УДК 512.543

Р.В. СКУРАТОВСКИЙ

КОПРЕДСТАВЛЕНИЕ СИЛОВСКОЙ p-ПОДГРУППЫ ГРУППЫ S_n

Ключевые слова: *автоматная группа, копредставление, соотношения*.

Силовские p-подгруппы конечной симметрической группы подстановок играют в классе конечных p-групп такую же важную роль, как и симметрические группы в классе всех конечных групп. Каждая конечная p-подгруппа изоморфно погружается в силовскую p-подгруппу некоторой симметрической группы. Поэтому в настоящей статье исследовано представление таких групп в виде порождающих и соотношений. Также исследуется итерированное сплетение [1], которое связано с группой конечных автоматных преобразований.

Как известно, силовская p-подгруппа симметрической группы степени n изоморфна прямому произведению

$$P = P_1^{a_1} \times P_2^{a_2} \times \ldots \times P_m^{a_m},$$

где P_k — силовская p-подгруппа группы S_{p^k}, причем [2, теорема 3.3.3] каждая такая P_k изоморфна k-кратному сплетению регулярных циклических групп степени p:

$$P_k \cong \wr_{i=1}^{k} C_i .$$

Если $R(T_k)$ — копредставление для P_k, то соответствующее копредставление для P есть силовская подгруппа в S_n:

$$P \simeq \left\langle \begin{matrix} t_{ikz} \mid R(T_k),\ t_{ikz}t_{jks} = t_{jks}t_{ikz},\ 0 \le i,\ j < k \le m,\ 1 \le z,\ s \le \alpha_k, \\ t_{lkz}t_{j\upsilon s} = t_{j\upsilon s}t_{lkz},\ 1 \le z \le \alpha_k,\ 1 \le s \le \alpha_\upsilon,\ 1 \le k, \upsilon \le m \end{matrix} \right\rangle,$$

где t_{ikz} — i-й образующий подгруппы P_z, сопряженной к P_k; T_k — образующие подгруппы P_k, $1 \le k \le m$. Отметим, что P является нильпотентной как p-группа. Найдем копредставление для силовской p-подгруппы группы S_{p^k}. Легко убедиться, что она является максимальной нильпотентной транзитивной подгруппой в S_{p^k}. Напомним основные понятия.

Дано две группы подстановок: (G, M) и (H, N). Рассмотрим сплетение групп $(G, M) \wr H$, определим действие $(G, M) \wr H$ на $M \times N$: $\{[f_1; f_2(x)] \mid f_1 \in G$, $f_2 : M \to H, (m, n)^{[f_1; f_2(x)]} \to (m^{g_1}, n^{h_2(m)})\}$.

Правило умножения в группе $G \wr H$ в общем виде запишется как $[f_1; f_2(x)] \times [g_1; g_2(x)] = [f_1 g_1; f_2(x) g_2(x^{f_1})]$, где $[f_1; f_2(x)]$, $[g_1; g_2(x)]$ — элементы группы $G \wr H$. В данном случае $G = C_p = M$ и $H = N = C_p$, т.е. обе группы действуют сами на себе. Необходимо лишь задать действие, пусть это будут левые сдвиги.

Представим элементы группы $C_p \wr C_p$ в виде таблиц $[g; h_1, \ldots, h_p] \times [g'; h_1', \ldots, h_p'] = [gg'; h_1 h'_{g(1)}, h_2 h'_{g(2)}, \ldots, h_p h'_{g(p)}]$.

Лемма 1. Элементы $x_1 = [a; e, e, \ldots, e]$, $x_2 = [e; a, e, \ldots, e]$ являются системой образующих в $C_p \wr C_p$, где x_1, x_2 — управляющий и пассивный элементы, а система образующих для $P_k \cong \wr_{i=1}^{k} C_p$ имеет вид

$$\begin{aligned} x_{n,1} &= [[[[[a; e, e, \ldots, e] e, e, \ldots, e] e, e, \ldots, e] \ldots] e, e, \ldots, e] = \\ &= [[[[[x_{2,1}] e, e, \ldots, e] e, e, \ldots, e] \ldots] e, e, \ldots, e], \\ x_{n,2} &= [[[[[e; a, e, \ldots, e] e, e, \ldots, e] e, e, \ldots, e] \ldots] e, e, \ldots, e] = \\ &= [[\ldots[[[x_{2,2}] e, e, \ldots, e] e, e, \ldots, e] \underbrace{\ldots}_{n-4}] e, e, \ldots, e], \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n,n-1} &= [[x_{n-1,n-1}] e, e, \ldots, e], \\ x_{n,n} &= [[E] a, e, e, \ldots, e] = [[[[[e; e, e, \ldots, e] e, e, \ldots, e] e, e, \ldots, e] \ldots] a, e, \ldots, e]. \end{aligned} \tag{1}$$

Докажем это индукцией по количеству множителей. Так, для $C_p \wr C_p$ имеем $x_1 \cdot x_2 = [a; e, e, \ldots, e] \cdot [e; a, e, \ldots, e] = [a \cdot e; e \cdot e, e \cdot e, \ldots, e \cdot a]$.

Если подействовать слева элементом x_1^{-i} на x_2, то он «смещает» элементы таблицы, которые есть элементами подгруппы, являющейся базой сплетения H, влево на i позиций. Тогда

$$x_1^{-1} x_2 x_1 = [a^{-1}; e, e, \ldots, e] \cdot [e; a, e, \ldots, e] \cdot [a; e, e, \ldots, e] = [e; e, a, \ldots, e].$$

Таким образом, можно «переставлять» элемент a в таблице $[e; a, \ldots, e, e] = WT = x_2$ на любую позицию из H.

Пусть $WT[i]$ — i-й элемент таблицы $i \in \{0, \ldots, p\}$. Перемножив $\underbrace{x_2 \cdot x_2 \cdot \ldots \cdot x_2}_{i \text{ раз}} = [e; a^i, e, e]$, $i = \overline{0, p-1}$, аналогичным образом, можно смещать элемент a^i на любую позицию, которой соответствуют элементы из базы H, т.е. $WT[j]$, $j \in \{1, \ldots, p\}$.

Далее очевидно, что элементы вида $[e; h_1, h_2, \ldots, h_p] \cdot [e; h_1', h_2', \ldots, h_p']$ умножаются прямо, т.е. поэлементно, поэтому можно получить любой элемент вида $[e; a^{i_0}, a^{i_2}, \ldots, a^{i_{p-1}}] = WT$, $i_j \in \{0, 1, \ldots, p-1\}$. Отсюда ясно, что $x_1^{-i} x_2 x_1^i x_2 = x_2 x_1^{-i} \times x_2 x_1^i$, $i \in \{1, \ldots, p-1\}$.

Определение 1. Назовем элементами k-го уровня L_k элементы, образовавшиеся при сопряжении образующего группы C_p, которую умножили на k-й итерации.

На n-м шаге индукции имеем группу $G=(\ldots((C_p \wr C_p)\wr C_p)\ldots)\wr C_p$, где C_p — подгруппа группы подстановок. В силу ассоциативности сплетения групп подстановок на классе всех групп подстановок [1] имеем $G=C_p \wr (\ldots(C_p \wr (C_p \wr C_p))\ldots)$. Здесь элементы группы, которую умножили на произведение, полученное на последней итерации, принадлежат L_n. Они являются пассивными элементами самой большой таблицы. Элементы, образовавшиеся на n-й итерации, обозначим $x_{n,m}$, где m — номер образующего, в частности $x_{n,n}=[[[[[e;e,e,\ldots,e]e,e,\ldots,e]e,e,\ldots,e]\ldots]a,e,\ldots,e]$ — образующий элемент из L_n. Поскольку элементы из L_n образуют прямое произведение, то умножаются они прямо. Элементы из всех предшествующих уровней действуют левым сдвигом на элементах из L_n и перемещают образующий из L_n по всем позициям пассивной части $x_{n,n}$. Значит, образующими для G являются элементы (1).

Легко убедиться, что $x_{m-1,1}^{-i}x_{m,1}x_{m-1,1}^{i}x_{n,1}=x_{n,1}x_{m-1,1}^{-i}x_{m,1}x_{m-1,1}^{i}$, $i\in\{1,\ldots,p-1\}$, где x_m — образующий m-го уровня, x_{m-1} и x_n — образующие из L_{m-1} и L_n.

Итерируя операцию сплетения, получаем на n-й итерации следующую конструкцию: таблицы предыдущего уровня вложены в таблицы следующего уровня и являются их активными элементами. В силу изменения порядка умножения элемент первой группы является чисто активным и действует на остальных элементах. Он содержится в первой таблице, которая имеет наиболее глубокий уровень вложения. Кроме того, p пассивных элементов этой таблицы действуют на соответствующих сегментах пассивной части второй таблицы, которая непосредственно содержит описанную выше таблицу в качестве активной, а именно первый пассивный элемент h_1 первой таблицы действует на первых p пассивных элементах $h_{1,i}$, $i=1,\ldots,p$, второй таблицы. Аналогично первый пассивный элемент h_2 второй таблицы действует на следующих p пассивных элементах $h_{2,i}$, $i=1,\ldots,p$, третьей таблицы и т.д. Таким образом, вторая таблица содержит p^2 пассивных элементов. Третья таблица содержит p^3 пассивных элементов, которые также разделены на сегменты действия пассивных элементов из предыдущей таблицы.

Далее обозначим образующий элемент из L_k как $x_{n,k,1}$ для $k\in\{1,\ldots,n\}$.

Лемма 2. Выполняются соотношения $x_{n,n,1}x_{n,k,l}=x_{n,k,l}x_{n,n,1}$, $l\neq 1 \pmod p$, $x_{n,n,m}x_{n,k,1}=x_{n,k,1}x_{n,n,m}$, где $x_{n,n,m}$ — m-й элемент из L_n, $k\le n$, $m>p^{n-k}$, для n-кратного сплетения.

