

Об одном способе поиска больших подгрупп в группах симметрий графов

А. Ю. Овчаренко

В работе находятся определяющие соотношения для хорошо известных систем образующих групп всех подстановок конечных множеств. Это дает возможность в некоторых случаях найти без особых вычислительных сложностей большие подгруппы симметрий для графов с большим числом вершин. Приводится пример применения полученных результатов к нахождению группы симметрий некоторого графа степени 10.

Ключевые слова: симметрическая группа, порождающие, определяющие соотношения, подстановка.

1. Введение

Группы подстановок являются одним из основных средств комбинаторных объектов с большим числом симметрий, и их всестороннее изучение является задачей, имеющей важные приложения в комбинаторике и ее прикладных аспектах (теории кодирования, криптографии, проектировании электронной техники и т.д.).

В работе находятся определяющие соотношения для хорошо известных систем образующих групп всех подстановок конечных множеств. Это дает возможность в некоторых случаях найти без особых вычислительных сложностей большие подгруппы симметрий для графов с большим числом вершин. Приводится пример применения полученных результатов к нахождению группы симметрий некоторого графа степени 10. Все необходимые понятия и определения можно найти в [1].

2. Порождающие элементы симметрических групп

Лемма 1.

1. Пусть S_n – симметрическая группа подстановок степени n . Любая подстановка $\pi \in S_n$ представляется в виде произведения независимых циклов.

2. Любая подстановка $\pi \in S_n$ представляется в виде произведения транспозиций (циклов длины 2).

3. Пусть $a_1 = (12), a_2 = (13), \dots, a_{n-1} = (1n)$. Тогда $S_n = \langle a_1, \dots, a_{n-1} \rangle$.

Доказательство.

Утверждения 1–2 общеизвестны.

3. Поскольку S_n порождается транспозициями, утверждение сразу следует из следующего равенства: $(i, j) = (1, i)(1, j)(1, i)$.

Лемма 2. Пусть $b_1 = (12), b_2 = (23), \dots, b_{n-1} = (n-1, n)$. Тогда $S_n = \langle b_1, \dots, b_{n-1} \rangle$.

Доказательство. В силу леммы 1 $S_n = \langle a_1, \dots, a_{n-1} \rangle$, где $a_1 = (12), a_2 = (13), \dots, a_{n-1} = (1n)$, т.е. любая подстановка из S_n представляется в виде произведения элементов a_i . Поэтому нам достаточно найти выражение для произвольного a_i в виде произведения b_i . Имеем $a_1 = b_1$,
 $a_i = (1, i+1) = (i, i+1)(1, i)(i, i+1) = b_i(1, i)b_i = b_i b_{i-1}(1, i-1)b_{i-1}b_i = \dots = b_i b_{i-1} \dots b_2 b_1 b_2 \dots b_{i-1} b_i$,
 где $i = 2, \dots, n-1$. Лемма доказана.

Лемма 3. Пусть $c_1 = (12 \dots n), c_2 = (12)$. Тогда $S_n = \langle c_1, c_2 \rangle$.

Доказательство. Поскольку $S_n = \langle a_1, \dots, a_{n-1} \rangle$ (см. лемму 1), то нам достаточно найти выражения для произвольного a_i в виде произведения c_1 и c_2 . Легко показать, что $a_1 = c_2$,
 $a_i = (c_1 c_2)^{n-1-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{1-n+i}$, где $i = 2, \dots, n-1$.

Лемма 4. Пусть $d_1 = (12), d_2 = (23 \dots n)$. Тогда $S_n = \langle d_1, d_2 \rangle$.

Для доказательства достаточно заметить, что $c_1 = d_2 d_1$, $c_2 = d_1$. В частности, $a_1 = d_1$, $a_i = d_2^{n-i} d_1 d_2^{i-n}$, где $i = 2, \dots, n-1$.

Следующее предложение общеизвестно. Мы приводим его доказательство для полноты изложения.

Предложение 1.

Пусть $G_n = \langle x_1, \dots, x_{n-1} \mid x_i^2 = (x_i x_{i+1})^3 = (x_i x_j)^2 = 1, \text{ где } |j-i| \geq 2, 2 \leq i \leq n-1 \rangle$.

Тогда $G_n \simeq S_n$.

