2009 Теоретические основы прикладной дискретной математики №3(5)

DOI 10.17223/20710410/5/4

УДК 65.012.810(075.8)

ПОЧТИ ВСЕ ЛАТИНСКИЕ КВАДРАТЫ ИМЕЮТ ТРИВИАЛЬНУЮ ГРУППУ АВТОСТРОФИЙ[1]

А. В. Черемушкин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: avc238@mail.ru

Доказано, что при $n \to \infty$ почти все латинские квадраты имеют тривиальную группу автострофий. Как следствие выводится асимптотическая оценка числа главных классов эквивалентности латинских квадратов порядка n.

Ключевые слова: *латинские квадраты, квазигруппы, ортогональные массивы, автострофии.*

1. Основные определения

Пусть $I_n = \{1, 2, \ldots, n\}$. Латинским квадратом порядка n называется $n \times n$-матрица $L = (l_{ij})$, строки и столбцы которой являются подстановками множества I_n. Каждый латинский квадрат L порядка n можно рассматривать как табличное задание квазигрупповой операции «$\circ$» на множестве I_n, задаваемой равенством $i \circ j = l_{ij}$, $i, j \in I_n$, либо как ортогональный массив OA(n,3,1) вида

$$L = \{(i, j, k) \mid i, j \in I_n, k = i \circ j\}. \tag{1}$$

Изотопия — это тройка подстановок $\alpha = (r, c, s) \in S_n^3$. Здесь r переставляет строки, c — столбцы, а s осуществляет замену элементов. Действие группы изотопий на множестве латинских квадратов определяется как $\alpha : L \to L^\alpha$, где

$$L^\alpha = \{(i^r, j^c, k^s) \mid (i, j, k) \in L\}.$$

Если $L^\alpha = L$, то $\alpha \in S_n^3$ называется *автотопией*. *Изострофия* — это преобразование (α, σ), где $\alpha \in S_n^3$ — изотопия, а $\sigma \in S_3$ действует на множестве троек ортогонального массива (1) путем перестановки координат в каждой тройке $(i, j, k) \in I_n$, причем

$$L^{(\alpha,\sigma)} = \{(i^r, j^c, k^s)^\sigma \ : \ (i, j, k) \in L\}.$$

Классы эквивалентности относительно группы преобразований $\langle S_n^3, S_3 \rangle = S_n^3 \wr S_3$ называются главными классами. Наконец, (α, σ) — *автострофия*, если $L^{(\alpha,\sigma)} = L$.

2. Вспомогательная лемма

Воспользуемся следующим результатом из работы [1].

Лемма 1 [1]. Пусть L — латинский квадрат с нетривиальной группой автострофий. Тогда найдется некоторый изострофный ему латинский квадрат L', имеющий изострофию (α, σ) с одной из следующих структур:

(i) $\alpha = (r, c, s)$ для некоторого простого числа p, где r, c имеют порядок p и одинаковое число m неподвижных точек, $1 \leqslant m \leqslant n/2$;

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.

(ii) $\alpha = (r, c, s)$ для некоторого простого числа p, делящего n, где r, c имеют порядок p и не имеют неподвижных точек, а s имеет порядок 1 или p; более того, если $p = 2$ и $n \equiv 2 \pmod 4$, то s имеет по крайней мере две неподвижные точки;

(iii) $(\alpha, \sigma) = (1, 1, s, (RC))$, где s имеет порядок 1 или 2 и по крайней мере одну неподвижную точку;

(iv) $\sigma = (RCS)$.

Здесь подстановка σ записывается в цикловой записи, с использованием больших букв R, C и S, соответствующих номерам строк, столбцов и элементам латинского квадрата. Поэтому запись $\sigma = (RC)$ означает транспонирование квадрата относительно главной диагонали, а $\sigma = (RCS)$ — циклическую замену элементов (i, j, k) ортогонального массива (1) на (k, i, j), где $i, j, k \in I_n$.