Докажем индуктивно справедливость соотношений в группе G. База индукции доказана ранее. Предположим, что для произведения $n-1$ группы соотношения выполняются. Далее умножим полученное сплетение на группу C_p и докажем справедливость соотношений для элементов из новообразовавшегося уровня L_n. Сопрягая образуюший из L_n, получаем все элементы из L_n. В новообразовавшейся таблице эти элементы порождают циклические подгруппы и образуют нормальную подгруппу H_n, которая является прямым произведением этих подгрупп. Действительно, $\forall x\in L_n$, $\forall g\in G$ имеем

$$g^{-1}x_i g=[[\ldots[a^{-j}ea^{j};e,\ldots,e]\ldots];h_1x_{n_{(g^{-1})}}h^{-1}_{1_{(g^{-1}x_n)}},\ldots]=$$
$$=[[\ldots[e;e,\ldots,e]\ldots];h_1x_{n_{(g^{-1})}}h^{-1}_{1_{(g^{-1}x_n)}},\ldots]\in H\Rightarrow H\lhd G.$$

Элементы $x_{n,n-1,l}^{-k}x_{n,n,m}x_{n,n-1,l}^{k}$, $k\in\{0,1,\ldots,p-1\}$, $1\le l\le p^{n-1}$, $x_{n,n,m}\in L_n$, $lp\le m\le$ $\le(l+1)p$, порождают подгруппы $\langle x_{n,n,l}\rangle\simeq C_p$ в $H_n\lhd G$, которые дают прямое разложение H_n-базы сплетения.

Действительно, $\langle x_{n,n,i}\rangle\cap\langle x_{n,n,j}\rangle=e$ при $i\neq j$, $\forall h\in H_n: h=\langle x_{n,n,1}\rangle\times\langle x_{n,n,2}\rangle\times\ldots$ $\ldots\times\langle x_{n,n,p^n}\rangle$ однозначно записывается в виде $h=x_{n,n,1}^{i_1}x_{n,n,2}^{i_2}\ldots x_{n,n,p^{n-1}}^{i_{p-1}}\Rightarrow$ подгруппа, $H_n=\langle x_{n,n,1},\dots,x_{n,n,p^{n-1}}\rangle$. Кроме того, $\forall x_{n,i}\in H_n$, $\forall g\in G$ имеем $g^{-1}x_{n,i}g=$ $=[[\dots[e;e,\dots,e]\dots];\dots,h_1 x_{n,i_{(g^{-1})}} h^{-1}_{1_{(g^{-1}x_{n,i})}},\dots]\in\langle x_i\rangle$, т.е. $\langle x_i\rangle\lhd H_n$. Более детально $H_n=\langle x_{n,n,1}\rangle\times\langle x_{n,n,2}\rangle\times\dots\times\langle x_{n,n,p^{n-1}}\rangle$ и $\langle x_{n,n,m}\rangle\rhd H_n$, поскольку $x^{-k}_{n,n-1,j}x_{n,n,m}\times$ $\times x^{k}_{n,n-1,j}=\langle x_{n,n,m}\rangle$, $k\in\{0,1,\dots,p-1\}$, $1\le j\le p^{n-1}$, $x_{n,n,m}\in L_n$.

Поэтому согласно второму определению внутреннего прямого произведения имеем $x_{n,n,i}x_{n,n,j}=x_{n,n,j}x_{n,n,i}$. Тогда в силу того, что образующий элемент $x_{n,k,1}$ действует только на первые p^{n-k} элементов из L_n и не действует на остальные его элементы, следует $x_{n,n,m}x_{n,k,1}=x_{n,k,1}x_{n,n,m}$ при $k\le n$, $p^{n-k}<m<p^n$. Третий индекс изменяется от 1 до n. Аналогично имеем $x_{n,n,1}x_{n,k,l}=x_{n,k,l}x_{n,n,1}$, поскольку $x_{n,k,l}$, $l\ne 1\,(\mathrm{mod}\,p)$, не действует на первые p^{n-l} элементов из L_n. Выполнение соотношения $x_i^p=e$ очевидно.

Пусть $F(t_0,t_1,\dots,t_n)$ — свободная группа. Введем расстояние между элементами F. Все элементы, которые сопряжены с t_i, имеют расстояние до t_0, равное i. Будем называть их элементами i-го ранга и обозначать $t_k^{-1}t_it_k\in R_i$, где t_0 — образующий ранга 0 (вершина дерева), t_i — образующий ранга i.

Определение 2. Индексной структурой элемента $u_{i_0i_1i_2\dots i_{m-1}}=t_0^{-i_0}t_1^{-i_1}\dots$ $\dots t_{m-1}^{-i_{m-1}}t_m t_{m-1}^{i_{m-1}}\dots t_1^{i_1}t_0^{i_0}$ называется вектор $\delta(u_{i_0,i_1\dots i_{m-1}})=(i_0,i_1,i_2\dots i_{m-1})$, состоящий из индексов, которые задаются степенями всех элементов $t_j^{i_j}\in L_j$, $j<n$, $j\in\mathbb{N}$, $i_j=\overline{0,p-1}$, сопрягающими t_m в $u_{i_0i_1i_2\dots i_{m-1}}$, например $u^s_{ijk0}=t_0^{-i}t_1^{-j}t_2^{-k}t_4^st_2^kt_1^jt_0^i$, $\delta(u_{0123})=(i,j,k,0)$, t_m назовем базовым элементом из $u_{i_0i_1i_2\dots i_{m-1}}$, обозначим $\delta_{01\dots r-1}(u_{i_0\dots i_{n-1}})=i_0\dots i_{r-1}$ первые r координат индекса сдвига для $u_{i_0i_1i_2\dots i_{n-1}}$. (Легко убедиться, что элементы $u_{i_0i_1i_2\dots i_{n-1}}$ составляют систему образующих.)

Теорема 1. Группа $G=(\dots((C_p\wr C_p)\wr C_p)\dots)\wr C_p$ — силовская p-подгруппа группы $S_{p^{n+1}}$ имеет копредставление

$$\left\langle t_j,\,j\in\{0,\dots,n\}\,\middle|\,t_j^p=e,\ [t_k^{-i}t_mt_k^i,t_l]=e,\ 1\le i\le p-1,\ n\ge l\ge m>k\ge 0\right\rangle.$$

Доказательство. Количество основных соотношений составляет $\sum\limits_{j=1}^{n}\frac{j(j+1)}{2}\times$ $\times(p-1)+(n+1)-\frac{n(n+1)}{2}\frac{p-1}{2}$, $n\ge m\ge l>k\ge 0$, из них $n+1$ — число циклических соотношений. Действительно, количество соотношений коммутации $[t_k^{-i}t_mt_k^i,t_l]=e$, $n\ge m\ge l>k\ge 0$, определяется как $\sum\limits_{l=0}^{n}\sum\limits_{m=0}^{l}\sum\limits_{k=0}^{m-1}1=\sum\limits_{l=0}^{n}\sum\limits_{m=0}^{l}m=\sum\limits_{l=0}^{n}\frac{l(l+1)}{2}=\sum\limits_{j=1}^{n}\frac{j(j+1)}{2}$, поскольку слагаемое $l=0$ можно не учитывать. Отметим, что $\frac{p-1}{2}$ — достаточное число степеней i, при которых соотношения $[t_k^{-i}t_lt_k^i,t_l]=e$ порождают все остальные соотношения вида

$$[t_0^{i_0}t_1^{i_1}\cdot\ldots\cdot t_k^{-i}\cdot\ldots\cdot t_{l-1}^{-i_{m-1}}t_lt_{l-1}^{i_{m-1}}\cdot\ldots\cdot t_k^{i}\cdot\ldots\cdot t_1^{i_1}t_0^{i_0},\,t_0^{-i_0}t_1^{-i_1}\cdot\ldots\cdot t_{k-1}^{-i_{k-1}}t_lt_{k-1}^{i_{k-1}}\cdot\ldots\cdot t_1^{i_1}t_1^{i_0}]=e,$$

$$[t_0^{-i_0}t_1^{-i_1}\cdot\ldots\cdot t_k^{-j_k}t_lt_k^{j_k}\cdot\ldots\cdot t_1^{i_1}t_0^{i_0},\,t_0^{-i_0}t_1^{-i_1}\cdot\ldots\cdot t_{k-1}^{-i_{k-1}}t_k^{-s_k}\cdot\ldots\cdot t_l\cdot\ldots\cdot t_k^{s_k}t_{k-1}^{i_{k-1}}\cdot\ldots\cdot t_1^{i_1}t_1^{i_0}]=e.$$

Действительно, при выведении соотношений с одинаковыми базовыми элементами имеем $t_k^{-p+1}\left| t_k^{-1} t_l t_k t_l = t_l t_k^{-1} t_l t_k \right| t_k^{p-1} \Rightarrow t_l t_k^{-p+1} t_l t_k^{p-1} = t_k^{-p+1} t_l t_k^{p-1} t_l$, поэтому достаточно $\dfrac{p-1}{2}$ значений i. При различных базовых элементах t_m, t_l в соотношении $t_k^{-1} t_l t_k t_m = t_m t_k^{-1} t_l t_k$ необходимо $p-1$ значений $i = \overline{0, p-1}$ для такого порождения. Поэтому учитываем, что для соотношений $t_k^{-i} t_l t_k^i t_l = t_l t_k^{-i} t_l t_k^i$ достаточно лишь $\dfrac{p-1}{2}$ значений степени i.

Пусть N — нормальное замыкание множества соотношений R в группе $F(t_0, t_1, \ldots, t_n)$. Значит, имеем эпиморфизм $F/N \to G$, заданный на образующих $t_i \mapsto x_{i+1}$ $(i = 0, \ldots, n)$. Поэтому $|F/N| \geq |G|$. Докажем, что такой эпиморфизм является изоморфизмом. Для этого в дальнейшем будет доказано неравенство

$$|F/N| \leq \left| (\ldots((C_p \wr C_p) \wr C_p) \ldots) \wr C_p \right| = p^{p^n + \ldots + p + 1}.$$

Определение 3. Элемент $u_{i_0 i_1 \ldots i_k}$ будем называть элементом k-го ранга, если он получен сопряжением элемента t_k образующими с индексами, меньшими k.