Доказательство. Положим $b_i = (i, i+1) \in S_n$, $i = 1, \dots, n-1$. Очевидно, что соотношения группы G_n выполняются для $B = \langle b_i \mid i = 1, \dots, n-1 \rangle$. Так как по лемме 2 $B = S_n$, то отображение $\Theta: x_i \rightarrow b_i$, $i = 1, \dots, n-1$ продолжается до сюръективного гомоморфизма $\Theta: G_n \rightarrow S_n$. Таким образом, $|G_n| \geq |S_n| = n!$. Докажем, что $|G_n| \leq n!$, используя индукцию по n . При $n = 1, 2, 3$ утверждение тривиально: $S_3 = \langle x_1, x_2 \mid x_1^2 = x_2^2 = (x_1 x_2)^3 = 1 \rangle$.

Предположим, что $|G_n| \leq n!$, и докажем, что $|G_{n+1}| \leq (n+1)!$. Положим $H = \langle x_2, \dots, x_n \rangle \leq G_{n+1}$. Очевидно, $H \simeq G_n$, поэтому $|H| \leq n!$. Остается доказать, что $|G_n : H| \leq n+1$. Заметим, что $\Theta(H) \simeq S_n$ является стабилизатором 1 в S_{n+1} . Выберем представителей $g_0, \dots, g_n$ смежных классов G_n по H так, чтобы $\Theta(g_0), \dots, \Theta(g_n)$ отображали 1 в $1, 2, \dots, n+1$ соответственно. Положим $\Theta(g_i) = b_1 \dots b_i$. Тогда $1^{\Theta(g_i)} = 1^{b_1 \dots b_i} = i+1$. Положим $g_0 = 1$, $g_i = x_1 x_2 \dots x_i$, т.е. $g_i = g_{i-1} x_i$. Пусть $S = \bigcup_{i=0}^n H g_i$. Необходимо доказать, что $S = G_n$. Достаточно показать, что $g_i x_j \in S$ для любых i, j .

Случай 1. Если $j > i+1$, то $g_i x_j = x_j g_i \in S$ (так как $x_j \in H$).

Случай 2. Если $j = i+1$, то $g_i x_j = g_{i+1} \in S$.

Случай 3. Если $j = i$, то $g_i x_j = g_{i-1} \in S$.

Случай 4. Пусть $j < i$. Докажем индукцией по $i - j$, что $g_i x_j = x_{j+1} g_i \in S$, для $x_{j+1} \in H$.

База индукции: $i - j = 1$ (тогда $i \geq 2$ и $j = i - 1$). В этом случае $g_i x_j = g_{i-2} x_{i-1} x_i x_{i-1} = g_{i-2} x_i x_{i-1} x_i = x_i g_{i-2} x_{i-1} x_i = x_i g_i = x_{j+1} g_i$.

Шаг индукции: если $i - j > 1$, то $g_i x_j = g_{i-1} x_i x_j = g_{i-1} x_j x_i = x_{j+1} g_{i-1} x_i = x_{j+1} g_i$.

Таким образом, $G_n = S$, откуда $|G_n : H| \leq n + 1$ и $|G_n| \leq (n + 1)!$, т.е. Θ является изоморфизмом. Предложение доказано.

3. Определяющие соотношения

Теорема 1. Пусть $G = \langle x_1, \dots, x_m \mid R \rangle$, $\{x_1, \dots, x_m\}$ – порождающее множество, $R = \{v_1(x_1, \dots, x_m), \dots, v_s(x_1, \dots, x_m)\}$ – набор определяющих соотношений группы G .

Предположим, что $X = \{y_1, \dots, y_n\}$, $G = \langle X \rangle$ и $x_i = w_i = w_i(y_1, \dots, y_n)$, $i = 1, \dots, m$, $y_i = u_i = u_i(x_1, \dots, x_m)$, $i = 1, 2, \dots, n$. Тогда $G \simeq \langle y_1, \dots, y_n \mid S \rangle$, где $S = \{v_1(w_1, \dots, w_m), \dots, v_s(w_1, \dots, w_m), u_1(w_1, \dots, w_m) y_1^{-1}, \dots, u_n(w_1, \dots, w_m) y_n^{-1}\}$.

Доказательство. Пусть $H = \langle y_1, \dots, y_n \mid S \rangle$. Соотношения S выполнены для $y_1, \dots, y_n$, поэтому G – гомоморфный образ H . Если теперь выразить x_i через $y_1, \dots, y_n$, т.е. вместо w_i написать x_i , то полученная подгруппа из H (на самом деле она совпадает с H) будет гомоморфным образом G . Поэтому $G \simeq H$ и S – определяющие соотношения в алфавите $y_1, \dots, y_n$.

Нам известно представление симметрической группы S_n из предложения 1. Воспользовавшись теоремой 1, найдем наборы определяющих соотношений, соответствующих наборам порождающих из лемм 2 – 4.

