

## 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  $\alpha_i$  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.

Рассчитаны мощности слоев  $J_N^k$  для  $N \leq 20$ . В приводимой ниже таблице указано количество классов сопряженных элементов, содержащихся в слое  $J_N^k$  для  $k = 2, 3, 4, 5$ .

| $N$ | 2  | 3   | 4   | 5   |
|-----|----|-----|-----|-----|
| 2   | 1  |     |     |     |
| 4   | 2  |     |     |     |
| 6   | 3  | 4   | 6   | 5   |
| 8   | 5  | 8   | 12  |     |
| 10  | 7  | 16  | 22  | 20  |
| 12  | 11 | 36  | 40  |     |
| 14  | 15 | 62  | 69  | 66  |
| 16  | 22 | 113 | 118 |     |
| 18  | 30 | 186 | 195 | 190 |
| 20  | 42 | 313 | 317 |     |

#### ЛИТЕРАТУРА

1. *Brenner J. L.* Covering theorems for FINANSIGS VIII — Almost all conjugacy classes in  $A_n$  have exponent  $\leq 4$  // *J. Austral. Math. Soc.* 1978. V. 25. P. 210–214.
2. Products of conjugacy classes in groups / eds. Z. Arad, M. Herzog // *Lecture Notes in Math.* Berlin: Springer Verlag, 1985. V. 1112. P. 198–221.
3. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. II. М.: Гелиос АРВ, 2003.
4. *Тужилин М. Э.* О порождении знакопеременной группы полурегулярными инволюциями // *Обзор прикладной и промышленной математики.* 2004. Т. 11. Вып. 4. С. 938–939.

УДК 519.1

### СВОЙСТВА ВНЕШНИХ УПРАВЛЯЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В. М. Фомичев

Свойства выходной гаммы и преобразований состояний генератора с внешним управлением неравномерным движением существенным образом определяются свойствами управляющей гаммы. Например, в генераторах « $\delta$ - $\tau$ -шагов» и в генераторах с перемежающимся шагом, построенных на основе линейных регистров сдвига (ЛРС) с максимальными длинами периодов, порядок линейной подгруппы циклической группы преобразований состояний генератора определяется длиной периода  $t$  управляющей гаммы [1, разд. 18.4.2, 2]: линейные уравнения гаммообразования соответствуют всем тактам работы генератора, номера которых кратны  $t$ .

Показано, что в генераторах с внешним управлением доля линейных уравнений гаммообразования тем больше, чем меньше  $h$ -период управляющей последовательности, где  $h$  — функция, отображающая отрезки управляющей последовательности в подходящее множество. Свойства  $h$ -периодов последовательностей над  $\mathbb{N}_0$  для конкретной функции  $h$  суммирования членов последовательности, полученные в [3], в работе обобщены.

Для аддитивных функций  $h$  доказано, что длина  $h$ -периода периодической последовательности делит длину периода, для некоторых  $h$  исследованы длины  $h$ -периодов последовательностей де Брёйна и линейных рекуррентных последовательностей над конечными полями.