S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 11, стр. 345–353 (2014) УДК 512.54

MSC 13A99

О ПОРОЖДАЮЩИХ ГРУПП ПОДСТАНОВОК С КОНЕЧНЫМИ ПАРАМЕТРАМИ РАССЕИВАНИЯ

Н.М. СУЧКОВ, Ю.С. ТАРАСОВ

Abstract. It is proved that permutation groups of the sets of integers and natural numbers with finite dispersion parameters may be generated by a permutations, for which dispersion parameter is equal to the unit.

Keywords: permutation group, generate, dispersion parameter.

1. Введение

Пусть N, Z - множества всех натуральных и целых чисел соответственно. Если M - любое из этих множеств, то через $S(M)$ обозначена группа всех подстановок множества M. Напомним, что подстановка $x \in S(M)$ называется финитарной, если множество $\{\alpha | \alpha \in M,\ \alpha^x \neq \alpha\}$ конечно. Все такие подстановки образуют группу $Fin(M)$.

Подстановка $g \in S(M)$ называется ограниченной, если

$$w(g) = \max_{\alpha \in M} |\alpha - \alpha^g| < \infty.$$

Множество $Lim(M)$ всех ограниченных подстановок множества M является группой. Очевидно включение $Fin(M) < Lim(M)$.Группа $Fin(M)$ счетна, а группа $Lim(M)$ является уже континуальной.

Для любой подстановки $g \in S(M)$ определим её параметр рассеивания $\lambda(g)$ следующим образом. Для каждого $\alpha \in M$ полагаем

$$M_\alpha(g) = \{\beta \mid \beta \in M,\ \beta \leqslant \alpha,\ \beta^g > \alpha\},\ L_\alpha(g) = \{\beta \mid \beta \in M, \beta > \alpha,\ \beta^g \leqslant \alpha\}.$$

Пусть теперь

$$t(g) = \max_{\alpha \in M} |M_\alpha(g)|,\ s(g) = \max_{\alpha \in M} |L_\alpha(g)|,\ \lambda(g) = \max(t(g), s(g)).$$

Suchkov N.M., Tarasov Y.S., On generators of the permutation groups with finite dispersion parameters.

Поступила 1 марта 2014 г., опубликована 20 мая 2014 г.

Нетрудно понять, что множество

$$Disp(M) = \{g | g \in S(M),\, \lambda(g) < \infty\}$$

образуют группу и $\lambda(g) \leqslant w(g)$. Отсюда немедленно следует, что $Lim(M)$ есть подгруппа группы $Disp(M)$. Заметим, что при этом группа $Disp(M)$ существенно больше группы $Lim(M)$. Например, если $\alpha_1, \beta_1, \alpha_2, \beta_2, ..., \alpha_n, \beta_n, ...$ - строго возрастающая последовательность чисел из M и $\lim\limits_{n\to\infty}(\beta_n - \alpha_n) = \infty$, то для подстановки $x = (\alpha_1\,\beta_1)(\alpha_2\,\beta_2)...(\alpha_n\beta_n)...$ выполняются равенства $w(x) = \infty$, $\lambda(x) = 1$, т.е. $x \notin Lim(M)$, $x \in Disp(M)$.

Группа $Fin(M)$ является объединением строго возрастающей цепочки конечных симметрических групп. Поэтому она порождается транспозициями $b_i = (i\ \ i+1)$, где $i \in M$. Очевидно, $w(b_i) = \lambda(b_i) = 1$.

В работе [1] доказано, что

$$Lim(M) = \langle g | g \in S(M),\, w(g) = 1\rangle.$$

Заметим, что $w(g) = 1$ тогда и только тогда, когда либо g - инволюция, в разложении которой на независимые циклы учавствуют только транспозиции вида b_i, $i \in M$, либо $M = Z$ и $g \in \{d, d^{-1}\}$, где d - сдвиг, $\alpha^d = \alpha + 1$ при всех $\alpha \in Z$.

В настоящей работе мы доказываем следующую основную теорему.

Теорема 1. *Группа $Disp(M)$ порождается подстановками g множества M, для которых параметр рассеивания $\lambda(g) = 1$.*

Для случая $M = N$ получено некоторое усиление основной теоремы.

Теорема 2. *Группа $Disp(N)$ порождается подстановками множества N, которые имеют параметр рассеивания 1 и разлагаются в произведение конечных независимых циклов.*

Подробное описание подстановок множества N с параметром рассеивания равным 1 дано в леммах 2-4,6,7.

