Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ
ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.1

DOI 10.17223/2226308X/8/1

СВОЙСТВА СТАТИСТИК МАК-МАГОНА НА МНОЖЕСТВАХ СЛОВ¹

Л. Н. Бондаренко, М. Л. Шарапова

Рассматриваются свойства статистик Мак-Магона maj и inv на трёх множествах слов над алфавитом $\{1, \dots, n\}$: 1) перестановки степени n ; 2) все слова длины n ; 3) вогнутые перестановки степени n . На множествах п. 1 и 3 получены новые рекурсивные описания производящих многочленов пар (des, maj) и (des, inv) ; на множестве слов п. 2 найдены только соответствующие рекурсивные описания для пары (des, maj) и статистики inv . Эти рекурсивные описания использованы на множествах п. 1 и 2 для другого доказательства известной теоремы Мак-Магона о совпадении распределений maj и inv . На множестве слов п. 2 определены статистики fas и cas как особые средние значения символа в слове, причем fas и des одинаково распределены, и доказана теорема о совпадении распределений пар (fas, maj) и (fas, inv) , а также пар (cas, maj) и (cas, inv) .

Ключевые слова: статистики Мак-Магона, производящий многочлен, рекурсивное описание, статистики Эйлера.

Для слов $\sigma = \sigma_1 \dots \sigma_l$ длины $l = r_1 + \dots + r_n$ над алфавитом $\{1, \dots, n\}$, являющихся перестановками мультимножества $M = \{1^{r_1}, \dots, n^{r_n}\}$ (иначе, $\sigma \in S(M)$), функции $\text{maj}(\sigma) = \sum_{i=1, \sigma_i > \sigma_{i+1}}^{l-1} i$ и $\text{inv}(\sigma) = \#\{(i, j) : 1 \leq i < j \leq l, \sigma_i > \sigma_j\}$ называются статистиками Мак-Магона [1]. Справедлива известная теорема Мак-Магона: $\sum_{\sigma \in S(M)} q^{\text{maj}(\sigma)} = \sum_{\sigma \in S(M)} q^{\text{inv}(\sigma)} = G_\lambda(q)$, т.е. гауссовский полиномиальный коэффициент $G_\lambda(q) = \left[\begin{smallmatrix} l \\ r_1, \dots, r_l \end{smallmatrix} \right]_q = \frac{(q; q)_l}{(q; q)_{r_1} \dots (q; q)_{r_l}}$, где $\lambda = (1^{r_1} \dots l^{r_l})$ — разбиение числа l , а $(t; q)_l = (1 - t)(1 - tq) \dots (1 - tq^{l-1})$, служит производящим многочленом статистик Мак-Магона на $S(M)$ [2], иначе эти статистики одинаково распределены на $S(M)$.

При длине $l = n$ и $r_1 = \dots = r_n = 1$, т.е. $\sigma \in S_n$, в [1] приводится рекурсивное описание полиномов $A_n(t, q)$, задающих, как показал Л. Карлитц, распределение пары (des, maj) , где $\text{des}(\sigma) = \#\{i : 1 \leq i \leq n, \sigma_i > \sigma_{i+1}, \sigma_{n+1} = 0\}$, а также описание полиномов $A_n^*(t, q)$, задающих распределение пары (des, inv) , с помощью соответствующей производящей функции, найденное Р. Стенли. Отметим, что в [1] вместо des употребляется статистика rise , причём $\text{des}(\sigma) = \text{rise}(\mathbf{c}\sigma)$, где инволюция $\mathbf{c} : S_n \rightarrow S_n$ определяется соотношением $\mathbf{c}\sigma_i = n + 1 - \sigma_i$, $i = 1, \dots, n$.

Рассмотрим получение рекурсивных описаний производящих многочленов пар (des, maj) и (des, inv) на трёх множествах слов σ длины n над алфавитом $\{1, \dots, n\}$: 1) перестановки $\sigma \in S_n$; 2) все слова $\sigma \in \hat{S}_n$; 3) вогнутые перестановки $\sigma \in \tilde{S}_n$, у

¹Работа поддержана грантом РФФИ, проект № 14-01-00273.

