — бент-функция. В этом случае f_3 также является бент-функцией, причем она однозначно определяется равенством $\tilde{f}_0 + \tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 = 1$.

Пусть $\mathcal{B}_n$ — множество бент-функций от n переменных.

Непосредственно из теоремы вытекает

Следствие 1. Для числа бент-функций от n переменных справедлива оценка

$$|\mathcal{B}_n| \geq \sum_{f_0 \in \mathcal{B}_{n-2}} \sum_{f_1 \in \mathcal{B}_{n-2}} |(\mathcal{B}_{n-2} + f_0) \cap (\mathcal{B}_{n-2} + f_1)|.$$

Например, несложно заметить, что при любых f_0, f_1 выполняется

$$|(\mathcal{B}_{n-2} + f_0) \cap (\mathcal{B}_{n-2} + f_1)| \geq 2^{n-1}.$$

Тогда из следствия сразу получается нижняя оценка вида $2^{2^{n/2}}$ (типа Мак-Фарланда) на число бент-функций от n переменных. Интересно найти более нетривиальные варианты оценки из приведенного следствия.

¹Исследование выполнено при поддержке гранта Президента РФ для молодых российских ученых (грант МК №1250.2009.1), РФФИ (проекты 08-01-00671, 09-01-00528, 10-01-00424) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0429).

ЛИТЕРАТУРА

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. № 1. С. 15–37.
3. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискрет. анализ и исслед. операций. 2010. Т. 17. № 1. С. 34–64.

УДК 512.54.05

О СКОРОСТИ ПОРОЖДЕНИЯ ЗНАКОПЕРЕМЕННОЙ ГРУППЫ ПОЛУРЕГУЛЯРНЫМИ ИНВОЛЮЦИЯМИ

М. Э. Тужилин

В ряде работ Дж. Бреннера [1] и других авторов изучался вопрос об экспоненте класса сопряженных элементов C конечной неабелевой группы G , то есть минимальном e , для которого выполняется условие $C^e = G$. Показано, что в знакопеременной группе A_N почти все классы сопряженных элементов имеют экспоненту e , меньшую или равную 4. Единственным классом, имеющим экспоненту 4, как доказано в [2], является класс полурегулярных инволюций.

Пусть $N = 2n$.

Условимся обозначать цикловую структуру $[h]$ подстановки h через $[t_1^{\alpha_1}, t_2^{\alpha_2}, \dots, t_m^{\alpha_m}]$. Это означает, что в разложении подстановки h на независимые циклы есть ровно α_i циклов длины $t_i, i \in \{1, 2, \dots, m\}$.

Определение. Подстановка h степени N называется полурегулярной инволюцией, если $[h] = [2^n]$.

Множество всех полурегулярных инволюций степени N обозначим через J_N . Мощность этого множества равна $(N-1)!!$.

Утверждение 1. Подстановка h принадлежит множеству J_N^2 тогда и только тогда, когда $[h] = [t_1^{2\beta_1}, t_2^{2\beta_2}, \dots, t_m^{2\beta_m}]$.

Утверждение 2. При $N \neq 4$ справедливо равенство $J_N^4 = A_N$, при $N = 4$ выполнено $J_N^2 = W_4$, где W_4 — четверная группа Клейна.

Утверждение 3. Множество J_N^3 не содержит подстановок с цикловыми структурами $[1^{N-3}, 3^1]$, $[1^1, 2^{(N-4)/2}, 3^1]$, $[1^{N-5}, 5^1]$, $[2^{(N-8)/2}, 3^1, 5^1]$, $[1^{N-5}, 2^1, 3^1]$, $[1^{N-7}, 3^1, 4^1]$, $[1^1, 3^5]$.

Напомним [3], что длиной $l(G, M)$ группы $G = \langle M \rangle$ относительно системы образующих M называется минимальное r , при котором выполняется равенство $G = \bigcup_{k=1}^r M^k$, а шириной $d(G, M)$ называется минимальное число слоев M^k , которыми может быть исчерпана группа G .

Утверждение 4.

а) Если n четно и $n \neq 2$, то $\langle J_N \rangle = A_N$, $d(A_N, J_N) = 1$, $l(A_N, J_N) = 4$. При $n = 2$ выполнено $J_N^4 = W_4$.

б) Если n нечетно, то $\langle J_N \rangle = S_N$, $d(S_N, J_N) = 2$. При $n > 1$ выполнено $l(S_N, J_N) = 5$; при $n = 1$ справедливо $l(S_N, J_N) = 2$, где S_N — симметрическая группа.