Предполагая, что подстановки группы $Disp(N)$ действуют тождественно на числах $Z\backslash N$, мы получим естественное вложение $Disp(N) < Disp(Z)$. В работах [2,3] доказано, что если $G = Disp(N)$, то

$$Disp(Z) = (Fin(Z) \cdot (G \times G^t)) \rightthreetimes \langle d\rangle,$$

где t - инволюция группы $S(Z)$, для которой $\alpha^t = -\alpha (\alpha \in Z)$. Ввиду равенства $Fin(Z) = \langle (1\,2)^{d^i} | i \in Z\rangle$ отсюда выводим, что следствием теоремы 2 является

Теорема 3. *Группа $Disp(Z)$ порождается подстановками g, g^t ($g \in G$, $\lambda(g) = 1$) и сдвигом d.*

Поскольку из равенства $\lambda(g) = 1$ следует, что и $\lambda(g^t) = 1$, то теорема 1 является непосредственным следствием теорем 2,3.

Все обозначения, используемые в данной статье, либо оговариваются, либо стандартны [4].

2. Подстановки с параметром рассеивания 1

Подстановка множества M называется равномерной, если

$$|M_\alpha(g)| = |L_\alpha(g)| < \infty$$

при любом $\alpha \in M$. Для такой подстановки $\lambda(g) = t(g) = s(g)$. В лемме 5 из [2] доказано, что множество R всех равномерных подстановок множества Z является группой, а в работе [3] доказана следующая

Лемма 1. *Пусть $x \in S(Z)$. Если $M_\gamma(x) = L_\gamma(x) = \varnothing$ для некоторого $\gamma \in Z$, то $x \in R$.*

В частности, из этой леммы следует, что $S(N) < R$. Примером подстановки, которая не является равномерной, служит сдвиг d.

Если $\alpha, \beta \in M$ и $\alpha < \beta$, то всюду в дальнейшем через $[\alpha, \beta]$ будет обозначаться множество $\{\varepsilon | \varepsilon \in M, \alpha \leqslant \varepsilon \leqslant \beta\}$, которое будем называть отрезком целых чисел.

Пусть $Q = \{\alpha_1, ..., \alpha_r\}$ - подмножество множества $M (r > 1), \alpha_1$ - наименьшее число из Q, а α_n - наибольшее. Рассмотрим подстановку

$$x = (\alpha_1 ... \alpha_r),$$

множества M, которая является конечным циклом, т.е. $\alpha_i^x = \alpha_{i+1}$ $(i = 1, ..., r-1)$, $\alpha_r^x = \alpha_1$ и $\beta^x = \beta$ при любом $\beta \in M \backslash Q$.

Лемма 2. $\lambda(x) = 1 \Leftrightarrow \alpha_1 < \alpha_2 < ... < \alpha_n$ *и либо* $n = r$, *либо* $\alpha_n > \alpha_{n+1} > ... > \alpha_r > \alpha_1$.

Доказательство. Пусть $\lambda(x) = 1$. Предположим, что $\alpha_{i+1} < \alpha_i$ для некоторого индекса $i (1 < i < n-1)$. Тогда $\alpha_i \in L_{\alpha_{i+1}}(x)$. Ясно, что найдется такой индекс $j (n \leqslant j \leqslant r)$, что $\alpha_j > \alpha_{i+1}$, $\alpha_j^x < \alpha_{i+1}$, а значит, выполняется включение $\alpha_j \in L_{\alpha_{i+1}}(x)$ и $\lambda(x) \geqslant 2$. Противоречие. Итак, $\alpha_i < \alpha_{i+1}$ при $i = 1, ..., n-1$.

Допустим теперь, что $n < r$ и $\alpha_s < \alpha_{s+1}$ для некоторого $s (n < s < r)$. Тогда $\alpha_s \in M_{\alpha_s}(x)$. Поскольку по доказаному выше $\alpha_1 < ... < \alpha_n$, то найдется такой индекс $i (1 \leqslant i \leqslant n-1)$, что $\alpha_i < \alpha_s < \alpha_{i+1}$, а потому $\alpha_i \in M_{\alpha_s}(x)$ и $|M_{\alpha_s}(x)| \geqslant 2$. Снова получили противоречие. Следовательно, либо $n = r$, либо $\alpha_n > \alpha_{n+1} > ... > \alpha_r > \alpha_1$.

Обратно. Пусть $\alpha_i < \alpha_i^x = \alpha_{i+1} (1 \leqslant i \leqslant n-1)$ и либо $n = r$, либо $\alpha_n > \alpha_{n+1} > > ... > \alpha_r > \alpha_1$. Заметим, что тогда

$$\gamma^x > \gamma (\gamma \in M) \Leftrightarrow \gamma \in \{\alpha_1, ..., \alpha_{n-1}\}.$$

Следовательно, если θ - целое число и $\alpha_i \leqslant \theta < \alpha_{i+1}$ для некоторого $i = = 1, ..., n-1$, то $M_\theta(x) = \{\alpha_i\}$. Очевидно, $M_{\alpha_n}(x) = \varnothing$, а так как $[\alpha_1, \alpha_n]^x = = [\alpha_1, \alpha_n]$ и $\varepsilon^x = \varepsilon$ при $\varepsilon \notin [\alpha_1, \alpha_n]$, то $M_\theta(x) = \varnothing$ при всех $\theta \notin [\alpha_1, \alpha_n]$. Поэтому $t(x) = 1$. Отсюда выводим, что $\lambda(x) = 1$ поскольку x - равномерная подстановка ввиду леммы 1. Лемма доказана.

