ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 2
2014

В. П. Зязин, **М. В. Федюкин** (Москва, МГТУ МИРЭА, ООО «Линфо»)**. О некоторых параметрах базисов из транспозиций и упорядоченных систем образующих симметрической группы.**

Пусть симметрическая группа подстановок S_n действует на множестве $X_n = \{1, 2, \ldots, n\}$. Упорядоченная последовательность таких транспозиций $\tau_1, \tau_2, \ldots, \tau_m$ этой группы, что среди произведений вида

$$\tau_1^{\varepsilon_1}\tau_2^{\varepsilon_2}\cdots\tau_m^{\varepsilon_m}, \quad \text{где} \quad \varepsilon_i \in \{0, 1\}, \tag{1}$$

содержатся все элементы (подстановки), называется *упорядоченной системой образующих* (далее — УСО) группы S_n. В работах [3–6], в которых дано это определение, предложены методы построения и описаны некоторые свойства УСО. Приведены примеры прикладных задач, в которых используется УСО. Применяемый авторами метод построения УСО связан с выбором систем представителей смежных классов симметрической группы S_n по стабилизатору некоторого подмножества множества X_n. Отметим сходство этого подхода с методом каскада, предложенным Ч. Симсом для построения на ЭВМ сильных систем образующих групп подстановок [7]. Среди параметров, характеризующих УСО S_n, особо выделяются параметры: m — наименьшее число, для которого произведения транспозиций вида (1) содержат все подстановки группы S_n, и f — число различных транспозиции в (1).

Очевидно, что $m \geqslant L(S_n, T)$, где $L(S_n, T)$ — длина группы в системе образующих T (см. [1]).

Ответ на вопрос о возможном числе различных транспозиций в (1) дает следующее

Утверждение 1. *Для любой системы образующих из транспозиций T группы S_n, в том числе для любого базиса, содержащего $n-1$ транспозицию, можно построить УСО, в состав которой входят только элементы T.*

Доказательство утверждения фактически сводится к построению следствия теоремы 1 работы [3].

Утверждение 2. *Последовательность транспозиций*

$$\tau_1\tau_2\tau_1\tau_3\tau_2\tau_1\cdots\tau_{n-1}\tau_{n-2}\cdots\tau_1, \tag{2}$$

где $\tau_i = (i, i+1)$, является УСО симметрической группы S_n.

Параметр m этой системы равен длине симметрической группы S_n в базисе вида

$$T = \{(1, 2), (2, 3), \ldots, (n-1, n)\}, \tag{3}$$

$m = L(S_n, T) = n(n-1)/2$.

Отметим, что для базиса (3) М. М. Глуховым получена рекуррентная формула для числа элементов длины k группы S_n, а Г. И. Ивченко и В. Н. Сачковым для случайной величины ξ_n, равной длине случайно выбранного элемента из группы S_n,

доказана асимптотическая нормальность и найдены значения математического ожидания $E\xi_n$ и дисперсии $D\xi_n$ (см. [1]). Эти результаты могут представлять интерес при выборе методов построения криптографических систем, предлагаемых в работах [5, 6].

Очевидно, что число различных транспозиции УСО влияет на величину параметра m. Например, для группы S_4 УСО, построенная на основе базиса $\{(12),(23),(34)\}$ имеет вид $(12)(23)(12)(34)(23)(12)$, $m = 6$; а для системы образующих $T = \{(12),(13),(14),(23),(24)\}$ УСО имеет, например, следующий вид $(12)(13)(24)(14)(23)$, параметр $m = 5$.

Отметим, что для каждого базиса из транспозиций можно построить УСО по аналогии с (2), и таких УСО будет не меньше, чем n^{n-2} (число различных базисов). Этот факт также может представлять интерес при выборе параметров криптографических систем.

СПИСОК ЛИТЕРАТУРЫ

1. *Глухов М. М.*, *Зубов А. Ю.* О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор). Математические вопросы кибернетики. М.: Наука, 1999, в. 8, с. 5–32.
2. *Глухов М. М.*, *Погорелов Б. А.* О некоторых применениях групп в криптографии. Математика и безопасность информационных технологий. М.: МЦНМО, 2005, с. 19–31.
3. *Калинчу С. А.*, *Сагалович Ю. Л.* Наименьшая из известных длин упорядоченной системы образующих симметрической группы. — Проблемы передачи информации, 2009, т. 45, в. 3, с. 56–72.
4. *Калинчук С. А.*, *Сагалович Ю. Л.* Упорядоченная система образующих симметрической группы для решения задач коммутации. — Автомат. телемех., 2009, № 2, с. 142–152.
5. *Калинчук С. А.*, *Сагалович Ю. Л.* Криптографические возможности упорядоченной системы образующих симметрической группы для решения задач коммутации. — Информ. системы, 2009, т. 9, № 3, с. 138–146.
6. *Kalinchuk S. A.*, *Sagalovich Yu. L.* Cryptographic capabilities of an ordered systeem of generators of a semmetric group. — J. Comm. Technol. Electron., 2010, v. 55, is. 12, p. 1485–1490.
7. *Sims C. C.* Computation with permutation groups. — In: Proceedings of Second ACM Symposium on Symbolic and Algebraic Manipulation. (Los Angeles, March 23-25, 1971.)/ Ed. by S. R. Petrick. N. Y.: ACM, 1971, p. 23–28.