

Теорема 2. Для любой подстановки h вида (1) верно неравенство $d_2(\Sigma h) \geq 4$.

Теорема 3. Пусть $R = \text{GR}(q^2, p^2)$, $m = 1$, $p > 2$. Тогда если разрядное множество $P = \Gamma(R)$ удовлетворяет условию

$$\{\gamma_1(a + e) \ominus \gamma_1(b + e) : a, b \in P\} = P,$$

то для любой подстановки h вида (1) справедливо равенство $d_2(\Sigma h) = 4$.

Если при этом $R = \mathbb{Z}_{p^2}$, то группа $\langle \Sigma h \rangle$ содержит знакопеременную группу A_{p^2} .

Теорема 4. Пусть $R = \text{GR}(q^2, 4)$, $m > 1$. Тогда если все миноры матрицы U_0 в (1) ненулевые, то для подстановки h из (1) справедливо равенство $d_2(\Sigma h) = 4$.

Автор выражает глубокую благодарность профессору А. А. Нечаеву за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. Кузьмин А. С., Нечаев А. А. Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и Логика. 1995. Т. 34. № 2. С. 169–189.
2. Глухов М. М. О 2-транзитивности произведения регулярных групп подстановок // Труды по дискретной математике. М.: Физико-математическая литература, 2000. С. 37–52.
3. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. Т 2. М.: Гелиос АРВ, 2003. 416 с.

УДК 519.1

СВОЙСТВА СТАТИСТИКИ var НА ГРУППЕ ПЕРЕСТАНОВОК¹

Л. Н. Бондаренко

Рассматриваются некоторые свойства статистики var , определяющей число различных символов слова, полученного поэлементным сложением по $\text{mod } n$ перестановки степени n с фиксированной перестановкой — ключом.

Ключевые слова: перестановка, статистика, производящий многочлен, перманент, циркулянт.

Ряд статистик на симметрической группе S_n перестановок σ , где $\sigma = \sigma_1 \dots \sigma_n$ — слово над алфавитом $\{1, \dots, n\}$, рассматривался в [1].

В криптографии применяется биекция $\text{vp} : \sigma \mapsto \tau$ перестановки $\sigma \in S_n$ на слово $\tau = \tau_1 \dots \tau_n \in T_n$, определяемая фиксированным ключом $\varkappa = \varkappa_1 \dots \varkappa_n \in S_n$. Она отображает $\sigma \in S_n$ на слово $\tau \in T_n$ по правилу $\tau = \sigma \oplus \varkappa$, где $\tau_i = \sigma_i + \varkappa_i \pmod{n}$, $i = 1, \dots, n$, а τ_i — наименьший положительный вычет, и индуцирует статистику $\text{var}(\sigma, \varkappa) = \text{card}\{\tau_1, \dots, \tau_n\}$ — число различных символов слова $\tau = \text{vp}(\sigma)$.

Так как для любого ключа $\varkappa \in S_n$ статистика var имеет производящий многочлен

$$V_n(t) = \sum_{k=1}^n V_{n,k} t^k = \sum_{\sigma \in S_n} t^{\text{var}(\sigma, \varkappa)},$$

то в качестве ключа удобно использовать перестановку $\nu = \nu_1 \dots \nu_n \in S_n$, где $\nu_i = n - i + 1$, $i = 1, \dots, n$. Многочлен $V_n(t)$ не изменяется и при замене перестановок σ на обратные $\sigma^{-1} \in S_n$.

По определению статистики var многочлен $V_n(t)$ имеет коэффициенты $V_{n,k} \geq 0$, а их нахождение уже при сравнительно небольших n является трудной задачей. Вычисление даёт $V_1(t) = V_2(t)/2 = t$, $V_3(t)/3 = t + t^3$, $V_4(t)/4 = t + t^2 + 4t^3$, $V_5(t)/5 = t + 20t^3 + 3t^5$.

¹Работа поддержана грантом РФФИ, проект № 11-01-00212а.

Теорема 1. Справедливы следующие свойства коэффициентов многочлена $V_n(t)$: а) $n|V_{n,k}$; б) при чётном n все $V_{n,k} > 0$, кроме $V_{n,n} = 0$; в) при нечётном составном n все $V_{n,k} > 0$, кроме $V_{n,n-1} = 0$, а для простого n , кроме того, $V_{n,2} = 0$.

Доказательство теоремы 1 основано на применении перманента циркулянта

$$\text{circ}(z_1, \dots, z_n) = \begin{pmatrix} z_1 & z_2 & \dots & z_n \\ z_n & z_1 & \dots & z_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_2 & z_3 & \dots & z_1 \end{pmatrix},$$

порожденного вектором $(z_1, \dots, z_n)$. Каждый член $\text{per circ}(z_1, \dots, z_n)$ имеет вид $z_1^{m_1} \dots z_n^{m_n}$, причём $0 \leq m_i \leq n$, а сумма $\sum_{i=1}^n im_i$ кратна n . Число различных членов $\text{per circ}(z_1, \dots, z_n)$ равно [2]

$$\frac{1}{n} \sum_{d|n} \binom{2d-1}{d} \varphi\left(\frac{n}{d}\right),$$

где $\varphi(d)$ — функция Эйлера числа d . Рассматриваемый $\text{per circ}(z_1, \dots, z_n)$ преобразуется в многочлен $V_n(t)$ при замене каждого m_i в выражении $z_1^{m_1} \dots z_n^{m_n}$ на $\text{sign}(m_i)$ и отождествлении $z_1 = \dots = z_n = t$.

Задание равномерной меры на множестве S_n и использование нормировки многочлена $V_n(t)$, заключающейся в его делении на число $V_n(1)$, позволяет вместо последовательности коэффициентов $\{V_{n,k}\}_{k=1}^n$ рассматривать распределение, отвечающее случайной величине X_n .

Теорема 2. Математическое ожидание

$$E(X_n) = n \left(1 - \frac{D_n}{n!}\right) \sim n \left(1 - \frac{1}{e}\right),$$

где D_n — число беспорядков на множестве S_n , т. е. число перестановок $\sigma \in S_n$, не имеющих неподвижных элементов.

Для доказательства теоремы 2 с помощью свойств чисел D_n [3] устанавливается, что при фиксации символа $i \in \{1, \dots, n\}$ количество слов $\tau \in T_n$, не содержащих этого символа, равно D_n , и применяются свойства математического ожидания. Асимптотика $E(X_n)$ следует из соотношения $D_n \sim n! e^{-1}$.

Записывая $V_n(t) = V_n^+(u) + tV_n^-(u)$, где $u = t^2$, с помощью теоремы 1 получаем, что при $n \geq 6$ $V_n^+(u) = u^m U_n^+(u)$, причём $m = 2$ для простого n и $m = 1$ для составного n . Вычисления показывают, что при $n \geq 6$ все корни многочленов $U_n^+(u)$ и $V_n^-(u)$, исключая $U_7^+(u) = 1$, различны и отрицательны.

Доказательство этого свойства явилось бы существенным моментом для нахождения асимптотики функции распределения случайной величины X_n .

ЛИТЕРАТУРА

1. Фоата Д. Распределения типа Эйлера и Макмагона на группе перестановок // Проблемы комбинаторного анализа: сб. статей. М.: Мир, 1980. С. 120–141.
2. Brualdi R. A. and Newman M. An enumeration problem for a congruence equation // J. Research National Bureau Standards. Math. Sci. 1970. V. 74B. No. 1. P. 37–40.
3. Риордан Дж. Введение в комбинаторный анализ. М.: ИЛ, 1963.