Рассмотрим счетное подмножество $S = \{..., \beta_{-n}, ..., \beta_{-1}, \beta_0, \beta_1, ..., \beta_n, ...\}$ множества M и подстановку

$$w = (... \beta_{-n} ... \beta_{-1} \beta_0 \beta_1 ... \beta_n ...)$$

множества M, которая является бесконечным циклом, т.е. $\beta_i^w = \beta_{i+1} (i \in Z)$ и $\gamma^w = \gamma$ при любом $\gamma \in M \backslash S$.

Предположим, что множество S ограничено снизу(сверху). Если, например, $S \subseteq N$, то S ограничено снизу. Пусть $\beta_0 = \min\limits_{\beta \in S} \beta$ $(\beta_0 = \max\limits_{\beta \in S} \beta)$. Справедлива следующая

Лемма 3. $\lambda(w) = 1 \Leftrightarrow \beta_i < \beta_{i+1}$ *для* $i \geqslant 0$; $\beta_j < \beta_{j-1}$ *для* $j \leqslant 0$*(*$\beta_i > \beta_{i+1}$ *для* $i \geqslant 0$; $\beta_j > \beta_{j-1}$ *для* $j \leqslant 0$*)*.

Доказательство. Пусть $\lambda(w) = 1$ и, например, $\beta_0 = \min\limits_{\beta \in S} \beta$. Если $\beta_{i+1} < \beta_i$ для некоторого $i > 0$, то β_i содержится в множестве $L_{\beta_{i+1}}(w)$ в силу определений. Но при этом найдется такой индекс $j > 0$, что выполняются неравенства

$\beta_j > \beta_{i+1}$, $\beta_j^w = \beta_{j+1} < \beta_{i+1}$, а значит, $\beta_j \in L_{\beta_{i+1}}(w)$ и $|L_{\beta_{i+1}}(w)| \geqslant 2$. Получили противоречие с равенством $\lambda(w) = 1$. Итак, $\beta_i < \beta_{i+1}$ при всех $i \geqslant 0$. Так как $\lambda(w^{-1}) = \lambda(w) = 1$, то аналогично вышеизложенному устанавливаем справедливость неравенств $\beta_0 < \beta_{-1} < ... < \beta_{-n} < ...$.

Обратно. Допустим, что $\beta_i < \beta_{i+1} = \beta_i^w (i \geqslant 0)$ и $\beta_j = \beta_{j-1}^w < \beta_{j-1}$ $(j \leqslant 0)$. Если θ - произвольное число из множества M и $\theta < \beta_0$, то $\alpha^w = \alpha$ при всех $\alpha \leqslant \beta_0$, а потому $M_\theta(w) = \varnothing$. Если же $\theta \geqslant \beta_0$, то $\beta_i \leqslant \theta < \beta_{i+1}$ для некоторого неотрицательного индекса i. Из этого следует, что $M_\theta(w) = \{\beta_i\}$. В силу леммы 1 $\lambda(w) = 1$. Лемма доказана.

Пусть теперь множество S не является ограниченным сверху и снизу. Ясно, что это возможно только при $M = Z$.

Лемма 4. $\lambda(w) = 1 \Leftrightarrow \beta_i < \beta_{i+1} (\beta_i > \beta_{i+1})$ *при всех целых* i.

Доказательство. Пусть $\lambda(w) = 1$. Предположим, что $\beta_0 < \beta_1$ и найдется такое натуральное s, что $\beta_0 < \beta_1 < ... < \beta_s$, $\beta_{s+1} = \beta_s^w < \beta_s$. Тогда в силу определений $\beta_{s-1} \in M_{\beta_s - 1}(w)$, $\beta_s \in L_{\beta_s - 1}(w)$. Так как множество S не является ограниченным сверху, то найдется такое целое k, что $\beta_k > \beta_s$. Из определения цикла следует, что $\beta_k = \beta_s^{w^j}$ для некоторого целого j. Если $j > 0$, то найдется такой индекс $e (0 < e < j)$, что $\beta_s^{w^e} = \beta_{s+e} \leqslant \beta_s - 1$, $\beta_{s+e}^w > \beta_s - 1$ и, следовательно, $\beta_{s+e} \in M_{\beta_s - 1}(w)$. Но тогда $|M_{\beta_s - 1}(w)| \geqslant 2$. Получили противоречие с равенством $\lambda(w) = 1$. Если же $j < 0$, то $\beta_s = \beta_k^{w^{-j}}$. Поэтому существует такое целое $m (0 \leqslant m < -j)$, что выполняются неравенства $\beta_k^{w^m} = \beta_{k+m} > \beta_s - 1$, $\beta_{k+m}^w \leqslant \beta_s - 1$. Отсюда $\beta_{k+m} \in L_{\beta_s - 1}(w)$ и множество $L_{\beta_s - 1}(w)$ содержит не менее двух элементов. Снова получили противоречие.

