

Утверждение 1. Если $N \geq 6$, $2 \leq q_1 < q_2 \leq N/2$, то $\Gamma_N(q_1) \cdot \Gamma_N(q_1) \subseteq \Gamma_N(q_2) \times \Gamma_N(q_2)$.

Теорема 1. Пусть $N \geq 8$, $4 \leq q \leq N/2$, $G \in S_N$. Если $|\Gamma(G)| \leq 2q - 2$, то существуют подстановки $H_1, H_2 \in \Gamma_N(q)$, для которых выполняется равенство $G = H_1 \cdot H_2$.

Далее рассмотрим, какие подстановки из множеств $\Gamma_N(2q-1)$, $\Gamma_N(2q)$ принадлежат произведению $\Gamma_N(q) \cdot \Gamma_N(q)$.

Утверждение 2. Пусть $N \geq 4$, $2 \leq q \leq N/2$, подстановка $G \in \Gamma_N(2q)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \dots, m_r$, $\sum_{i=1}^r m_i = 2q$. Подстановка G лежит в $\Gamma_N(q) \cdot \Gamma_N(q)$ в том и только в том случае, когда существует такое подмножество $\{i_1, \dots, i_k\} \subseteq \{1, \dots, r\}$, что $m_{i_1} + \dots + m_{i_k} = q$.

Утверждение 3. Пусть $N \geq 4$, $2 \leq q \leq N/2$, подстановка $G \in \Gamma_N(2q-1)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \dots, m_r$, $\sum_{i=1}^r m_i = 2q - 1$. Подстановка G лежит в $\Gamma_N(q) \cdot \Gamma_N(q)$ в том и только в том случае, когда выполнено условие: существует $i_0 \in \{1, \dots, r\}$ и существует такое подмножество $\{i_1, \dots, i_k\} \subseteq \{1, \dots, r\} \setminus \{i_0\}$, что $m_{i_0} > 2$ и $q - m_{i_1} + m_{i_2} + \dots + m_{i_k} \in \{2, \dots, m_{i_0} - 1\}$.

Итак, в теореме 1, утверждениях 2 и 3 полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q)$ при $4 \leq q \leq N/2$.

ЛИТЕРАТУРА

1. Bertram E. Even permutations as a product of two conjugate cycles // J. Combin. Theory (A). 1972. V. 12. No. 3. P. 368–380.
2. Bertram E. and Wei V. K. Decomposing a permutation into two large cycles; an enumeration // SIAM J. Algebraic Discrete methods. 1980. V. 1. No. 4. P. 450–461.
3. Moran G. Reflection classes whose cubes cover the alternating group // J. Combin. Theory (A). 1976. V. 21. No. 1. P. 1–19.
4. Moran G. Permutations as products of k conjugate involutions // J. Combin. Theory (A). 1975. V. 19. No. 2. P. 240–242.
5. Product of conjugacy classes in groups / eds. Z. Arad, M. Herzog. Lecture Notes in Mathematics. V. 1112. Berlin: Springer Verlag, 1985. 244 p.
6. Тужлилин М. Э. О порождении знакопеременной группы полурегулярными инволюциями // Обозрение прикладной и промышленной математики. 2004. Т. 11. Вып. 4. С. 938–939.

УДК 519.7

О ПРИБЛИЖЕНИИ ПОДСТАНОВОК ИМПРИМИТИВНЫМИ ГРУППАМИ

Б. А. Погорелов, М. А. Пудовкина

С 70-х годов прошлого века изучаются и строятся классы функций, максимально далёких от множества всех аффинных функций. Однако вместо множества всех таких функций можно также рассматривать симметрическую группу на конечном множестве X , а вместо множества всех аффинных функций — множество всех подстановок, сохраняющих некоторую систему импримитивности W с r блоками мощности w ,

которая берётся из множества $W_{w,r}$ всех таких нетривиальных систем и фиксирована. Максимальная группа подстановок, сохраняющая данную систему импримитивности $W \in W_{w,r}$, есть группа сплетения $IG_W = (S_w \wr S_r, W)$ в её импримитивном действии. Близость между подстановками $g, h \in S_n$ измеряется расстоянием Хемминга $\chi(g, h)$.

В работе рассматриваются два параметра:

- порядок W -примитивности, то есть число

$$\chi_W(g) = \min \{ \chi(g, h) : h \in IG_W \};$$

- порядок (w, r) -примитивности, то есть число

$$\chi_{(w,r)}(g) = \min \{ \chi(g, h) : h \in IG_W, W \in W_{w,r} \}.$$

Если соответствующие параметры больше нуля, то подстановку g будем называть W -примитивной, (w, r) -примитивной; в противном случае — W -импримитивной, (w, r) -импримитивной. При рассмотрении W -примитивности каждой подстановке ставится в соответствие матрица, характеризующая удалённость данной подстановки от группы IG_W . Через коэффициенты данной матрицы получено выражение для $\chi_W(g)$. Описаны классы максимально W -примитивных подстановок, являющихся «бент-подстановками» относительно системы импримитивности. Приведены оценки числа таких подстановок.

Порядок (w, r) -примитивности подстановки $g \in S(X)$ определяется только её цикловой структурой, то есть является функцией на классах сопряжённых элементов в группе $S(X)$. Перечислены цикловые структуры подстановок из множества $IG_{(w,r)} = \bigcup_{W \in W_{(w,r)}} IG_W$. Поскольку множество $IG_{(w,r)}$ является объединением классов сопряжённых элементов группы $S(X)$, то цикловая структура элемента g однозначно характеризует его принадлежность множеству $IG_{(w,r)}$. В целом задача нахождения порядка (w, r) -примитивности оказалась сложнее. Получены порядки (w, r) -примитивности при чётном n в крайних случаях $w = 2$ и $r = 2$.

Исходя из общего подхода, получены порядки (w, r) -примитивности для s -боксов криптосистем AES, ARIA, Whirlpool, MISTY1, Camellia, FOX.

УДК 519.14

О СОВЕРШЕННЫХ 2-РАСКРАСКАХ q -ЗНАЧНОГО ГИПЕРКУБА¹

В. Н. Потапов

Обозначим через Z_q множество $\{0, \dots, q-1\}$. Декартово произведение Z_q^n называется q -значным n -мерным кубом (гиперкубом). Функция $f : Z_q^n \rightarrow Z_q$ называется *корреляционно-иммунной порядка $n - t$* , если мощность пересечения грани размерности t с множеством $f^{-1}(a)$ зависит только от $a \in Z_q$. Через $\text{cor}(f)$ будем обозначать максимальный порядок корреляционной иммунности. *Плотностью* булевозначной функции χ^S будем называть отношение $\rho(S) = |S|/q^n$. Если $\rho(S) = 1/2$, то булевозначную корреляционно-иммунную функцию χ^S называют *уравновешенной*.

¹Работа выполнена при поддержке РФФИ (проекты №10-01-00424, 10-01-00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0429).