Определение 4. Индексной структурой элемента $t_m^{i_k}$, k — номер позиции t_m в $W = t_{j_0}^{i_0} t_{j_1}^{i_1} \ldots t_m^{i_k} \ldots t_{j_l}^{i_l}$, является вектор, состоящий из суммарных индексов сдвига, приведенных по модулю p, которые задаются предыдущими элементами, являющимися элементами меньших рангов и действующими на данный элемент $t_m^{i_k}$, т.е. $\delta_{01\ldots n-1}(t_m^{i_k}) = (s_0, s_1, \ldots, s_{m-1})$. Здесь s_l — сумма, взятая по модулю p, степеней всех элементов t_l, которые действуют на $t_m^{i_k}$, $l < m$. Обозначим $i_l(k) = \delta_l(t_m^{i_k})$ l-ю координату индекса сдвига элемента $t_m^{i_k}$ в слове W. Докажем, что из соотношений $t_j^p = e$, $[t_k^{-i} t_m t_k^i, t_l] = e$, $1 < i \leq p-1$, $n \geq m$, $l \geq k \geq 0$, $j \in Z_{n+1}$, выводятся остальные:

$$[t_{i_0}^{-s_0} t_{i_1}^{-s_1} t_{i_2}^{-s_2} \ldots t_{i_{n-1}}^{-s_{n-1}} t_m^{s_n} t_{i_{n-1}}^{s_{n-1}} \ldots t_{i_2}^{s_2} t_{i_1}^{s_1} t_{i_0}^{s_0}, t_{j_0}^{-z_0} t_{j_1}^{-z_1} \ldots t_l^h \ldots t_{j_1}^{z_1} t_{j_0}^{z_0}] = e, \qquad (2)$$

а также соотношения вида $v_{i_0 i_1 i_2 \ldots i_r}^{-s} u_{j_0 j_1 j_2 \ldots j_r \ldots j_{n-1}} = u_{j_0 j_1 j_2 \ldots j_{r+s} \ldots j_{n-1}} v_{i_0 i_1 i_2 \ldots i_r}^{-s}$.

Оставшиеся соотношения выводятся из следующих:

$$t_k^{-i_k} t_l^{-i_l} t_k^{i_k} \left| t_k^{-i_k} t_b t_k^{i_k} t_m \right| t_k^{-i_k} t_l^{i_l} t_k^{i_k} = t_k^{-i_k} t_l^{i_l} t_k^{i_k} \left| t_m t_k^{-i_k} t_b t_k^{i_k} \right| t_k^{-i_k} t_l^{i_l} t_k^{i_k}, \; k < l < b < m,$$

$$t_k^{-i_k} t_l^{-i_l} t_b t_l^{i_l} t_k^{i_k} t_m = t_m t_k^{-i_k} t_l^{-i_l} t_b t_l^{i_l} t_k^{i_k} \Rightarrow [t_k^{-i_k} t_l^{i_l} t_b t_l^{i_l} t_k^{i_k}, t_m] = e,$$

поскольку

$$t_k^{-i_k} t_l^{-i_l} t_k^{i_k} t_m = t_m t_k^{-i_k} t_l^{-i_l} t_k^{i_k},$$

$$t_l^{-i_l} \left| t_k^{-i} t_n t_k^i t_m \right| t_l^{i_l} = t_l^{-i_l} \left| t_m t_k^{-i} t_n t_k^i \right| t_l^{i_l}, \; k > l,$$

$$t_l^{-i_l} t_k^{-i} t_n t_k^i t_l^{i_l} t_l^{-i_l} t_m t_l^{i_l} = t_l^{-i_l} t_m t_l^{i_l} t_l^{-i_l} t_k^{-i} t_n t_k^i t_l^{i_l} \Rightarrow [t_l^{-i_l} t_k^{-i} t_n t_k^i t_l^{i_l}, t_l^{-i_l} t_m t_l^{i_l}] = e.$$

В случае $k < l$ получаем возможность независимого приращения l-й координаты $\delta_{01\ldots b-1}(u_b)$, поэтому можно наращивать степень каждой образующей, которая имеет индекс больше k.

Далее аналогичными преобразованиями получаем произвольное выражение вида (2). При этом существенным при выведении из соотношений $t_k^{-i} t_b t_k^i t_m = t_m t_k^{-i} t_b t_k^i$ является возможность лишь параллельного наращивания степеней элементов t_k^{i+j} и t_l, $l < k$.

Действительно,

$$t_k^{-j} \left| t_k^{-i} t_l t_k^i t_k^{-s} t_m t_k^s = t_k^{-s} t_m t_k^s t_k^{-i} t_l t_k^i \right| t_k^j \Rightarrow$$

$$\Rightarrow t_k^{-i-j} t_l t_k^{i+j} t_k^{-s-j} t_m t_k^{s+j} = t_k^{-s-j} t_m t_k^{s+j} t_k^{-i-j} t_l t_k^{i+j}.$$

Таким образом, степени сопрягающих элементов изменились на одинаковую величину. Поэтому имея соотношения с разными величинами $\min\{|s-i|,\ p-|s-i|\}$, можно вывести все соотношения. Отсюда $1 \le i \le \dfrac{p-1}{2}$, $s=0$.

Пусть на m-й итерации выведения имеем $u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_n} = u_{j_0 j_1 \ldots j_n} u_{i_0 i_1 i_2 \ldots i_n}$, т.е. индексы сдвигов различны. Тогда возможно независимое наращивание индекса сдвига в каждом из сомножителей $u_{i_0 i_1 i_2 \ldots i_n}$, $u_{j_0 j_1 \ldots j_n}$.

Лемма 3. В случае $\delta(u_{m+1}) = j_k j_{k+1} \ldots j_m$, $\delta(u_b) = i_l i_{l+1} \ldots i_b$ можно из соотношения $u_{i_l i_{l+1} i_{l+2} \ldots i_b} u_{j_k j_{k+1} \ldots j_m} = u_{j_k j_{k+1} \ldots j_m} u_{i_l i_{l+1} i_{l+2} \ldots i_b}$ вывести соотношения, имеющие элементы с произвольными индексными структурами, кроме индекса с наименьшим номером из индексных структур элементов данного соотношения, т.е. $\{j_k, j_{k+1}, \ldots, j_m;\ i_l, i_{l+1}, \ldots, i_b\}$, $k<l$, который наращивается параллельно. В данном случае i_k наращивается паралельно и элемент $t_k^{s_k}$, $s_k = 1, \ldots, p-1$, не уничтожается в этом соотношении. В частности, при $\delta(u_{j_0 \ldots j_n}) = j_0 j_1 \ldots j_k j_{k+1} \ldots j_n$, $\delta(v_{i_0 \ldots i_b}) = i_0 i_1 \ldots i_b$ из соотношения $u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} = u_{j_0 j_1 \ldots j_b} u_{i_0 i_1 i_2 \ldots i_n}$ можно вывести соотношения, имеющие элементы с произвольными индексными структурами, кроме индексов с наименьшим номером, т.е. i_0, j_0, которые наращиваются параллельно.

Сначала докажем лемму для частного случая. Преобразуем левую часть равенства $u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} = u_{j_0 j_1 \ldots j_b} u_{i_0 i_1 i_2 \ldots i_n}$, правая часть преобразуется аналогично:

$$t_0^{-i_0} t_1^{-i_1} \ldots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}} \ldots t_1^{i_1} t_0^{i_0} \,|\, u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} =$$
$$= u_{j_0 j_1 \ldots j_b} u_{i_0 i_1 i_2 \ldots i_n} \,|\, t_0^{-i_0} t_1^{-i_1} \ldots t_k^{m} \ldots t_1^{i_1} t_0^{i_0} \Rightarrow .$$

Рассмотрим изменение призведения $u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b}$:

$$(t_0^{-i_0} t_1^{-i_1} \ldots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}} \ldots t_1^{i_1} t_0^{i_0}) \cdot$$
$$\cdot\, t_0^{-i_0} t_1^{-i_1} \ldots t_k^{-i_k} \ldots t_n \ldots t_k^{i_k} \ldots t_1^{i_1} t_0^{i_0} \underbrace{(t_0^{-i_0} \ldots t_{k-1}^{i_{k-1}} t_k^{m} t_{k-1}^{i_{k-1}} \ldots t_0^{i_0} \cdot t_0^{-i_0} \ldots t_k^{-m} \ldots t_0^{i_0})}_{e} \times$$
$$\times\, t_0^{-j_0} t_1^{-j_1} \ldots t_b^{j_n} \ldots t_1^{j_1} t_0^{j_0} (t_0^{-i_0} t_1^{-i_1} \ldots t_k^{m} \ldots t_1^{i_1} t_0^{i_0}) =$$
$$= u_{i_0 \ldots i_{k-1}}^{-m} u_{i_0 i \ldots i_n} (u_{i_0 \ldots i_{k-1}}^{m} u_{i_0 \ldots i_{k-1}}^{-m}) u_{j_0 \ldots j_b} u_{i_0 \ldots i_{k-1}}^{m} =$$
$$= t_0^{-i_0} t_1^{-i_1} \ldots t_k^{-m} t_k^{-i_k} \ldots t_n \ldots t_k^{i_k} t_k^{m} \ldots t_1^{i_1} t_0^{i_0} \cdot t_0^{-j_0} t_1^{-j_1} \ldots t_b^{j_n} \ldots t_1^{j_1} t_0^{j_0} =$$
$$= u_{i_0 i_1 \ldots k+m \ldots n} u_{j_0 j_1 \ldots j_b} .$$

Здесь изменилась k-я координата индекса смещения элемента $u_{i_0 i_1 \ldots i_n}$ при сопряжении его элемента ранга k, который имеет соответствущий индекс сдвига $\delta(u_k) = i_0 i_1 \ldots i_{k-1}$, т.е. $u_{i_0 \ldots i_{k-1}}^{m}$.

Аналогичны преобразования для остальных n индексов, кроме наименьщего. Так, можно вывести соотношения с любыми индексами сдвига, кроме наименьшей координаты, которая наращивается параллельно.