Итак, следствиями неравенства $\beta_0 < \beta_1$ являются все неравенства $\beta_0 < \beta_1 < \beta_2 < ... < \beta_n < ...$. Точно так же доказывается, что если $\beta_i < \beta_{i+1}$ для некоторого целого i, то $\beta_i < \beta_{i+1} < ... < \beta_{i+n} < ...$. Поэтому если $\beta_i < \beta_{i+1}$, $\beta_{i-1} > \beta_i$, то $\beta_i < \beta_{i-1} < \beta_{i-2} < ... < \beta_{i-n} < ...$ и $\beta_i = \min\limits_{\beta \in S} \beta$, что противоречит определению множества S. Таким образом, либо $\beta_i > \beta_{i+1}$ при всех целых i, либо все эти неравенства противоположны.

Обратно. Пусть $\beta_i < \beta_i^w = \beta_{i+1} (\beta_i > \beta_i^w = \beta_{i+1})$ при всех целых i. Фиксируем любое $\theta \in Z$. Тогда $\beta_m \leqslant \theta < \beta_{m+1} (\beta_{m+1} \leqslant \theta < \beta_m)$ для единственного целого m. Поэтому $M_\theta(w) = \{\beta_m\} (M_\theta(w) = \varnothing)$, $L_\theta(w) = \varnothing (L_\theta(w) = \{\beta_m\})$, а значит, $\lambda(w) = 1$. Лемма доказана.

В последних трех леммах мы полностью описали циклы множества M с параметром рассеивания равным 1. Перейдем теперь к изучению произвольных таких подстановок. Любая подстановка g группы $S(M)$ разлагается в произведение независимых циклов x_i, где i пробегает конечное или счетное множество индексов I. Ясно, что если $\lambda(g) = 1$, то и $\lambda(x_i) = 1$ при любом $i \in I$.

Пусть $u = (\gamma_1 ... \gamma_m)$, $v = (\varepsilon_1 ... \varepsilon_k)$, $w = (... \beta_{-n} ... \beta_{-1} \beta_0 \beta_1 ... \beta_n ...)$ - три цикла группы $S(M)$. Полагаем по определению

$$u < v \Leftrightarrow \gamma_i < \varepsilon_j (1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant k),$$

$$u < w \Leftrightarrow \gamma_i < \beta_j (1 \leqslant i \leqslant m;\ j \in Z).$$

Лемма 5. *Если* u, v *- различные циклы из разложения подстановки* $g \in S(M)$ *на независимые циклы и* $\lambda(g) = 1$, *то либо* $u < v$, *либо* $v < u$.

Доказательство. Мы можем считать, что $\gamma_1 = \min(\gamma_1, ..., \gamma_m)$, $\varepsilon_1 = \min(\varepsilon_1, ..., \varepsilon_k)$. Пусть $\gamma_n = \max(\gamma_1, ..., \gamma_m)$, $\varepsilon_s = \max(\varepsilon_1, ..., \varepsilon_k)$. В силу условия $\lambda(u) =$

$= \lambda(v) = 1$. Описание таких циклов дано в лемме 2. В частности, выполняются неравенства

$$\gamma_1 < \gamma_2 < ... < \gamma_n;\ \varepsilon_1 < \varepsilon_2 < ... < \varepsilon_s.$$

Предположим для определенности, что $\gamma_1 < \varepsilon_1$. Покажем, что тогда $u < v$. В самом деле, для этого достаточно установить неравенство $\gamma_n < \varepsilon_1$. Пусть это не так, т.е. $\gamma_n > \varepsilon_1 (\gamma_n \neq \varepsilon_1$, в силу независимости по условию циклов $u, v)$. Тогда $\gamma_i < \varepsilon_1 < \gamma_{i+1}$ для некоторого индекса $i (1 \leqslant i \leqslant n-1)$. Отсюда из определений следует, что $\gamma_i, \varepsilon_1 \in M_{\varepsilon_1}(g)$ и $\lambda(g) > 1$. Получили противоречие с условием леммы. Итак, $\gamma_n < \varepsilon_1$, а значит, $u < v$. Если $\varepsilon_1 < \gamma_1$, то аналогично проверяется, что $v < u$. Лемма доказана.