которых префикс задает убывающую, а оставшийся после его удаления суффикс — возрастающую последовательность символов [3]. Отметим, что $|S_n| = n!$, $|\widehat{S}_n| = n^n$, $|\widetilde{S}_n| = 2^{n-1}$ и $\widetilde{S}_n \subset S_n \subset \widehat{S}_n$ при $n \geq 3$.

Теорема 1. На множестве перестановок S_n производящие многочлены $A_n(t, q)$ пары (des, maj) и $A_n^*(t, q)$ пары (des, inv) имеют следующие рекурсивные описания при $A_{1,1}(t, q) = A_{1,1}^*(t, q) = t$ и $m = 2, \dots, n$, $k = 1, \dots, m$:

$$A_{m,k}(t, q) = tq^{n-m+1} \sum_{i=1}^{k-1} A_{m-1,i}(t, q) + \sum_{i=k}^{m-1} A_{m-1,i}(t, q), \quad A_n(t, q) = \sum_{k=1}^n A_{n,k}(t, q),$$

$$A_{m,k}^*(t, q) = q^{k-1} \left(t \sum_{i=1}^{k-1} A_{m-1,i}^*(t, q) + \sum_{i=k}^{m-1} A_{m-1,i}^*(t, q) \right), \quad A_m^*(t, q) = \sum_{k=1}^m A_{m,k}^*(t, q).$$

Рекурсивное описание $A_n(t, q)$ теоремы 1 значительно отличается от их рекурсивного описания в [1], а соответствующее описание $A_n^*(t, q)$ в [1] отсутствует (в [4] приведены два рекуррентных соотношения для многочленов $A_n^*(t, q)$).

Теорема 2. На множестве слов $\widehat{S}_n$ производящие многочлены $\widehat{A}_n(t, q)$ пары (des, maj) и $\widehat{B}_n^*(q)$ статистики inv при $k = 1, \dots, n$, $\widehat{A}_{1,k}(t, q) = 1$, $\widehat{B}_{1,k}^*(t, q) = 1$ и $m = 2, \dots, n$ имеют следующие рекурсивные описания:

$$\widehat{A}_{m,k}(t, q) = tq^{n-m+1} \sum_{i=1}^{k-1} \widehat{A}_{m-1,i}(t, q) + \sum_{i=k}^n \widehat{A}_{m-1,i}(t, q), \quad \widehat{A}_n(t, q) = \sum_{k=1}^n \widehat{A}_{n,k}(t, q),$$

$$\widehat{B}_{m,k}^*(q) = q^{m-1} \sum_{i=1}^{k-1} \widehat{B}_{m-1,i}^*(q) + \sum_{i=k}^n \widehat{B}_{m-1,i}^*(q), \quad \widehat{B}_n^*(q) = \sum_{k=1}^n \widehat{B}_{n,k}^*(q).$$

Применение теоремы Мак-Магона к множеству слов $\widehat{S}_n$ приводит к следующему соотношению: $\widehat{B}_n(q) = \widehat{B}_n^*(q) = \sum_{|\lambda|=n} \binom{n}{\#\lambda} c_\lambda G_\lambda(q)$, где $\widehat{B}_n(q) = \widehat{A}_n(1, q)$; λ — разбиение числа n ; $|\lambda|$ — вес, а $\#\lambda$ — число частей разбиения λ ; c_λ — число композиций, соответствующих разбиению λ с записанными $n - \#\lambda$ нулями; $G_\lambda(q)$ — гауссовский полиномиальный коэффициент.

Теорема 3. На множестве вогнутых перестановок $\widetilde{S}_n$ производящие многочлены $\widetilde{A}_n(t, q)$ пары (des, maj) и $\widetilde{A}_n^*(t, q)$ пары (des, inv) имеют тривиальные рекурсивные описания, которые приводят к соотношениям

$$\widetilde{A}_n(t, q) = \sum_{k=1}^n \binom{n-1}{k-1} q^{k(k-1)/2} t^k, \quad \widetilde{A}_n^*(t, q) = \sum_{k=1}^n \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right]_q q^{k(k-1)/2} t^k = \frac{t(-t; q)_{n+1}}{1+t}$$

с биномиальными и соответственно q -биномиальными коэффициентами (аналогичное выражение для $\widetilde{A}_n^*(t, q)$ имеется в [3]).