Аналогично для равенства $u_{i_l i_{l+1} \ldots i_b} u_{j_k j_{k+1} \ldots j_m} = u_{j_k j_{k+1} \ldots j_m} u_{i_l i_{l+1} \ldots i_b}$ доказывается соотношение

$$t_k^{-m} \,|\, u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} = u_{j_0 j_1 \ldots j_b} u_{i_0 i_1 i_2 \ldots i_n} \,|\, t_k^{m} \Rightarrow$$
$$\Rightarrow t_k^{-i_k - m} t_{k+1}^{-i_{k+1}} \ldots t_n \ldots t_{k+1}^{i_{k+1}} t_k^{i_k + m} \cdot t_k^{-m} t_l^{-i_l} t_{l+1}^{-i_{l+1}} \ldots t_m \ldots t_{l+1}^{i_{l+1}} t_l^{i_l} t_k^{m} =$$
$$= t_k^{-m} t_l^{-i_l} t_{l+1}^{-i_{l+1}} \ldots t_m \ldots t_{l+1}^{i_{l+1}} t_l^{i_l} t_k^{m} \cdot t_k^{-i_k - m} t_{k+1}^{-i_{k+1}} \ldots t_n \ldots t_{k+1}^{i_{k+1}} t_k^{i_k + m} .$$

В результате получим $u_{s_k i_l i_{l+1} \ldots i_b} u_{j_k + s_k j_{k+1} \ldots j_m} = u_{j_k + s_k j_{k+1} \ldots j_m} u_{s_k i_l i_{l+1} \ldots i_b}$.

Лемма 4. При условии

$$\delta(u_{i_0\ldots i_{n-1}})=i_0 i_1\ldots i_{k-1} j_k j_{k+1}\ldots j_n,\ \delta(u_{i_0\ldots i_{b-1}})=i_0 i_1\ldots i_{k-1} i_k\ldots i_b$$

имеем возможность лишь параллельного наращивания для $1,\ldots,k$ индексов из $u_{i_0 i_1 i_2\ldots i_n} u_{j_0 j_{k+1}\ldots j_b} = u_{j_0 j_{k+1}\ldots j_b} u_{i_0 i_1 i_2\ldots i_n}$.

Докажем это для k-го индекса (для остальных $k-1$ индексов доказательство аналогично):

$$u_{i_0 i_1 i_2\ldots i_{k-1}\ldots i_n} u_{i_0 i_1\ldots i_{k-1} j_k\ldots j_b} = u_{i_0 i_1\ldots i_{k-1} j_k\ldots j_b} u_{i_0 i_1 i_2\ldots i_n} \Rightarrow$$

$$\Rightarrow u_{i_0 i_1\ldots i_k+m\ldots n} u_{i_0 i_1\ldots j_k+m\ldots j_b} = u_{i_0 i_1\ldots j_k+m\ldots n} u_{j_0 j_1\ldots i_k+m\ldots j_b}.$$

Для доказательства преобразуем левую часть равенства, в правой части преобразования аналогичны:

$$t_0^{-i_0} t_1^{-i_1}\ldots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}}\ldots t_1^{i_1} t_0^{i_0} \,|\, u_{i_0 i_1 i_2\ldots i_n} u_{i_0 i_1\ldots i_k\ldots j_b} =$$

$$= u_{i_0 i_1\ldots j_b} u_{i_0 i_1 i_2\ldots i_n} \,|\, t_0^{-i_0} t_1^{-i_1}\ldots t_k^{m}\ldots t_1^{i_1} t_0^{i_0} \Rightarrow$$

$$\Rightarrow (t_0^{-i_0} t_1^{-i_1}\ldots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}}\ldots t_1^{i_1} t_0^{i_0}) t_0^{-i_0} t_1^{-i_1}\ldots t_k^{-i_k}\ldots t_n\ldots t_k^{i_k}\ldots t_1^{i_1} t_0^{i_0}\cdot$$

$$\cdot (t_0^{-i_0}\ldots t_{k-1}^{i_{k-1}} t_k^{m} t_{k-1}^{i_{k-1}}\ldots t_0^{i_0}\cdot t_0^{-i_0}\ldots t_k^{-m}\ldots t_0^{i_0}) t_0^{-i_0} t_1^{-i_1}\ldots t_k^{-j_k} t_b^{j_n} t_k^{j_k}\ldots t_2^{i_1} t_0^{i_0}\cdot$$

$$\cdot (t_0^{-i_0} t_1^{-i_1}\ldots t_k^{m}\ldots t_1^{i_1} t_0^{i_0}) = u^{-m}_{i_0\ldots i_{k-1}} u_{i_0\ldots i_n} (u^{m}_{i_0\ldots i_{k-1}} u^{-m}_{i_0\ldots i_{k-1}}) u_{i_0\ldots j_b} u^{m}_{i_0\ldots i_{k-1}} =$$

$$= t_0^{-i_0} t_1^{-i_1}\ldots t_k^{-m} t_k^{-i_k}\ldots t_n\ldots t_k^{i_k} t_k^{m}\ldots t_1^{i_1} t_0^{i_0}\cdot t_0^{-j_0} t_1^{-j_1}\ldots t_k^{-m} t_k^{-j_k} t_b^{j_n}\ldots t_k^{m} t_k^{-j_k} t_2^{j_1} t_0^{j_0} =$$

$$= u_{i_0 i_1\ldots i_k+m\ldots n} u_{j_0 j_1\ldots j_k+m\ldots j_b}.$$

Здесь изменились k-е координаты индекса сдвига всех элементов при сопряжении их элементов ранга k, поскольку $t_k^{-i_k}$ имеет такой же индекс сдвига $\delta(u)= = i_0 i_1\ldots i_{k-1}$ и действует на все элементы большего ранга в $u_{i_0 i_1 i_2\ldots i_n} u_{i_0 i_1\ldots j_b}$. Отметим, что при $\delta_{12\ldots r-1}(u_r)=\delta_{12\ldots r-1}(v_n)$ для $u_{i_0 i_1\ldots i_{r-1}}\in L_r$ и $v_{i_0 i_1\ldots i_{n-1}}\in L_n$, $r<n$, имеем $v^{-s}_{i_0 i_1 i_2\ldots i_r} u_{i_0 i_1 i_2\ldots i_r\ldots j_{n-1}} = u_{i_0 i_1 i_2\ldots i_r+s, j_{r+1}\ldots j_{n-1}} v^{-s}_{i_0 i_1 i_2\ldots i_r}$.

Действительно, при таком совпадении индексов сдвига для элементов t_r из $v^{-s}_{i_0 i_1 i_2\ldots i_{r-1}}$ и $u_{i_0 i_1 i_2\ldots i_r\ldots j_{n-1}}$ элемент $v^{-s}_{i_0 i_1 i_2\ldots i_{r-1}}$ после перемещения до элемента $t_r\in \in u_{i_0 i_1 i_2\ldots i_r\ldots j_{n-1}}$ будет иметь индекс сдвига такой же, как и элемент $t_r^{i_r}$ из $u_{i_0 i_1 i_2\ldots i_r\ldots j_{n-1}}$, поэтому $v^{-s}_{i_0 i_1 i_2\ldots i_{r-1}}$ действует на все следующие элементы (т.е. на элементы, имеющие ранг R_m, $n\ge m>r$) левым сдвигом. Иными словами,

$$v^{-s}_{i_0 i_1 i_2\ldots i_{r-1}} u_{i_0 i_1 i_2\ldots i_r\ldots i_{n-1}} = t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_r^{-s}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0}\cdot$$

$$\cdot t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_r^{-s}\ldots t_2^{i_2} t_1^{i_1} t_1^{-i_1} e\cdot t_2^{-i_2}\ldots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_r^{-s-i_r} t_{r+1}^{-i_{r+1}}\ldots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0}\cdot e =$$

$$= t_0^{-i_0} t_1^{-i_1}\ldots t_r^{-s-i_r} t_{r+1}^{i_{r+1}}\ldots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}}\ldots t_{r+1}^{i_{r+1}} t_r^{s+i_r}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0}\cdot$$

$$\cdot t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_r^{s}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0} t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_r^{-s}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= t_0^{-i_0} t_1^{-i_1}\ldots t_r^{-s-i_r} t_{r+1}^{i_{r+1}}\ldots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}}\ldots t_{r+1}^{i_{r+1}} t_r^{s+i_r}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0}\cdot$$

$$\cdot t_0^{-i_0} t_1^{-i_1} t_2^{-i_2}\ldots t_r^{-s}\ldots t_2^{i_2} t_1^{i_1} t_0^{i_0} = u_{i_0 i_1 i_2\ldots i_r+s\ldots i_{n-1}} v^{-s}_{i_0 i_1 i_2\ldots i_{r-1}}.$$

Таким образом, это равенство выводится.

Определение 5. Каноническим словом W_c данного класса эквивалетных слов называется самое короткое слово, состоящее из элементов $u_{i_0 i_1 i_2 \ldots i_{m-1}} = t_0^{-i_0} t_1^{-i_1} \ldots$ $\ldots t_{m-1}^{-i_{m-1}} t_m t_{m-1}^{i_{m-1}} \ldots t_1^{i_1} t_0^{i_0}$, $m \le n$, $i_j = \overline{0, p-1}$, причем их произведение упорядочено по убыванию номеров рангов, т.е. в начале слова стоят элементы n-го ранга, затем $(n-1)$-го и так далее до элемента $u_{00\ldots 0}$ 0-го ранга. Между собой элементы каждого ранга упорядочены по возрастанию индекса сдвига.

Лемма 5. Покажем, что в каждом фактор-классе из группы F/N имеется представитель слова вида W_c.