3. Основная теорема

Основным результатом данной работы является следующая теорема, анонсированная в [2] и уточняющая теорему 4 из работы автора [3].

Теорема 1. При $n \to \infty$ почти все латинские квадраты порядка n имеют тривиальную группу автострофий.

Доказательство. Доля латинских квадратов порядка n с нетривиальной группой автотопий составляет $T(n)/L_n$, где $T(n)$ — число латинских квадратов порядка n с нетривиальной группой автотопий, а L_n — число латинских квадратов порядка n. Для оценки этой величины воспользуемся оценкой из [4] (с. 141): при $n \to \infty$ для числа латинских квадратов L_n справедлива оценка

$$L_n > \frac{n^{n^2}}{e^{n^2}}. \tag{2}$$

В силу леммы 1 число $T(n)$ можно оценить сверху выражением

$$T(n) < (R_1(n) + R_2(n) + R_3(n) + R_4(n)) \cdot (n!)^3 3!,$$

где $R_i(n)$, $1 \leqslant i \leqslant 4$, — число латинских квадратов, имеющих автострофию, вид которой указан соответственно в пп. (i)–(iv) леммы. Найдем верхние оценки каждой из величин $R_i(n)$, $1 \leqslant i \leqslant 4$.

В случае (i) для некоторого простого числа p имеем $\alpha = (r, c, s)$, где подстановки r, c имеют порядок p и одинаковое число m неподвижных точек, $1 \leqslant m \leqslant n/2$. Пусть подстановки r и c имеют i циклов длины p, $n = ip + m$, $n/(2p) \leqslant i \leqslant n/p$. Так как при действии подстановки r строки латинского квадрата, соответствующие одному циклу этой подстановки, переходят одна в другую, то достаточно задать только i строк, а остальные $ip - i$ строк определятся однозначно. Поскольку аналогичное свойство выполняется и для столбцов, то для задания оставшихся неопределенными элементов латинского квадрата, лежащих на ip столбцах, соответствующих циклам подстановки c, достаточно задать еще по $n - ip$ элементов в i столбцах. В результате осталась неопределенной только часть латинского квадрата, содержащая $(n - ip) \times$ $\times (n - ip)$ элементов.

Поэтому число латинских квадратов, имеющих автострофию указанного вида, можно оценить выражением

$$R_1(n) \leqslant \sum_{p|n, p \geqslant 2} \sum_{\frac{n}{2p} \leqslant i \leqslant \frac{n}{p}} \left(\binom{n}{ip} \frac{(ip)!}{p^i i!} \right)^2 n! n!^i ((n - ip)!)^{n - ip + i}) <$$

$$< n^2 n!^3 \max\{n!^i((n-ip)!)^{n-i(p-1)}\}.$$

Максимальное значение величины $n!^i((n-ip)!)^{n-i(p-1)}$ на интервале $n/2 \leqslant ip < n$ достигается при $i = n/4,\ p = 2$. Применяя формулу Стирлинга

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\left(1+\frac{\theta}{12n}\right)}, \quad 0 < \theta < 1,$$

имеем

$$R_1(n) \leqslant n^2 n!^3 n!^{n/4}((n/2)!)^{3n/4} \leqslant \exp\left\{\frac{5}{8}n^2 \ln n + O(n^2)\right\}.$$

В случае (ii) для некоторого простого числа p, делящего n, имеем $\alpha = (r, c, s)$, где r, c имеют порядок p и не имеют неподвижных точек, а s имеет порядок 1 или p. Поэтому величину $R_2(n)$ можно оценить с помощью аналогичных рассуждений следующим образом:

$$R_2(n) \leqslant \sum_{p|n, p\geqslant 2}\left(\frac{n!}{p^{n/p}(n/p)!}\right)^2 n!(n!)^{n/p} < n(n!)^{n/2+3} \leqslant \exp\left\{\frac{1}{2}n^2 \ln n + O(n^2)\right\}.$$