Простым следствием леммы 5 является следующий результат

Лемма 6. *Пусть подстановка g множества N разлагается на конечные независимые циклы. Параметр рассеивания подстановки g равен 1 тогда и талько тогда, когда это разложение имеет вид $g = x_1 x_2 ...$, где $x_1 < x_2 < ...$ и $\lambda(x_i) = 1$, $i = 1, 2, ...$.*

Лемма 7. *Пусть в разложении подстановки g множества N на независимые циклы имеется бесконечный цикл w. Если $\lambda(g) = 1$, то это разложение имеет вид*

$$g = x_1 ... x_m\, w,$$

где $x_1 ... x_m$ - конечные циклы и $x_1 < x_2 < ... < x_m < w$.

Доказательство. Пусть $w = (... \beta_{-n} ... \beta_{-1}\, \beta_0\, \beta_1 ... \beta_n ...)$, где $\beta_0 = \min\limits_{i \in Z} \beta_i$. В силу условия $\lambda(w) = 1$, следовательно, согласно лемме 3

$$\beta_0 < \beta_1 < ... < \beta_n < ...;\ \beta_0 < \beta_{-1} < ... < \beta_{-n} < ... .$$

Предположим, что в разложении g на независимые циклы есть еще один бесконечный цикл $w_1 = (... \gamma_{-n} ... \gamma_{-1}\, \gamma_0\, \gamma_1 ... \gamma_n ...)$ и $\gamma_0 = \min\limits_{i \in Z} \gamma_i$. Так как $\lambda(w_1) = 1$, то снова по лемме 3

$$\gamma_0 < \gamma_1 < ... < \gamma_n < ... .$$

Обозначим через s любой такой положительный индекс, что $\beta_s > \gamma_0$. Тогда $\gamma_k < \beta_s < \gamma_{k+1}$ для некоторого $k \geqslant 0$. Поскольку $\gamma_{k+1} = \gamma_k^{w_1} = \gamma_k^g > \gamma_k$, то $\beta_s, \gamma_k \in M_{\beta_s}(g)$. Противоречие с равенством $\lambda(g) = 1$. Итак, w - единственный бесконечный цикл в разложении g на независимее циклы. Предположим теперь, что в этом разложении имеется конечный цикл $x = (\alpha_1 ... \alpha_r)$, $\alpha_n = \max(\alpha_1, ..., \alpha_r)$ и найдется такой индекс $l \leqslant 0$, что $\beta_l < \alpha_n < \beta_{l-1}$. Тогда

$$\beta_{l-1}^w = \beta_{l-1}^g = \beta_l \leqslant \alpha_n - 1,\ \alpha_n^x = \alpha_n^g \leqslant \alpha_n - 1$$

и мы имеем $\beta_{l-1}, \alpha_n \in L_{\alpha_n - 1}(g)$. Это противоречит равенству $\lambda(g) = 1$. Итак, выполняется неравенство $\alpha_n < \beta_0$, а потому $x < w$. Отсюда следует конечность числа конечных независимых циклов в разложении подстановки g. В силу леммы 5 их можно линейно упорядочить. Лемма доказана.

3. Разложение цикла

Рассмотрим произвольный конечный цикл $x = (\alpha_1\, \alpha_2 ... \alpha_r)$, где $\alpha_1, ..., \alpha_r$ - целые числа, $\alpha_1 = \min(\alpha_1, ..., \alpha_r)$, $\alpha_n = \max(\alpha_1, ..., \alpha_r)$. Исходя из x, определим цикл

$$\overline{x} = (\alpha_{i_1} ... \alpha_{i_s}),$$

где $\alpha_{i_1} = \alpha_1$; если α_{i_j} определено и $i_j < n$, то $\alpha_{i_{j+1}}$ - первое из чисел последовательности α_{i_j+1}, ..., α_n, которое больше α_{i_j}. Пусть k такое натуральное число, что $i_k = n$. Если $n = r$, то полагаем $s = k$ и цикл $\overline{x}$ определен. Если же $i_k = n < r$ и α_{i_t} определено ($t \geqslant k$, $i_t < r$), то $\alpha_{i_{t+1}}$ - первое из чисел последовательности α_{i_t+1}, ..., α_r, которое меньше α_{i_t} (если такого числа нет, то полагаем $s = t$ и цикл $\overline{x}$ определен). В силу наших построений найдется такое натуральное s, что либо $i_s = r$, либо α_{i_s} меньше каждого из чисел α_{i_s+1}, ..., α_r. Построение цикла $\overline{x}$ завершено.