Любой элемент группы F/N, т.е. слово любой длины, можно представить в виде произведения множителей $u_{i_0 i_1 i_2 \ldots i_{m-1}}$, используя указанные в теореме 1 соотношения, а также соотношения вида $v_{i_0, i_1 \ldots i_r}^{-s} u_{i_0, i_1 \ldots i_r \ldots j_{n-1}} = u_{i_0, i_1, i_2 \ldots i_r, j_{r+1}+s \ldots j_{n-1}} v_{i_0, i_1 \ldots i_r}^{-s}$ и следующий переписывающий процесс:

а) двигаясь по элементам слова, находим первый элемент, индекс сдвига которого меньше предыдущего;

б) найденный элемент группы сопрягаем всеми предшествующими и, взяв в скобки, выносим полученное произведение в начало слова, оставив дубликат всех элементов, кроме найденного, на прежнем месте;

в) начиная с места инверсии, повторяем процесс, но при этом спрягаем всеми предыдущими элементами, имеющими индекс, меньший, чем у элемента, который дал следующую инверсию порядка индексов. Таким образом, элементы из R_i могут сопрягаться только элементами t_0, $t_1, \ldots, t_{i-1}$:

$$W = t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{-i_3} t_k^{-i_4} t_n^{i_5} t_{i_5}^{-i_5} \ldots t_{i_l}^{i_h} = (t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{i_1} t_0^{i_0}) t_0^{-i_0} t_1^{-i_1} \cdot$$

$$\cdot t_1^{-i_3} t_k^{-i_k} t_1^{i_3} t_1^{i_1} t_0^{i_0} \ldots = (t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{i_1} t_0^{i_0})(t_0^{-i_0} t_1^{-i_1} t_1^{-i_3} t_k^{-i_k} t_1^{i_3} t_2^{i_2} t_1^{i_1} t_0^{i_0}) \ldots =$$

$$= (t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{i_1} t_0^{i_0})(t_0^{-i_0} t_1^{-i_1-i_3} t_k^{-i_k} t_1^{i_1+i_3} t_0^{i_0}) = (t_0^{-s_0} t_1^{-s_1} t_2^{-s_2} t_1^{s_1} t_0^{s_0}) \cdot$$

$$\cdot (t_0^{-s_0} t_1^{-s_3} t_k^{-s_k} t_1^{s_3} t_0^{s_0}) \ldots, \text{ где } s_3 = i_1 + i_3,\ s_1 = i_1,\ s_2 = i_2,\ s_k = i_k,\ s_0 = i_0.$$

Элемент $t_2^{-i_2}$ в третьих скобках пропущен, поскольку он действует левым сдвигом на базовый элемент $t_k^{-i_k}$, давший следующую инверсию порядка индексов, находясь слева от него в первых скобках, где $|s_i|$ принадлежит приведенной системе вычетов по модулю p. Далее, применяя соотношения, справедливые в данной группе, упорядочиваем

$$W = (t_{j_0}^{-s_{j0}} t_{j_1}^{-s_{j1}} t_{j_2}^{-s_{j2}} t_{j_3}^{-s_{j3}} t_{j_4}^{-s_4} t_n^{j_1} t_{j_4}^{s_{j4}} t_{j_3}^{s_{j3}} t_{j_2}^{s_{j2}} t_{j_1}^{s_{j1}} t_{j_0}^{s_{j0}}) \cdot \ldots$$

$$\ldots \cdot (t_{i_0}^{-s_{i0}} t_{i_1}^{-s_{i1}} t_{i_2}^{-s_{i2}} t_{i_3}^{-s_{i3}} t_{i_4}^{-s_{i4}} t_{i_5}^{-s_{i5}} t_{i_6}^{-s_{i6}} t_{i_7}^{-s_{i6}} t_n^{j_2} t_{i_7}^{s_{i7}} t_{i_6}^{s_{i6}} t_{i_5}^{s_{i5}} t_{i_4}^{s_{i4}} t_{i_3}^{s_{i3}} t_{i_2}^{s_{i2}} t_{i_1}^{s_{i1}} t_{i_0}^{s_{i0}}) \cdot \ldots$$

$$\ldots \cdot (t_{z_0}^{-s_{z0}} t_{z_1}^{-s_{z1}} \ldots t_{z_l}^{-s_{zl}} t_n^{s_b} t_{z_l}^{s_{zl}} \ldots t_{z_1}^{s_{z1}} t_{z_0}^{s_{z0}}) \cdot \ldots \cdot (t_1^{-s_w} t_2^{-s_e} t_1^{s_w}) t_n^{z_n} \cdot \ldots \cdot t_3^{z_3} t_2^{z_2} t_1^{z_1} t_0^{-z_0},$$

$$i_0 < j_0, \text{ если } i_0 = j_0, \text{ то } s_{j_0} < s_{i_0} \ldots$$

В скобках стоят элементы $u_{i_0 i_1 \ldots i_{k-1}}$, $0 \le k \le n$, у которых базовый элемент сопрягается серией элементов меньших рангов, расположенных перед ним, но вне скобок на данной итерации переписывающего процесса, применяемого к слову W. Теперь перепишем W в образующих $u_{i_0 i_1 \ldots i_n}$ и, используя соотношения и их следствия вида $u_{ijk}^s u_{i,j,k,k+1,\ldots,l} = u_{i,j,k,k+1+s,\ldots,l} u_{ijk}^s$, сводим к W_c. Для этого упорядочиваем элементы $u_{i_0 i_1 \ldots i_k}$ по убыванию рангов базовых элементов. При совпадении рангов упорядочиваем такие элементы в обратном лексико-графическом порядке индексов сдвига. При совпадении рангов и индексных структур базовых элементов перемножаем такие элементы, в результате чего степени их базовых элементов суммируются. Преобразовывая таким образом слово W, в конце его получим элемент $t_0^{k_0}$, где $k_0 = \deg\left(\prod t_0^{s_i}\right) \bmod p$.

Определение 6. Степенной структурой слова W называется n-мерный вектор из результирующих степеней элементов $t_0, \ldots, t_n$ со всеми наявными индексами сдвига в слове W. При этом результирующие степени упорядочены в обратном лексико-графическом порядке по $\delta_{01\ldots n-1}(t_m^{i_k}) = (s_0, \ldots, s_{m-1})$ всех $t_m^{i_k} \in W$.

Легко проверить, что слова с равными степенными структурами эквивалентны. Понятно, что элементы, являющиеся базовыми в $u_{i_0 i_1 \ldots i_n}$ из W_c, имели иные позиции в W, но их индексы сдвигов не изменились. Результирующие степени для элементов с остальными индексами сдвига также не изменились, поэтому не изменилась и степенная структура исходного слова. Действительно, j-я координата индекса сдвига для базового элемента в $u_{i_0 i_1 i_2 \ldots i_{n-1}}^{s_k}$ из W_c равна j-й координате индекса сдвига в W для элемента $t_n^{i_m} \in W$, т.е. координаты равны $i_j(m) = \delta_j(t_n^{i_m})$, где m — номера мест элементов $t_n^m : \delta(u_{i_0 \ldots i_{n-1}}^{s_k}) = (i_0, i_1, i_2 \ldots i_{n-1}) = \delta_{01\ldots n-1}(t_n^{i_m}) = (i_0, i_1, \ldots, i_{n-1})$, поскольку последовательность активных относительно $t_n^{i_m}$ (вместо n может быть $l \in \{0, \ldots, n\}$) элементов в слове W, которые стоят перед ним и действуют на него, совпадает с сопрягающей последовательностью для этого элемента в $u_{i_0 i_1 i_2 \ldots i_{n-1}}^{s_k}$ согласно построению переписывающего процесса. В результате получаем $W_c = u_{z_0 z_1 \ldots z_n}^{s_0} \cdot \ldots \cdot u_{i_0 i_1 i_2 \ldots i_{n-1}}^{s_k} \cdot u_{k_0 k_1 \ldots k-1}^{s_{k+1}} \ldots u_{l_0 \ldots l_{n-1}}^{s_l} \cdot \ldots \cdot u_{i_0}^{s_m} t_0^{z_0}$, где s_k — результирующий степень элементов с индексом сдвига, равным $\delta_{01\ldots n-1}(t_n^{i_m}) = (i_0, i_1, i_2 \ldots i_{n-1})$.

Отсюда следует, что $|F/N| \le p^{p^n + \ldots + p + 1}$, поскольку некоторые канонические слова теоретически могут оказаться равными. Однако все канонические слова различны. Убедимся в этом. Для элементов $n+1$-го ранга количество разных индексов сдвига $\delta(u_{i_0 i_1 \ldots i_n})$ равно p^n. Поэтому количество разных элементов $n+1$-го ранга равно p^{p^n}. Аналогично количество элементов n-го ранга составляет $p^{p^{n-1}}, \ldots$, 1-го ранга равно p^p, 0-го ранга равно p. Таким образом, общее их число составляет $p^{p^n + \ldots + p + 1}$.

Имеем также неравенство $|F/N| \ge p^{p^n + \ldots + p + 1}$, которое следует из эпиморфизма. Из рассмотренного выше неравенства с обратным знаком заключаем, что эти неравенства вырождаются в равенство $|F/N| = |(\ldots((C_p \wr C_p) \wr C_p)\ldots) \wr C_p| = p^{p^n + \ldots + p + 1}$, поэтому имеем изоморфизм. Следовательно, копредставление правильное.

Теорема 2. Описанная система имеет минимальное число образующих, а также минимальное число соотношений для данной системы образующих.

Доказательство представим тремя шагами.

Шаг 1. Легко убедиться, что k-кратное произведение регулярных циклических групп имеет минимум k образующих. Очевидно, если отбросить соотношение $t_i^p = e$, то получим группу бесконечного порядка. Далее используем индукцию по переменным, база которой t_1, t_2 в $C_p \wr C_p$.

Определение 7. Глубина сдвига образующей t_2 в соотношении вида $t_1^{-i} t_2 t_1^i t_1^{-j} t_2 t_1^j = t_1^{-j} t_2 t_1^j t_1^{-i} t_2 t_1^i$ называется $hzt_1(per) := \min\{|j-i|, p-|j-i|\}$, где per — левая часть соотношения. Так, для $t_1^{-p+2} t_2 t_1^{p-2} t_2 = t_2 t_1^{-p+2} t_2 t_1^{p-2}$ имеем $hzt_1(per) = 2$. Обозначим

$$r_1 = t_1^{-1} t_2 t_1 t_2 t_1^{-1} t_2^{-1} t_1 t_2^{-1} = e. \qquad (3)$$

Глубина сдвига для произвольного слова определена ниже.