Предложение 2.

Пусть $G = \left\langle x_1, \dots, x_{n-1} \mid \begin{array}{l} x_i^2 = (x_{i-1} x_{i+1})^3 = \\ \left(x_i^{x_{i-1}} x_j^{x_{j-1}} \right)^2 = (x_i x_{i+1})^3 = 1, \\ \text{где } |j - i| \geq 2, \quad 2 \leq i \leq n - 1 \end{array} \right\rangle$. Тогда $G \simeq S_n$.

Доказательство. Пусть a_i и b_i – подстановки, определенные в леммах 1 и 2. Напомним, что $a_1 = b_1$, $a_i = b_i b_{i-1} \dots b_2 b_1 b_2 \dots b_{i-1} b_i$, $i = 2 \dots n - 1$.

$$w_1 = b_1 = a_1, \quad w_i = b_i = (i, i+1) = (1, i)(1, i+1)(1, i) = a_{i-1} a_i a_{i-1} = a_i^{a_{i-1}}, \quad i = 2 \dots n - 1.$$

По предложению 1 $S_n = \langle b_1, \dots, b_{n-1} \mid b_i^2 = (b_i b_{i+1})^3 = (b_i b_j)^2 = 1 \rangle$. Выразим слова $v_1 = b_i^2$, $v_2 = (b_i b_{i+1})^3$, $v_3 = (b_i b_j)^2$ через a_i .

$$v_1 = b_i^2 = \left(a_i^{a_{i-1}} \right)^2 = 1, \quad \text{так как } a_i^2 = 1.$$

$v_2 = (b_i b_{i+1})^3 = \left((a_{i-1} a_i a_{i-1}) (a_i a_{i+1} a_i) \right)^3$. Преобразовывая это выражение, с учетом того, что $(a_i a_{i+1})^3 = 1$, получаем определяющее соотношение $(a_{i-1} a_{i+1})^3 = 1$.

$$v_3 = (b_i b_j)^2 = \left(a_i^{a_{i-1}} a_j^{a_{j-1}} \right)^2, \text{ где } |j-i| \geq 2.$$

$$u_1(w_1, \dots, w_{n-1}) a_1^{-1} = a_1 a_1^{-1} = 1.$$

Учитывая соотношения $(a_i a_{i+1})^3 = 1$, получим что

$u_i(w_1, \dots, w_{n-1}) a_i^{-1} = a_i^{a_{i-1}} a_{i-1}^{a_{i-2}} \dots a_1 a_2 a_1 a_2 a_1 \dots a_{i-1}^{a_{i-2}} a_i^{a_{i-1}} a_i = 1$, где $i = 2, \dots, n-1$. Действительно, легко показать по индукции, что $u_k(w_1, \dots, w_{n-1}) = a_{k-1} a_k a_{k-1} a_k a_{k-1}$.

Тогда по теореме 1 $S_n \simeq G$.

Предложение 3.

$$\text{Пусть } G = \left\langle \begin{array}{l} x_1, x_2 \\ \left| \begin{array}{l} x_2^2 = [x_1 x_2 x_1^{-1}, (x_1 x_2)^2]^3 = [x_1, x_2]^3 = [x_2^{x_1}, (x_1 x_2)^{j-i}]^2 = \\ x_1^n = (x_1 x_2)^{n-1} = 1, \\ \text{где } |j-i| \geq 2, \quad 2 \leq i \leq n-1 \end{array} \right. \end{array} \right\rangle.$$

Тогда $G \simeq S_n$.

Доказательство. Пусть теперь a_i и c_i – подстановки из лемм 1 и 3. Если $a_i = (1, i+1)$, то несложно понять, что $a_1 = c_2$, $a_i = (c_1 c_2)^{n-1-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{1-n+i}$, для $i > 1$ и $c_1 = a_1 a_2 \dots a_{n-1}$, $c_2 = a_1$. Выразим слова $v_1 = a_i^2$, $v_2 = (a_{i-1} a_{i+1})^3$, $v_3 = (a_i a_{i+1})^3$, $v_4 = (a_i^{a_{i-1}} a_j^{a_{j-1}})^2$ через c_1, c_2 .

$$v_1 = a_i^2 = \left((c_1 c_2)^{n-1-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{1-n+i} \right)^2 = 1, \text{ так как } c_2^2 = 1.$$

$$v_2 = (a_{i-1} a_{i+1})^3 = \left((c_1 c_2)^{n-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{i-n} (c_1 c_2)^{n-2-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{2-n+i} \right)^3.$$