В случае (iii) в группе автострофий с точностью до сопряжения есть подстановка вида $(\alpha, \sigma) = (1, 1, s, (RC))$, причем подстановка $\sigma = (RC)$ задает симметрию латинского квадрата относительно главной диагонали с точностью до замены элементов s. Поэтому для определения всех элементов латинского квадрата достаточно задать элементы, расположенные на главной диагонали и верхнем треугольнике. Отсюда число латинских квадратов с такими автострофиями можно оценить величиной

$$R_3(n) \leqslant 3(n!)^3 n^{n(n+1)/2} \leqslant \exp\left\{\frac{1}{2}n^2 \ln n + O(n^2)\right\}.$$

В случае (iv) в группе автострофий с точностью до сопряжения есть тройной цикл вида $\sigma = (RCS)$. Поэтому тройки (i, j, k), (k, i, j) и (j, k, i) в ортогональном массиве (1) будут либо все различны, либо все одинаковы, причем они будут совпадать в том и только в том случае, когда $i = j = k$. Отсюда число латинских квадратов с такими автострофиями можно оценить величиной

$$R_4(n) \leqslant 2(n!)^3 n^{(n^2-n)/3+n} \leqslant \exp\left\{\frac{1}{3}n^2 \ln n + O(n^2)\right\}.$$

Итак, число латинских квадратов с нетривиальной группой автострофий оценивается выражением

$$T(n) = \sum_{i=1}^{4} R_i(n) \leqslant \exp\left\{\frac{5}{8}n^2 \ln n + O(n^2)\right\} \leqslant \frac{n^{n^2}}{e^{n^2}} \exp\left\{-\frac{3}{8}n^2 \ln n(1 - O(\ln^{-1} n)\right\}.$$

Окончательно, с учетом неравенства (2), получаем

$$\frac{T(n)}{L_n} \leqslant \exp\left\{-\frac{3}{8}n^2 \ln n\ (1 - O(\ln^{-1} n))\right\}.$$

Теорема доказана. ■

В частности, из данной теоремы вытекает теорема 4 из [3].

Следствие 1. При $n \to \infty$ почти все бинарные квазигруппы порядка n имеют тривиальную группу автотопий.

4. Асимптотическая оценка

Приведем теперь асимптотическую оценку числа главных классов эквивалентности латинских квадратов порядка n.

Следствие 2. При $n \to \infty$ число главных классов эквивалентности латинских квадратов порядка n асимптотически равно

$$\frac{L_n}{6n!^3}(1 + o(1)),$$

где L_n — число латинских квадратов порядка n.

Пусть $N(n)$ — число главных классов эквивалентности порядка n, а M_n — множество представителей главных классов эквивалентности латинских квадратов порядка n с нетривиальной группой автострофий. Тогда доказательство вытекает из следующего равенства работы [1]:

$$N(n) = \frac{L_n}{6n!^3} + \sum_{L \in M_n} \frac{|Par(L)| - 1}{|Par(L)|},$$

где $Par(L)$ — группа автострофий латинского квадрата L.

ЛИТЕРАТУРА

1. *McKay B. D., Meynet A., Myrvold W.* Small latin squares, quasigroups and loops // J. Combin. Designs. 2007. V. 15. No. 2. P. 98–119. http://cs.anu.edu.au/7Ebdm/papers/ls_final.pdf
2. *Черемушкин А. В.* Почти все латинские квадраты имеют тривиальную группу автострофий // Материалы IX Междунар. семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2007 г.) / Под ред. О. М. Касим-Заде. М.: Изд-во механико-математического факультета МГУ, 2007. С. 459–460.
3. *Черемушкин А. В.* Некоторые асимптотические оценки для класса сильно зависимых функций // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 87–94.
4. *Минк М.* Перманенты. М.: Мир, 1982.