Докажем, что всевозможные сопряжения соотношений не изменяют их величины $hzt_1(u_k u_0)$. Покажем это для $X=\{t_1^m, t_2^n\}$, как базы индукции, все другие слова выражаются через них, поэтому они тоже не изменят глубины сдвига $hzt_1(u_k u_0)=k$. Докажем это. Возьмем соотношение r_k и проанализируем, как изменяется его глубина сдвига $hzt_1(per)$ при сопряжении r_k элементом t_1^k:

$$r_k = t_1^{-k} t_2^j t_1^k t_2^z \cdot t_1^{-k} t_2^{-j} t_1^k t_2^{-z} = e,$$

$$\mathrm{hzt}_1(\mathrm{u_k u_0}) = \mathrm{k} = |\mathrm{k}-0|,\ \mathrm{m, z, j} \in \{0, 1, \ldots, \mathrm{p}-1\},\ \mathrm{k} < \frac{\mathrm{p}-1}{2},$$

$$t_1^{-m} \cdot (t_1^{-k} t_2^j t_1^k t_2^z t_1^{-k} t_2^{-j} t_1^k t_2^{-z}) \cdot t_1^m =$$

$$= t_1^{-k-m} t_2^j t_1^{k+m} t_1^{-m} t_2^z (t_1^m t_1^{-m}) t_1^{-k} t_2^{-j} t_1^k (t_1^m t_1^{-m}) t_2^{-z} t_1^m =$$

$$= t_1^{-k-m} t_2^j t_1^{k+m} t_1^{-m} t_2^z t_1^m \cdot t_1^{-k-m} t_2^{-j} t_1^{k+m} t_1^{-m} t_2^{-z} t_1^m =$$

$$= t_1^{-m} |r_k| t_1^m = e \Rightarrow t_1^{-k-m} t_2^j t_1^{k+m} \cdot t_1^{-m} t_2^z t_1^m = t_1^{-m} t_2^z t_1^m \cdot t_1^{-k-m} t_2^j t_1^{k+m},$$

$$hzt_1(u_m u_{k+m}) = k = |k+m-m|,\ k < \frac{p-1}{2}.$$

Очевидно, что величина $hzt_1(per)$ не изменилась. Легко проверить, что эта величина не изменится и при сопряжении элементом t_2^m , поскольку t_2^m не действует ни на один элемент. Покажем это:

$$t_2^{-m} \cdot (t_1^{-k} t_2^j t_1^k t_2^z) t_2^m = t_2^{-m} (t_2^z t_1^{-k} t_2^j t_1^k) \cdot t_2^m \Leftrightarrow t_2^{-m} t_1^{-k} t_2^j t_1^k t_2^m t_2^z t_2^m =$$

$$= t_2^{-m} t_2^z t_2^{-m} t_1^{-k} t_2^j t_1^k t_2^m \Leftrightarrow t_1^{-k} t_2^j t_{p-k+1}^{-m} t_1^k t_2^m t_2^z = t_2^z t_2^{-m} t_1^{-k} t_{k+2}^m t_2^j t_1^k =$$

$$= t_1^{-k} t_2^j t_1^k (t_2^{-m} t_2^m) t_2^z = t_2^z (t_2^{-m} t_2^m) t_1^{-k} t_2^j t_1^k \sim u_k^j u_0^z = u_0^z u_k^j.$$

Таким образом, сопряжение не изменяет значения $hzt_1(per)$, но наращивает индексы на одинаковую величину при сопряжении t_1^m и не изменяет величины $hzt_1(per)$ при сопряжении t_2^m. Отсюда ясно, что сопряжение любой комбинацией элементов $t_1^m t_2^n t_1^l t_2^k t_1^j t_2^i \ldots$ не изменит глубины сдвига $hzt_1(per)$, т.е. не даст нового соотношения.

Шаг 2. Проанализируем нормальное замыкание множества $R=\left\{r_2, r_3, \ldots, r_m, m=\dfrac{p-1}{2}\right\}$, где r_i — образующие нормального замыкания, которые являются соотношениями с глубиной смещения i.

Определение 8. Глубиной сдвига $hzt_1(w, t_2^{i_m}, t_2^{i_k})$ элементов $t_2^{i_m}, t_2^{i_k}$ для произвольного слова $w \in N(R)$ называется модуль разницы их индексов сдвигов $\delta_1(t_2^{i_m}) = i_1(m)$ и $\delta_1(t_2^{i_k}) = i_1(k)$, где $i_1(m)$ — сумма степеней всех элементов t_1, действующих на $t_2^{i_m}$. Обозначим $i_l = \delta_l(t_m)$ l-ю координату индекса смещения элемента t_2^m в слове W.

Лемма 6. Если вставка происходит непосредственно в слове $v = r_j = t_1^{-j} t_2 t_1^j t_2 t_1^{-j} t_2^{-1} t_1^j t_2$, где $hzt_1(per) = j$, то элементарные преобразования типа вставки и вычеркивания слов, равных e, а также преобразования типа

$$t_2 t_1^{-1} = t_1^{-1} t_1 t_2 t_1^{-1}, \qquad (4)$$

применяемые к элементам рассматриваемого подслова, не изменяют $hzt_1(r_j, t_2^{i_m}, t_2^{i_k})$, т.е. $hzt_1(per) = j = hzt_1(r'_j, t_2^{i_m}, t_2^{i_k})$, где r'_j — слово r_j после преобразования.

Доказательство. Вставка слов, равных *e*, не изменяет индексов сдвига $\delta_1(t_2^{i_m}) = i_1(m)$ и $\delta_1(t_2^{i_k}) = i_1(k)$. Рассмотрим изменение этих же индексов сдвига в результате применения (4). Очевидно, что это преобразование не изменит суммарных индексов сдвига, задаваемых суммами степеней предшествующих элементов t_1.

Определение 9. Для произвольного слова $w \in N(R)$ определим величину $lz(t_1, k, t_2, v, w) = \sum_{i=0}^{l+k} \deg(t_1^{s_i})$, l — число элементов t_1 до подслова v, перед которым произошло непосредственно элементарное преобразование либо преобразование типа (4) в слове *w*, *k*, $k = \overline{0, n}$, — номер элемента t_2 в подслове v.

Свойство. После вставки, вычеркивании слов, равных *e*, а также после преобразований (4) слово w_0 изменяется на эквивалентное w_1, место элемента t_2 изменяется с k_0 на k_1, однако при этом $lz(t_1, k_0, t_2, v, w_0) = lz(t_1, k_1, t_2, v, w_1)$.

Замечание. Понятно, что при выведении соотношения с глубиной сдвига $hzt_1(per) = 1$ из соотношений с $hzt_1(per) \neq 1$ должна измениться величина $lz(t_1, k, t_2, v, w)$ для тех элементов t_2, которые сопрягаются элементами t_1. Таким образом, необходимым условием выводимости соотношений есть наличие изменений в слове $v = r_j$ имеющейся величины $lz(t_1, k, t_2, v, w)$ на $-i$ и $-j$: $\min\{|j-i|, p-|j-i|\} = 1$.

Доказательство. Применим преобразование (4), которое является элементарным преобразованием, а не соотношением и не изменяет значения $lz(t_1, k, t_2, v, w)$ для всех t_2 и все преобразования такого типа. Поэтому достичь с помощью таких преобразований изменения $hzt_1(per)$ с любого *i* на единицу невозможно. Остается выполнить элементарное преобразование — вставку и вычеркивание слова *e*.

1. Для вставки последовательностей, где всюду стоят $t_1^{-i} t_1^i, t_2 t_2^{-1}, \ldots$, можно применять преобразования типа (4) и элементарные преобразования. Соотношения здесь не применимы. В результате получим подслова вида $t_1^i t_1^{-i} t_2 t_2^{-1} \cdot e = t_1^i t_1^{-i} t_2 \cdot t_1^i t_1^{-i} t_2^{-1} (t_1^i t_1^{-i}) = t_1^i (t_1^{-i} t_2 t_1^i t_1^{-i} t_2^{-1} t_1^i) t_1^{-i} = t_1^i (t_1^{-i} t_2 t_1^i t_1^{-i} t_2^{-1} t_1^i \cdot (t_2^{-1} t_2)) t_1^{-i}$. Однако, как сказано выше, из слов в скобках не выводится требуемое соотношение, поскольку нет соотношений, чтобы переставить t_2 на нужное место с целью получения (3). Другими словами, сделанные преобразования не изменили $lz(t_1, k, t_2, v, w)$ для всех k.

2. Вставка единичных слов одно в одно: $uv = ut_1^i t_1^{-i} v = ut_1^{-i} t_2 t_2^{-1} t_1^i v = ut_1^{-i} t_2 t_1^i \cdot t_1^{-i} t_2^{-1} t_1^i v$ дает подслово, полученное в п. 1.

Проанализируем, что дает применение тех перестановок, которые определяются соотношениями из R. Попытаемся вывести нужное соотношение (3) с $hzt_1(per) = 1$ путем умножением r_j на $r_k^{\pm 1}$: $j - k = 1$, $j, k \in \mathbb{N}$.

Пусть исключены $r_1 = t_1^{-1} t_2 t_1 t_2 \cdot t_1^{-1} t_2^{-1} t_1 t_2^{-1}$, а также все соотношения с $hzt_1(per) = 1$: $r_1 = t_1^{-k} t_2 t_1^k t_1^{-k-1} t_2 t_1^{k+1} \cdot t_1^{-k} t_2^{-1} t_1^k t_1^{-k-1} t_2^{-1} t_1^{k+1} = u_k u_{k+1} u_k^{-1} u_{k+1}^{-1}$. Отметим, что инвариантом для r_1 является чередование индексов смещения, разность которых равна единице. Кроме того, сумма всех степеней элементов t_1, t_2 для всех r_k равна нулю.

Докажем, что выражение с глубиной сдвига $hzt_1(per) = 1$ нельзя получить, перемножая $r_3^{\pm 1}$ и $r_2^{\pm 1}$. Аналогично рассуждаем для других k_i, у которых $|k_1 - k_2| = 1$, $r_2 r_3 = t_1^{-2} t_2 t_1^2 t_2 \cdot t_1^{-2} t_2^{-1} t_1^2 t_2^{-1} \cdot t_1^{-3} t_2 t_1^3 t_2 \cdot t_1^{-3} t_2^{-1} t_1^3 t_2^{-1}$.