Доказательство теорем 1–3 основано на лексикографическом упорядочении S_n , $\widehat{S}_n$, $\widetilde{S}_n$ и рассмотрении их начальных частей, имеющих соответственно мощности $m!$, n^m , 2^{m-1} , $m = 1, \dots, n$. Эти подмножества дополнительно разбиваются соответственно на m , n и m частей, а затем применяется определение статистик и индукция.

Иное упорядочение множеств S_n и $\widehat{S}_n$ позволяет упростить рекурсивные описания многочленов пары (des, maj) теорем 1 и 2, в которых множитель q^{n-m+1} заменяется на q^{m-1} и $A_m(t, q) = \sum_{k=1}^m A_{m,k}(t, q)$, а сравнение полученных рекурсивных описаний приводит к другому доказательству равенств $A_n(1, q) = A_n^*(1, q)$ и $\widehat{A}_n(1, q) = \widehat{B}_n^*(q)$.

Определение 1. Статистики $\text{fas}(\sigma) = \left\lfloor n^{-1} \sum_{i=1}^n \sigma_i \right\rfloor$ и $\text{cas}(\sigma) = \left\lceil n^{-1} \sum_{i=1}^n \sigma_i \right\rceil$ задают соответственно «пол» и «потолок» средней величины символа в слове $\sigma \in \hat{S}_n$.

Статистика fas (под именем mes) введена в [5], где с помощью рекурсивного описания установлено, что fas и des на $\hat{S}_n$ имеют производящий многочлен $\hat{A}_n(t, 1)$, иначе, fas и des — эйлеровы статистики на $\hat{S}_n$. Легко показать, что $\text{fas}(\sigma) + \text{cas}(\sigma) = n + 1$, т.е. многочлен $t^{n+1} \hat{A}_n(t^{-1})$ является производящим для статистики cas .

Теорема 4. Пары (fas, maj) и (fas, inv) , а также пары (cas, maj) и (cas, inv) одинаково распределены на $\hat{S}_n$.

Доказательство. Разобьём $\hat{S}_n$ на минимальное число подмножеств, состоящих из перестановок подходящих мультимножеств символов из алфавита $\{1, \dots, n\}$. По теореме Мак-Магона и определению 1 пары (fas, maj) и (fas, inv) , а также пары (cas, maj) и (cas, inv) одинаково распределены на этих подмножествах, что и приводит к требуемому утверждению. ■

Отметим, что для пары (des, maj) на S_n неизвестна одинаково распределённая с ней пара (e, inv) , где e — эйлерова статистика [1].

ЛИТЕРАТУРА

1. Фоата А. Распределения типа Эйлера и Мак-Магона на группе перестановок // Проблемы комбинаторного анализа. М.: Мир, 1980. С. 120–141.
2. Эндрюс Г. Теория разбиений. М.: Наука, 1982. 256 с.
3. Гульден Я., Джексон Д. Перечислительная комбинаторика. М.: Наука, 1990. 504 с.
4. Chow C. A recurrence relation for the “inv” analogue of q -Eulerian polynomials // Electronic J. Combinatorics. 2010. V. 17. #N22.
5. Бондаренко Л. Н., Шарапова М. Л. Статистики спусков и средних на множествах слов // Проблемы теоретической кибернетики. Материалы XVII Междунар. конф. (Казань, 18–20 июня 2014 г.). Казань: Отечество, 2014. С. 63–65.

УДК 519.6

DOI 10.17223/2226308X/8/2

О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ ПРЕОБРАЗОВАНИЙ РЕГИСТРОВ СДВИГА С ДВУМЯ ОБРАТНЫМИ СВЯЗЯМИ

А. М. Дорохова

Среди преобразований двоичных регистров сдвига с двумя обратными связями выделен класс подстановок, для которого получен критерий примитивности перемешивающих графов. Получены оценки экспонентов некоторых примитивных графов из данного класса.

Ключевые слова: перемешивающий граф преобразования, регистр сдвига, экспонент графа.

Введение. Актуальность исследования перемешивающих свойств криптографических функций достаточно обоснована в ряде работ (см., например, [1–5]). Точное определение существенных переменных итеративных функций весьма трудоёмко, поэтому применяется оценочный матрично-графовый подход. Перемешивающие свойства преобразования векторного пространства V_n над полем $\text{GF}(2)$ кодируются перемешиваю-