Отметим, что непосредственным следствием определения $\overline{x}$ является следующие неравенства:

$$i_1 < i_2 < ... < i_k,\ \alpha_1 = \alpha_{i_1} < \alpha_{i_2} < ... < \alpha_{i_k} = \alpha_n \tag{1}$$

и либо $s = k$, либо

$$i_k < i_{k+1} < ... < i_s,\ \alpha_{i_k} = \alpha_n > \alpha_{i_{k+1}} > ... > \alpha_{i_s}. \tag{2}$$

В частности, ввиду леммы 2 $\lambda(\overline{x}) = 1$. Рассмотрим теперь подстановку $y = x\overline{x}^{-1}$. Прямое вычисление показывает, что

$$y = (\alpha_{i_1}\ \alpha_{i_1+1} \dots \alpha_{i_2-1})(\alpha_{i_2}\ \alpha_{i_2+1} \dots \alpha_{i_3-1}) \dots (\alpha_{i_s}\ \alpha_{i_s+1} \dots \alpha_r).$$

Лемма 8. $\lambda(y) = \lambda(x) - 1$.

Доказательство. Сравним множества $M_\theta(x)$ и $M_\theta(y)$ при каждом $\theta \in Z$. Так как $\gamma^x = \gamma^y = \gamma$ для $\gamma \notin [\alpha_1, \alpha_n]$, то $M_\theta(x) = M_\theta(y) = \varnothing$ при $\theta \notin [\alpha_1, \alpha_n]$. Очевидно, $M_{\alpha_n}(x) = M_{\alpha_n}(y) = \varnothing$. Если $\gamma^x = \gamma^y (\gamma \in Z)$, то $\gamma \in M_\theta(x) \Leftrightarrow \gamma \in M_\theta(y)$. Поэтому мы будем проверять принадлежность множествам $M_\theta(x)$ и $M_\theta(y)$ чисел γ, для которых $\gamma^x \neq \gamma^y$. Легко видеть, что такие γ составляют множество

$$T = \{\alpha_{i_j-1} | j = 2, ..., s\} \cup \{\alpha_r\}.$$

Так как $\alpha_r^x = \alpha_1 < \alpha_r$, $\alpha_r^y = \alpha_{i_s} \leqslant \alpha_r$ (определение цикла $\overline{x}$), то α_r не содержится в множествах $M_\theta(x)$, $M_\theta(y)$ при любом $\theta \in Z$ в силу их определений.

Далее, при каждом $j = 2, ..., s$ мы имеем

$$\alpha^x_{i_j-1} = \alpha_{i_j},\ \alpha^y_{i_j-1} = \alpha_{i_{j-1}}. \tag{3}$$

Пусть $k < j \leqslant s$. Тогда из (2) в силу определения цикла $\overline{x}$ выводим неравенства $\alpha_{i_j} < \alpha_{i_j-1}$, $\alpha_{i_{j-1}} \leqslant \alpha_{i_j-1}$, из которых с учетом соотношений (3) следует, что α_{i_j-1} не содержится в множествах $M_\theta(x)$, $M_\theta(y)$.

Таким образом, вместо множества T мы можем ограничится рассмотрением его подмножества

$$T_1 = \{\alpha_{i_j-1} | j = 2, ..., k\}$$

и при этом предполагать, что $\alpha_1 \leqslant \theta < \alpha_n$. Будем дополнительно считать, учитывая неравенства (1), что

$$\alpha_{i_{q-1}} \leqslant \theta < \alpha_{i_q}, \tag{4}$$

где $2 \leqslant q \leqslant k$. Из построения цикла $\overline{x}$ следует, что для $\alpha_{i_j-1} \in T_1$ выполняются неравенства

$$\alpha_{i_j-1} \leqslant \alpha_{i_{j-1}} < \alpha_{i_j}.$$

Отсюда ввиду (3) мы имеем $\alpha_{i_q-1} \leqslant \alpha_{i_{q-1}} \leqslant \theta$, $\alpha^x_{i_q-1} = \alpha_{i_q} > \theta$, $\alpha^y_{i_q-1} = \alpha_{i_{q-1}} \leqslant \theta$, а значит, $\alpha_{i_q-1} \in M_\theta(x)$ и $\alpha_{i_q-1} \notin M_\theta(y)$.

Предпложим теперь, что j целое отличное от q число и $2 \leqslant j \leqslant k$. Если $q > 2$ и $j < q$, то $\alpha^x_{i_j-1} = \alpha_{i_j} \leqslant \alpha_{i_{q-1}} \leqslant \theta$, $\alpha^y_{i_j-1} = \alpha_{i_{j-1}} < \alpha_{i_{q-1}} \leqslant \theta$, а потому

α_{i_j-1} не содержится в множествах $M_\theta(x)$ и $M_\theta(y)$. Пусть $q < k$ и $j > q$. Тогда $\alpha^x_{i_j-1} = \alpha_{i_j} > \alpha_{i_q} > \theta$, $\alpha^y_{i_j-1} = \alpha_{i_{j-1}} \geqslant \alpha_{i_q} > \theta$. Отсюда выводим, что если $\alpha_{i_j-1} \leqslant \theta$, то α_{i_j-1} содержится в множествах $M_\theta(x)$ и $M_\theta(y)$, а если $\alpha_{i_j-1} > \theta$, то α_{i_j-1} не содержится в этих множествах.