Прокоммутировав выделенные сомножители, можно сократить элементы $t_2^{\pm 1}$ (которые отвечают элементам $u_0^{\pm 1}$ и отсутствуют в (3)). Можно также прокоммутировать сомножители $t_1^{-3} t_2 t_1^3 t_1^{-3} t_2^{-1} t_1^3 = t_1^{-3} t_2^{-1} t_1^3 t_1^{-3} t_2 t_1^3$ и получить

$$t_1^{-2} t_2 t_1^2 [t_1^{-2} t_2^{-1} t_1^2 \cdot t_1^{-3} t_2 t_1^3] t_1^{-3} t_2^{-1} t_1^3 \neq r_1.$$

Однако получить выражение вида (3), пользуясь соотношениями из R, невозможно, поскольку перестановка между u_k^i и u_m^j, где $|k-m|=1$, $|i,j| \leq p-1$, в этих преобразованиях отсутствует. Поэтому выражение, где рядом стоят u_2 и u_3, а далее u_2^{-1}и u_3^{-1}, получить нельзя. Если же сократить элементы t_1^i, $i \in \{\pm 2, \pm 3\}$, которые стоят рядом, то получим $t_1^{-2} t_2 t_1^2 t_1^{-2} t_2^{-1} t_1^2 \cdot t_1^{-3} t_2 t_1^3 t_1^{-3} t_2^{-1} t_1^3 = t_1^{-2} \cdot t_2 t_2^{-1} \cdot t_1^{-1} \cdot$ $\cdot t_2 t_2^{-1} \cdot t_1^3 = t_1^{-3} t_1^3$, где отсутствует t_2. При частичном сокращении этих элементов получим $t_1^{-2} t_2 t_1^2 t_1^{-2} t_2^{-1} t_1^2 \cdot t_1^{-3} t_2 t_1^3 t_1^{-3} t_2^{-1} t_1^3 = t_1^{-2} t_2 t_1 t_1^{-1} t_2^{-1} \cdot t_1^{-1} t_2 t_1 t_1^{-1} t_2^{-1} t_1^3$, где в правой части равенства не будет чередования индексов сдвига $\delta_1(t_2^{i_m})$, как в r_1. Поэтому выражения вида (2) получить невозможно. Значит, для его образования необходимо использовать отброшенное соотношение с $hzt_1(per)=1$.

Понятно, что в результате умножения $r_k \cdot r_m : |k-m| \neq 1$ выражение типа (1) получить нельзя, поскольку

$$t_1^{-2} t_2 t_1^2 t_1^{-2} t_2^{-1} t_1^2 \cdot t_1^{-5} t_2 t_1^5 t_1^{-5} t_2^{-1} t_1^5 = t_1^{-2} t_2 t_1^2 t_1^{-5} t_2 t_1^5 t_1^{-2} t_2^{-1} t_1^2 t_1^{-5} t_2^{-1} t_1^5 =$$

$$= t_1^{-2} \cdot \underbrace{t_2 t_1^{-3} t_2 t_1^3 \cdot t_2^{-1} t_1^{-3} t_2^{-1} t_1^3}_{r_3} \cdot t_1^2, \ hz(per)=3.$$

Таким образом, имеем только $lz(t_1, k, t_2, v, w) \in \{-2, -5\}$, однако данными преобразованиями не выводится слово с $lz(t_1, k, t_2, v, w) = -1$. Аналогичные рассуждения для степеней $\forall i, j : |i-j| \neq 1$.

Шаг 3. Воспользовавшись методом математической индукции, предположим, что для t_{n-1} не будет выводимости. Докажем это для t_n. Возьмем произвольное

$$r_{m,n}^{k,1} = t_k^{-1} t_m t_k t_n \cdot t_k^{-1} t_m^{-1} t_k t_n^{-1} = 1, \ k > m > n, \tag{5}$$

и покажем, что это соотношение невыводимо в $N(\{t_i^p = e, r_{1,2}^{0,h}, r_{1,3}^{0,h}, \ldots, r_{l,m}^{k,h}, \ldots$ $\ldots, r_{n-1,n}^{n-2,h}\} \setminus r_{n,m}^{k,1})$, $1 \leq h \leq \dfrac{p-1}{2}$. Соотношение (5) имеет глубину сдвига по образующему $t_k : hzt_k(per)=1$. Как показано ранее, путем сопряжения элементами t_k^{-i} выражений вида $r_{m,n}^{k,r} = t_k^{-r} t_n t_k^r t_m \cdot t_k^{-r} t_n^{-1} t_k^r t_m^{-1} = e$ изменить глубину сдвига $hzt_k(per)=r$ не удается. Другие образующие не изменят этой глубины сдвига, поскольку не изменяют степень сопрягающих элементов t_k. Все рассуждения об элементарных преобразованиях, как это показано ранее, не изменяют величины $lz(t_k, k, t_n, v, w)$, поэтому (5) не выводится.

Вместе со словом (5) из нормального замыкания исключаем все слова вида $X^{-1} r_{m,n}^{k,1} X$, $X \in F$, как непосредственные следствия $r_{m,n}^{k,1}$. Поэтому нельзя использовать коммутации без доказательства. Аналогично рассуждаем для других образующих N и элементов, с ними сопряженными. Слова вида

$$(t_k^{-1} Z^{-1} t_m Z t_k) t_n (t_k^{-1} Z^{-1} t_m^{-1} Z t_k) t_n^{-1} = e, \tag{6}$$

где все элементы с Z упорядочены и имеют индексы, большие, чем k, есть непосредственным следствием из соотношения (5) (как показано в теореме 1), поэтому слова вида (6) не применяются без доказательства их выводимости.

В произведении вида

$$Y^{-1}t_nY\cdot X^{-1}t_k^{-1}Z^{-1}t_mZt_kX\cdot Y^{-1}t_n^{-1}YX^{-1}t_k^{-1}Z^{-1}t_m^{-1}Zt_kX\cdot$$

$$\cdot W^{-1}t_nW\cdot V^{-1}t_k^{-1}H^{-1}t_mHt_kH\cdot W^{-1}t_n^{-1}WV^{-1}t_k^{-1}H^{-1}t_m^{-1}Ht_kV \qquad (7)$$

подслова X, V являются последовательностями $t_0^{i_0}t_1^{i_1}\dots t_{k-1}^{i_{k-1}}$, где $\exists\, i_s\neq 0$ и $X\neq V$. Поэтому t_m, t_n имеют разные сопрягающие слова X,Y, W,H, которые не сокращаются, а при сопряжении произведения (7) различными словами (см. лемму 3) невозможно одновременно сократить элементы с наименьшими индексами сдвига, которые являются разными по построению. Поэтому подслово $r_{m,n}^{k,1}$ не может образоваться, поскольку имеются лишние элементы. Следовательно, из произведения $Y^{-1}t_nY\cdot t_k^{-1}X^{-1}t_mXt_k\cdot Y^{-1}t_n^{-1}Yt_k^{-1}X^{-1}t_m^{-1}Xt_k\cdot W^{-1}t_nW\cdot t_k^{-1}H^{-1}t_mHt_k\cdot$ $\cdot W^{-1}t_n^{-1}Wt_k^{-1}H^{-1}t_m^{-1}Ht_k$ не выводится (5). Если перемножать слова $r_{m,n}^{k,i}$ и $r_{m,n}^{k,j}$, где $\min\{|j-i|,\, p-|j-i|\}=l$, а $r_{m,n}^{k,1}$ исключено, то получим $hz(per)$ вида $\big||i-j|+l-1\big|=1$ или $p-\big||i-j|+l-1\big|=1$: $t_k^{-i}t_nt_k^it_k^{-j}t_mt_k^j\cdot t_k^{-i}t_n^{-1}t_k^it_k^{-j}t_m^{-1}t_k^j\cdot$ $\cdot t_k^{-i+l-1}t_nt_k^{i-l+1}t_k^{-j+l-1}t_mt_k^{j-l+1}\cdot t_k^{-i+l-1}t_n^{-1}t_k^{i-l+1}t_k^{-j+l-1}t_m^{-1}t_k^{j-l+1}$, где $[t_k^{-i}t_n^{-1}t_k^i,$ $t_k^{-j-l+1}t_mt_k^{j+l-1}]\neq e$, поскольку $\big||i-j|+l-1\big|=1$. Например, в произведении $t_k^{-2}t_n\,t_k^2\,t_k^{-4}t_m\,t_k^4t_k^{-2}t_n^{-1}t_k^2\,t_k^{-4}t_m^{-1}\,t_k^4\,\cdot t_k^{-1}t_n\,t_k\,t_k^{-3}t_m\,t_k^3\,t_k^{-1}t_n^{-1}t_kt_k^{-3}t_m^{-1}t_k^3$ подслово $t_k^{-3}t_mt_k^3$ можно переставить лишь до подслова $t_k^{-4}t_m^{-1}t_k^4$, поскольку эти два подслова не коммутируют. Иначе использовалось бы подслово $r_{m,m}^{k,1}=e$, как частный случай того слова, которое мы исключили.

Если перемножать $r_{m,n}^{k,i}$ и $r_{m,n}^{k,j}$, где $\min\{|j-i|,\, p-|j-i|\}=1$, то получим ситуацию, изложенную в шаге 2.

Рассматривать произведение $r_{m,r}^{k,i}\cdot r_{m,l}^{k,j}$, $r\neq n$, где хоть один ранг базового элемента из этого произведения не совпадает с рангами базових элементов из (5), нецелесообразно, поскольку в них отсутствуют необходимые элементы, которые не образуются путем сопряжения и элементарных преобразований.

Следствие. Копредставление силовской подгруппы P группы S_n имеет вид

$$P\simeq\left\langle \begin{matrix} t_{lkz}\,|\,t_{lkz}^p=e,\,[t_{lkz}^{-i}t_{jkz}t_{lkz}^i,t_{bkz}]=e,\ t_{lkz}t_{jks}=t_{jks}t_{lkz},\,1\le z,s\le\alpha_k, \\ 0\le l<j\le b<k,\ t_{lkz}t_{jvs}=t_{jvs}t_{lkz},\,1\le z\le\alpha_k,\,1\le s\le\alpha_v,\,1\le k,v\le m \end{matrix}\right\rangle,$$

где t_{ikz} — i-й образующий подгруппы P_{z_k}, сопряженной с P_k; T_k — система образующих подгруппы P_k, $1\le k\le m$, $P_k\cong \wr_{i=1} C_p$, $1\le k\le m$.

