

Пример 1. Пусть E — конечная верхняя полурешётка и ε — система её подмножеств с нижней гранью. Тогда клон $Q_E(\tilde{\varepsilon})$ совпадает с клоном квазимонотонных функций на полурешётке E , введённых Г. П. Агibalовым [2], а клон $\Phi_E(\tilde{\varepsilon})$ совпадает с клоном слабосущественных квазимонотонных функций из [3].

Пример 2. Как клон сохранения некоторой s -системы можно определить любой (предполный по теореме Розенберга) клон функций из P_E , сохраняющих произвольный отличный от диагонали центральный вполне рефлексивный симметричный предикат.

Проблема полноты в слабоцентральных клоне. Из-за указанных приложений слабоцентральных клонов представляется важной проблема полноты в них.

Теорема 2. Пусть A и B — s -слабоцентральные клоны, такие, что $A \subseteq B$. Тогда множество $\hat{\Lambda}(A, B)$ является безыбыточной A -критериальной системой для клона B ; в частности, для произвольных предикатов p и q из $\Lambda(A, B)$ строгое включение $B \cap \text{pol}_E(p) \subset B \cap \text{pol}_E(q)$ невозможно. Более того, для произвольных предикатов p и q из $\Lambda(A, B)$ равенство клонов $B \cap \text{pol}_E(p) = B \cap \text{pol}_E(q)$ равносильно перестановочной эквивалентности этих предикатов.

Сформулированная теорема сводит задачу построения безыбыточной A -критериальной системы в клоне B для слабоцентральных клонов A и B к нахождению B -предельных предикатов из $\Lambda(A, B)$. Помимо этого, имеет место

Следствие 1. Слабоцентральный клон обладает безыбыточной критериальной системой.

Отметим также, что доказанная в [3] теорема легко обобщается как теорема о $\Phi_E(\varepsilon)$ -полноте в клоне $Q_E(\varepsilon)$ для произвольной s -системы $\tilde{\varepsilon}$.

ЛИТЕРАТУРА

1. Парватов Н. Г. О выделении максимальных подклонов // Прикладная дискретная математика. 2011. № 1. С. 14–25.
2. Агibalов Г. П. Дискретные автоматы на полурешётках. Томск: Изд-во Том. ун-та, 1993. 227 с.
3. Парватов Н. Г. Теорема о функциональной полноте в классе квазимонотонных функций на конечной полурешётке // Дискр. анализ и исслед. опер. Сер. 1. 2006. Т. 13. № 3. С. 62–82.

УДК 519.7

ОПИСАНИЕ КЛАССА ПОДСТАНОВОК, ПРЕДСТАВИМЫХ В ВИДЕ ПРОИЗВЕДЕНИЯ ДВУХ ПОДСТАНОВОК С ФИКСИРОВАННЫМ ЧИСЛОМ МОБИЛЬНЫХ ТОЧЕК

А. Б. Пичкур

Пусть S_N — группа подстановок степени N ; $G \in S_N$; $\Gamma(G) \subseteq \{1, \dots, N\}$ — множество мобильных точек подстановки G ; $2 \leq q \leq N$; $\Gamma_N(q) = \{G \in S_N : |\Gamma(G)| = q\}$ — множество всех подстановок степени N , имеющих ровно q мобильных точек.

В данной работе описано множество всех подстановок из $\Gamma_N(q) \cdot \Gamma_N(q)$. Данный результат имеет практические приложения в криптографии.

В научной литературе рассматривается схожая задача описания множества подстановок, принадлежащих произведению двух или более классов сопряженных элементов из S_N (или из A_N — знакопеременной группы подстановок) [1–6].

Доказаны следующие результаты.

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. Туэсильин 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 ,