Итак, $M_\theta(x) = M_\theta(y) \cup \{\alpha_{i_q-1}\}$ для всех θ, удовлетворяющих неравенствам (4). Если же θ не удовлетворяет этим неравенствам при любом $q = 2, ..., k$, то по доказанному выше $M_\theta(x) = M_\theta(y) = \varnothing$. Это позволяет нам заключить, что $t(x) = t(y) + 1$. Согласно лемме 1 отсюда вытекает равенство $\lambda(x) = \lambda(y) + 1$. Лемма доказана.

4. Доказательство теоремы 2

Лемма 9. *Пусть подстановка g группы $Disp(M)$ разлагается на конечные независимые циклы. Тогда $g = g_1\, g_2 \ldots g_s$, где каждая подстановка $g_j (1 \leqslant j \leqslant s)$ содержится в этой группе и разлагается на конечные независимые циклы с параметром рассеивания равным 1.*

Доказательство. Пусть $\lambda(g) = m$ и $g = x_1\, x_2 \ldots$ - разложение g на конечные независимые циклы $x_1, x_2, \ldots$. Очевидно, что тогда $\lambda(x_i) \leqslant m$ для всех $i = 1, 2, \ldots$. Поэтому существует натуральное число

$$l = \max_i \lambda(x_i) \leqslant m.$$

Будем вести доказательство леммы индукцией по l. Если $l = 1$, то лемма верна ($s = 1$, $g_1 = g$). Пусть $l > 1$ и $x_{j_1}, x_{j_2}, \ldots$ - все циклы из разложения g, параметр рассеивания которых равен l. Для каждого $k = 1, 2, \ldots$ обозначим через $\overline{x}_{j_k}$ цикл с параметром рассеивания равным 1, построенный из x_{j_k} по схеме построения в самом начале раздела 3. Если $y_{j_k} = x_{j_k}\overline{x}^{-1}_{j_k}$, то согласно лемме 7 $\lambda(y_{j_k}) = l - 1$. В частности, в разложении y_{j_k} на независимые циклы, параметр рассеивания каждого из этих циклов не превосходит $l - 1$.

Пусть теперь $h = \overline{x}_{j_1}\, \overline{x}_{j_2} \ldots$; $y = gh^{-1}$. Каждый независимый цикл в разложении подстановки y либо совпадает с одним из циклов x_i, для которого $\lambda(x_i) < l$, либо является независимым циклом из разложения некоторой подстановки y_{j_k}, а потому его параметр рассеивания также меньше l. По индуктивному предположению $y = g_1 \cdot \ldots \cdot g_{s-1}$, где каждая подстановка g_j разлакается на конечные независимые циклы с параметром рассеивания 1. Так как $g = yh$, то полагая $g_s = h$, мы получим искомое разложение подстановки g. Лемма доказана.

Лемма 10. *Пусть подстановка h группы $G = Disp(N)$ разлагается на конечные независимые циклы с параметром рассеивания равным 1. Если $\lambda(h) = n$, то $h = h_1 \cdot \ldots \cdot h_n$, где $h_i \in G$, $\lambda(h_i) = 1$ и h_i разлагается на конечные независимые циклы $(1 \leqslant i \leqslant n)$.*

Доказательство. Индукция по n. Если $n = 1$, то лемма очевидна. Пусть $n > 1$. Для произвольного цикла $x = (\alpha_1 \ldots \alpha_r)$, составленного из натуральных чисел, введем обозначения

$$m(x) = \min\{\alpha_1, ..., \alpha_r\},\ l(x) = \max\{\alpha_1, ..., \alpha_r\}.$$

Заметим, что прямо из определений следует, что

$$M_\beta(x) \neq \varnothing \Leftrightarrow m(x) \leqslant \beta < l(x),$$

где $\beta \in N$. Обозначим через W множество всех циклов из разложения h на независимые циклы. В силу условия параметр рассеивания каждого цикла из W равен 1. Понятно, что следствием равенства $M_\beta(h) = n$ является существование таких n циклов t_1, ..., t_n из W, что

$$M_\beta(t_1) \cup ... \cup M_\beta(t_n) = M_\beta(h),\ |M_\beta(t_i)| = 1(1 \leqslant i \leqslant n).$$