Доказательство следует из теоремы 1 и структуры силовской подгруппы симметрической группы. При этом существует такое p-разбиение множества X на подмножества X_i, где действует P подстановками на различные подмножества таким образом, что порождающие элементы силовских подгрупп P_l, действующие на X_i, не могут быть редуцированы при построении прямого произведения $P=P_1^{a_1}\times P_2^{a_2}\times\ldots\times P_m^{a_m}$, поскольку они нецикличны. Однако если использовать для сопряжения элементы $g\notin P$, $g\in S_n$, то порождающие подгрупп, сопряженных к P_k, можно редуцировать, т.е. третий индекс можно не использовать.

Замечание. Доказывать минимальность соотношений по их количеству можно, построив действие группы на корневом дереве. Очевидно, если отбросить соотношение $t_i^p=e$, то получим группу бесконечного порядка.

Докажем, что система соотношений из теоремы минимальна. Пусть $[t_{i-1}^{-1}t_it_{i-1},t_{i+1}]=e$ выводимо. Тогда рассмотрим действие на вершинах корневого дерева группы с исходными соотношениями, но не имеющей соотношения указанного вида, в котором положим $i = n$. Взятое корневое дерево является сферически-однородным типа $T(p, p, \ldots, p, \infty)$ с $n+1$ уровнями:

уровень L_1 содержит вершину $y_{1,1,1}$;

L_2 содержим p вершин $y_{2,1,1}\, y_{2,1,2} \cdots y_{2,1,p}$;

L_3 содержит p^2 вершин $y_{3,1,1}\; y_{3,1,2} \cdots y_{3,1,p};\; y_{3,2,p+1} \cdots y_{3,2,2p}; \ldots;$ $y_{3,p,p^2-p} \cdots y_{3,p,p^2}$,

где первый индекс — номер уровня, второй — номер вершины из предыдущего уровня, с которой соединена данная вершина, третий индекс — номер данной вершины на текущем уровне (на последнем уровне при изменении второго индекса происходит изменение третьего с ∞ до 1);

L_4 содержит вершины $y_{4,1,1}\; y_{4,1,2} \cdots y_{4,1p}; \ldots; y_{4,p^2,p^3-p+1} \cdots y_{4,p^2,p^3}$;

…

L_n содержит вершины $y_{n,1,1}\; y_{n,1,2} \cdots y_{n,1,p}; \ldots; y_{n,p^{n-2},p^{n-1}-p+1} \cdots y_{n,p^{n-2},p^{n-1}}$;

L_{n+1} содержит вершины $y_{n+1,1,1}\; y_{n+1,1,2} \cdots y_{n+1,1,\infty};\; y_{n+1,2,1}\; y_{n+1,2,2} \cdots$ $\cdots y_{n+1,2,\infty}; \ldots; y_{n+1,p^{n-1},1} \cdots y_{n+1,p^{n-1},\infty}$.

Зададим действие (которое не будет свободным) такой группы на этом дереве: $t_i^s \cdot y_{i+1,k,j} = y_{i+1,k,j+(s) \bmod p}$, $1 \le s < p$, $1 \le j \le p^{i+1}$, при $i \le n-1$. На других сегментах i-го уровня действие аналогично. Если $i \le j$, то $t_i \cdot y_{j,l,1} = y_{j,l,1}$, т.е. t_i действует тривиально: $t_{i-m}^s \cdot y_{i+1,k,j} = y_{i+1,k,j+(sp^{i-m}) \bmod p^{i-m+1}}$, $1 \le s < p$, $1 \le j \le p^{i+1}$, при $i-m < n-1$.

Легко проверить, что ассоциативность выполняется: $t_l \cdot (t_i\, y_{l,j}) = (t_l t_i) \cdot y_{l,j}$.

При $i < n$ имеем $t_k^{-s} t_j t_k^s t_{i-1} \cdot y_{i,1,1} = y_{i,1,1+p^{i-j}+1} = t_{i-1} t_k^{-s} t_j t_k^s \cdot y_{i,1,1}$, $j \le i-1$, поскольку в левой части равенства сначала действует элемент $t_k^{-s} t_j t_k^s$ сдвигом на p^{i-j}, а затем t_{i-1} действует сдвигом на одну позицию. В правой части равенства действие происходит также, но в другом порядке. Строго говоря, такое действие представляет соответствие между элементами группы и подстановками вершин, которое задает гомоморфный образ (представление) группы:

$$\widehat{t_i\,(i+1)} \mapsto \begin{pmatrix} 1, & 2, & 3, & \ldots, & p^i \\ 2, & 3, & 4, & \ldots, & 1 \end{pmatrix}, \quad i < n,$$

где $1, 2, 3, \ldots, p^{i+1}$ — номера вершин с $i+1$-го уровня, $\widehat{t_i\,(i+1)}$ означает действие элемента t_i на L_{i+1},

$$\widehat{t_i\,(j)} \mapsto \begin{pmatrix} 1, & 2, & 3, & \ldots, & p^{j-1} \\ 1+p^{j-i-1}, & 2+p^{j-i-1}, & 3+p^{j-i-1}, & \ldots, & p^{j-i-1} \end{pmatrix}, \quad i < n, \; 1 < i < j \le n.$$

Легко проверить, что при $i < n$ выполняются соотношения

$$\widehat{t_i t_{i-1}\,(i+1)} \mapsto \begin{pmatrix} 1, & 2, & 3, & \ldots, & p^{i+1} \\ p+2, & p+3, & p+4, & \ldots, & p+1 \end{pmatrix}; \quad \widehat{t_{i-1} t_i t_{i-1}^{-1}\,(i+1)} \mapsto \begin{pmatrix} 1, & 2, & 3, & \ldots, & p^i \\ 2, & 3, & 4, & \ldots, & 1 \end{pmatrix};$$

при $i < n$ имеем

$$\widehat{t_{i-1} t_i t_{i-1}^{-1} t_i\,(i+1)} = \widehat{t_i t_{i-1} t_i t_{i-1}^{-1}\,(i+1)} \mapsto \begin{pmatrix} 1, & 2, & 3, & \ldots, & p^i \\ 3, & 4, & 5, & \ldots, & 2 \end{pmatrix};$$

при $i+1 < n$ имеем

$$\widehat{t_{i-1} t_i t_{i-1}^{-1} t_{i+1}\,(i+2)} = \begin{pmatrix} 1, & 2, & 3, & \ldots, & p^{i+1} \\ p+2, & p+3, & p+4, & \ldots, & p+1 \end{pmatrix} = \widehat{t_{i+1} t_{i-1} t_i t_{i-1}^{-1}\,(i+2)}.$$

Поэтому все соотношения выполняются при действии на всех уровнях, кроме последнего, где не выполняется исключаемое соотношение $[t_{n-1}^{-1} t_n t_{n-1}, t_n] = e$. Таким образом, данное действие — это гомоморфизм, заданный на образующих.

При $i = n$: $i, s \in \mathbb{N}$, элемент t_n действует на уровнях $L_1, \ldots, L_n$ тривиально, а на уровне L_{n+1}, который условно разделен на блоки α и β, он действует поблоково:

$$\widehat{t_n (n+1)} \cdot \alpha = \begin{pmatrix} 1 + j(n), & 2 + j(n), & 3 + j(n), & \ldots, & p + j(n) \\ 2 + j(n), & 3 + j(n), & 4 + j(n), & \ldots, & 1 + j(n) \end{pmatrix};$$

$$\widehat{t_n (n+1)} \cdot \beta = \begin{pmatrix} 1 + i(n), & 2 + i(n), & 3 + i(n), & 4 + i(n), & \ldots, & p + i(n), & p + 1 + i(n), & \ldots, & 2p \\ 1 + i(n), & 4 + i(n), & 3 + i(n), & 6 + i(n), & \ldots, & p + i(n), & p + 3 + i(n), & \ldots, & 2 \end{pmatrix}.$$

Здесь β — блок длины $2p$, причем подстановка, задаваемая таким действием, не распадается в произведение циклов, порядки которых не являются нетривиальными делителями p (это элементы порядков p и 1), поэтому построенное действие есть действием элемента порядка p.

Далее задаем действие элемента t_n на элементах с L_{n+1} поблоково так, чтобы блоки α и β образовывали апериодическую последовательность и таким образом формировали бесконечное слово. Теперь проанализируем действие слов $t_{n-1} t_n t_{n-1}^{-1} t_n$ и $t_n t_{n-1} t_n t_{n-1}^{-1}$ на α и β:

$$\widehat{t_{n-1} t_n t_{n-1}^{-1} t_n} (1)_{\alpha\beta} = 2, \ \widehat{t_{n-1} t_n t_{n-1}^{-1} t_n} (2)_{\alpha\beta} = 5, \ \widehat{t_{n-1} t_n t_{n-1}^{-1} t_n} (3)_{\alpha\beta} = 4 \ \ldots,$$

$$\widehat{t_n t_{n-1} t_n t_{n-1}^{-1}} (1)_{\alpha\beta} = 4, \ \widehat{t_n t_{n-1} t_n t_{n-1}^{-1}} (2)_{\alpha\beta} = 3, \ \widehat{t_n t_{n-1} t_n t_{n-1}^{-1}} (3)_{\alpha\beta} = 6 \ \ldots$$

Такое действие свидетельствует о некоммутации $[t_{n-1} t_n t_{n-1}^{-1}, t_n] \neq e$, и при действии $(t_{n-1} t_n t_{n-1}^{-1} t_n)^m$ точки залипания отсутствуют, так как в этом случае для каждого блока нет неподвижных точек.

Таким образом, получена бесконечная орбита. Поскольку это гомоморфный образ элементов группы, то действующая группа оказалась бесконечной. Следовательно, соотношения вида $[t_{n-1}^{i} t_n t_{n-1}^{-i}, t_n] = e$ невыводимы.

Итак, исследовано представление таких подгрупп в виде порождающих соотношений, число которых подсчитано, и (что чрезвычайно важно) доказана минимальность копредставления по числу соотношений и порождающих. Указаны важные свойства силовских p-подгрупп групп S_{p^k} и S_n.

СПИСОК ЛИТЕРАТУРЫ

1. Заровный В. П. Автоматные подстановки и сплетения групп // Докл. АН СССР. — 1965. — № 3. — С. 562–565.

2. Сущанський В. І., Сікора В. С. Операції на групах підстановок. — Чернівці: Рута, 2003. — 256 с.

3. Холл М. Теория групп. — М.: Изд-во иностр. лит., 1962. — 468 с.

Поступила 23.06.2008