Преобразуя это выражение, получаем определяющее соотношение $[c_1 c_2 c_1^{-1}, (c_1 c_2)^2]^3 = 1$.

$$v_3 = (a_{i+1} a_i)^3 = \left((c_1 c_2)^{n-2-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{2-n+i} (c_1 c_2)^{n-1-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{1-n+i} \right)^3.$$

После преобразования этого выражения получаем определяющее соотношение $[c_1, c_2]^3 = 1$.

$$v_4 = (a_i^{a_{i-1}} a_j^{a_{j-1}})^2 =$$

$$\left(\begin{array}{l} (c_1 c_2)^{n-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{i-n} (c_1 c_2)^{n-1-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{1-n+i} (c_1 c_2)^{n-i} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{i-n} \\ (c_1 c_2)^{n-j} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{j-n} (c_1 c_2)^{n-1-j} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{1-n+j} (c_1 c_2)^{n-j} (c_1 c_2 c_1^{-1}) (c_1 c_2)^{j-n} \end{array} \right)^2.$$

После преобразования этого выражения, получаем определяющее соотношение $[c_2^{c_1}, (c_1 c_2)^{j-i}]^2 = 1$, где $|j-i| \geq 2$.

$u_1(w_1, \dots, w_{n-1}) c_1^{-1} = a_1 a_2 \dots a_{n-1} c_1^{-1}$. После преобразований, с учетом соотношения $c_1^n = 1$, получаем определяющее соотношение $(c_1 c_2)^{n-1} = 1$.

$$u_2(w_1, \dots, w_{n-1})c_2^{-1} = a_1c_2^{-1} = c_2c_2^{-1} = 1.$$

Тогда по теореме 1 $S_n \simeq G$.

Предложение 4.

$$\text{Пусть } G = \left\langle x_1, x_2 \left| \begin{array}{l} x_1^2 = [x_1, x_2^2]^3 = [x_1, x_2]^3 = [x_1^{x_2x_1}, x_2^{j-i}]^2 = x_2^{n-1} = (x_1x_2^{-1})^n = 1, \\ \text{где } |j-i| \geq 2, \quad 2 \leq i \leq n-1 \end{array} \right. \right\rangle.$$

Тогда $G \simeq S_n$.

Доказательство. Пусть теперь a_i и d_i – подстановки из лемм 1 и 4. Если $a_i = (1, i+1)$, то несложно понять, что $a_1 = d_1$, $a_i = d_2^{n-i}d_1d_2^{i-n}$, где $i > 1$ и $d_1 = a_1$, $d_2 = a_1a_2 \dots a_{n-1}a_1^{-1}$. Аналогично доказательству предыдущих предложений выразим слова $v_1 = a_i^2$, $v_2 = (a_{i-1}a_{i+1})^3$, $v_3 = (a_i a_{i+1})^3$, $v_4 = (a_i^{a_{i-1}} a_j^{a_{j-1}})^2$ через d_1, d_2 .

$$v_1 = a_i^2 = (d_2^{n-i}d_1d_2^{i-n})^2 = 1, \text{ так как } d_1^2 = 1.$$

$v_2 = (a_{i-1}a_{i+1})^3 = (d_2^{n-i+1}d_1d_2^{i-1-n}d_2^{n-i-1}d_1d_2^{i+1-n})^3$. Преобразуя это выражение, получаем определяющее соотношение $[d_1, d_2^2]^3 = 1$.

$v_3 = (a_{i+1}a_i)^3 = (d_2^{n-i-1}d_1d_2^{i+1-n}d_2^{n-i}d_1d_2^{i-n})^3$. Преобразуя это выражение, получаем определяющее соотношение $[d_1, d_2]^3 = 1$.

$$v_4 = (a_i^{a_{i-1}} a_j^{a_{j-1}})^2 =$$

$$(d_2^{n-i+1}d_1d_2^{i-1-n}d_2^{n-i}d_1d_2^{i-n}d_2^{n-i+1}d_1d_2^{i-1-n}d_2^{n-j+1}d_1d_2^{j-1-n}d_2^{n-j}d_1d_2^{j-n}d_2^{n-j+1}d_1d_2^{j-1-n})^2.$$

Преобразуя это выражение, получаем определяющее соотношение $[d_1^{d_2d_1}, d_2^{j-i}]^2 = 1$, где $|j-i| \geq 2$.

$$u_1(w_1, \dots, w_{n-1})d_1^{-1} = a_1d_1^{-1} = d_1d_1^{-1} = 1.$$

$u_2(w_1, \dots, w_{n-1})d_2^{-1} = a_1a_2 \dots a_{n-1}a_1^{-1}d_2^{-1}$. После преобразований, с учетом соотношения $d_2^{n-1} = 1$, получаем определяющее соотношение $(d_1d_2^{-1})^n = 1$.