Пусть теперь $\alpha_1 < \alpha_2 < ...$ - все натуральные числа, для которых $|M_{\alpha_i}(h)| = n$ $(i = 1, 2, ...)$. Возьмем произвольный цикл $x_1 \in W$, для которого $M_{\alpha_1}(x_1) \neq \varnothing$ и обозначим через s такое натуральное число, что множества $M_{\alpha_1}(x_1)$, ..., $M_{\alpha_{s-1}}(x_1)$ не пусты, а $M_{\alpha_s}(x_1) = \varnothing$. Из определения α_s следует, что существуют точно n циклов $y_i(1 \leqslant i \leqslant n)$ множества W, для которых $M_{\alpha_s}(y_i) \neq \varnothing$. Мы утверждаем, что найдется такой индекс $j(1 \leqslant j \leqslant n)$, что

$$m(y_j) > \gamma = l(x_1).$$

В самом деле, предположим, что выполняются n неравенств

$$m(y_1) < \gamma,\ m(y_2) < \gamma,\ ...,\ m(y_n) < \gamma.$$

Тогда $m(y_i) \leqslant \gamma - 1 < l(x_1) < l(y_i)$ для каждого $i = 1, ..., n$. Это означает, как отмечалось выше, что $|M_{\gamma-1}(y_i)| = 1$, но поскольку и $|M_{\gamma-1}(x_1)| = 1$, то $|M_{\gamma-1}(h)| > n$. это противоречит условию теоремы. Итак, $m(y_j) > l(x_1)$ для некоторого индекса j.

Обозначим $y_j = x_2$. Нами установлено неравенство $x_1 < x_2$ и при этом $M_{\alpha_s}(x_2) \neq \varnothing$ в силу определения циклов y_1, ..., y_n. Пусть $M_{\alpha_{s+1}}(x_2)$, $M_{\alpha_{s+2}}(x_2)$, ..., $M_{\alpha_{k-1}}(x_2)$ - непустые множества, а $M_{\alpha_k}(x_2) = \varnothing$. Аналогично вышеизложенному установим существование такого цикла $x_3 \in W$, что $x_2 < x_3$ и $M_{\alpha_k}(x_3) \neq \varnothing$. Продолжая эти рассуждения, мы найдем циклы $x_1 < x_2 < x_3 < ...$ из множества W такие, что для каждого $\alpha_i(i = 1, 2, ...)$ существует цикл x_j для некоторого $j = 1, 2, ...$, что $M_{\alpha_i}(x_j) \neq \varnothing$. Поэтому если $h_1 = x_1 x_2 x_3 ...$, то $\lambda(h_1) = 1$ (лемма 6) и $\lambda(h_1^{-1}h) = n - 1$ (подстановка $h_1^{-1}h$ получается из разложения подстановки h на независимые циклы удалением циклов x_1, x_2, x_3, ...). По индуктивному предположению $h_1^{-1}h = h_2 \cdot ... \cdot h_n$, где $\lambda(h_i) = 1$ $(2 \leqslant i \leqslant n)$. Это доказывает лемму.

Приступим к непосредственному доказательству теоремы 2. Итак, пусть $G = Disp(N)$. При доказательстве теоремы 1 из работы [2] установленно, что каждое конечное подмножество группы G содержится в группе вида $H = AB$, где каждая из подгрупп A и B является объединением возрастающей цепочки подгрупп, которые оставляют на месте компоненты некоторых разбиений множеста N на отрезки натуральных чисел. В частности, подстановки из A и B разлагаются на конечные независимые циклы и группа G порождается такими подстановками. Отсюда и из лемм 9,10 непосредственно выводим, что группа G порождается подстановками с параметром рассеивания равным 1, которые разлагаются на конечные независимые циклы. Теорема 2 доказана.

Как отмечалось во введении, теоремы 1,3 являются следствиями теоремы 2.

Список литературы

[1] Н.М. Сучков, Н.Г. Сучкова, *О группах ограниченных подстановок, журнал СФУ, Сер. математика и физика, 3:2 (2010), 262-266.*

[2] Н.М. Сучков, А.А. Маньков, Ю.С. Тарасов, *Группы подстановок с конечными параметрами рассеивания*, Журнал СФУ, Сер. математика и физика, **5**:1 (2012), 116–121.

[3] Н.М. Сучков, Ю.С. Тарасов, *О равномерных подстановках с конечными параметрами рассеивания*, Тр. ИММ УрО РАН, **19**:3 (2013), 284-289.

[4] М.И. Каргаполов, Ю.И.Мерзляков, *Основы теории групп*, изд. Лань, (2009).

Николай Михайлович Сучков
Сибирский федеральный университет,
Институт математики и фундаментальной информатики
пр. Свободный, 79,
660041, Красноярск, Россия
E-mail address: ns7654321@mail.ru

Юрий Сергеевич Тарасов
Красноярское региональное отделение международной
академии экологии и природопользования
пр. Свободный, 68,
660041, Красноярск, Россия
E-mail address: gigtorus@yandex.ru