Тогда по теореме 1 $S_n \simeq G$.

4. Пример графа $n = 10$

Рассмотрим неориентированный граф Γ с вершинами $0, 1, 2, \dots, 9$ и множеством ребер $07, 08, 09, 15, 16, 19, 24, 26, 28, 34, 35, 37, 49, 58, 67$ (упрощая обозначения, мы здесь пишем $\alpha\beta$ вместо (α, β)).

Его матрица инцидентности равна

$$I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Предложение 5.

Группа симметрий Γ изоморфна S_5 .

Доказательство. Подстановки $b_1 = (14)(25)(36)$, $b_2 = (01)(57)(68)$, $b_3 = (12)(45)(89)$, $b_4 = (23)(56)(78)$ вершин графа Γ являются симметриями Γ , в чем легко убедиться, проверив, что подстановочные матрицы, соответствующие b_1, b_2, b_3, b_4 , перестановочны с I . Простая проверка показывает, что

$$b_1^2 = b_2^2 = b_3^2 = b_4^2 = (b_1 b_2)^3 = (b_2 b_3)^3 = (b_3 b_4)^3 = (b_1 b_3)^2 = (b_1 b_4)^2 = (b_2 b_4)^2 = 1.$$

По предложению 1 подгруппа $B = \langle b_1, b_2, b_3, b_4 \rangle$ является гомоморфным образом группы S_5 . Ясно, что $|B| > 2$. Поскольку гомоморфными образами S_5 являются, кроме самой S_5 , только группы порядков 1 и 2, то $B \simeq S_5$.

Покажем, что на самом деле B совпадает со всей группой симметрий Γ . Действительно, $4 \xrightarrow{b_1} 1 \xrightarrow{b_3} 2 \xrightarrow{b_4} 3 \xrightarrow{b_1} 6 \xrightarrow{b_4} 5 \xrightarrow{b_2} 7 \xrightarrow{b_4} 8 \xrightarrow{b_3} 9$, поэтому B транзитивна на вершинах Γ и, следовательно, G также транзитивна на вершинах Γ . Отсюда индекс стабилизатора G_1 вершины 0 в G равен 10 и G_1 действует на множестве ребер $\{07, 08, 09\}$, инцидентных вершине 0. Порядок стабилизатора любого из множеств $\{07\}, \{08\}, \{09\}$ не превосходит числа 2, поэтому $|G| \leq 10 \cdot |S_3| \cdot |S_2| = 10 \cdot 6 \cdot 2 = 120 = |B|$.

5. Заключение

В этой статье были определены различные представления для симметрической группы S_n . Представление группы – это один из способов определения группы указанием порождающего множества и множества соотношений между порождающими. Каждая группа имеет представление и, более того, много различных представлений. Зачастую представление является наиболее компактным способом описания группы. Поэтому поиск различных представлений заданной группы достаточно важен. Первая серия групп, для которых мы нашли различные представления, это симметрические группы S_n степени n . Поскольку любая конечная группа изоморфна подгруппе симметрической группы, то это особенно актуально. В

дальнейшем эти результаты будут использованы для нахождения представлений знакопеременной группы A_n .

Выражение благодарности

В заключение автор выражает благодарность своему научному руководителю, профессору Д. В. Лыткиной за помощь в подготовке работы. Также мы благодарим анонимного рецензента за ценные замечания, которые позволили существенно улучшить качество работы.

Литература

1. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. Представление групп в терминах образующих и соотношений. М.: Наука, Главная редакция физико-математической литературы, 1974. 456 с.

*Статья поступила в редакцию 19.02.2016;
переработанный вариант — 12.04.2016*

Овчаренко Алёна Юрьевна

аспирант СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. +7 (952) 917-20-27,
e-mail: shmatova_aaa@mail.ru.

On the method of searching large subgroups in groups of graphs symmetries

A. Ovcharenko

In this paper, defining relationships for the well-known systems of group generators of finite sets substitution are presented. It gives the possibility, in some cases, to find without too much computational complexity large sub-group symmetries for graphs with a large number of vertices. An example of the results application to the determination groups of symmetries of graph 10 degrees is given.

Keywords: symmetric group, group generator, finite set substitution.