О представлении подстановок в виде произведений транспозиции и полного цикла

А. Ю. ЗУБОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: Tat.z.69@mail.ru

УДК 512.542.74+512.543.72

Ключевые слова: уравнение в группе, кортеж подстановки, обобщённые инверсии перестановки, система булевых уравнений.

Аннотация

Предлагается метод решения уравнений вида $g^{y_1} \cdot h \cdot g^{y_2} \cdot h \cdot \ldots \cdot g^{y_l} \cdot h \cdot g^{y_{l+1}} = \sigma$ в симметрической группе S_n, где h — транспозиция, g — полный цикл, $\sigma \in \mathrm{S}_n$. Метод основан на построении всех множеств обобщённых инверсий нижней строки подстановки σ с помощью системы булевых уравнений, ассоциированных с σ. Приведён пример решения уравнения в группе S_6.

Abstract

A. Yu. Zubov, On the representation of substitutions as products of a transposition and a full cycle, Fundamentalnaya i prikladnaya matematika, vol. 15 (2009), no. 1, pp. 31—51.

A method of solving equations of the form $g^{y_1} \cdot h \cdot g^{y_2} \cdot h \cdot \ldots \cdot g^{y_l} \cdot h \cdot g^{y_{l+1}} = \sigma$ in the symmetric group S_n is proposed, where h is a transposition, g is a full cycle, and $\sigma \in \mathrm{S}_n$. The method is based on building all sets of generalized inversions of the bottom line of the substitution σ by means of a system of Boolean equations associated with σ. An example of solving an equation in a group S_6 is given.

Введение

В [1, 2] приведён ряд теоретико-групповых задач, имеющих приложения в криптографии, среди них задачи изучения параметров, связанных с заданием конечных групп системами образующих элементов, таких как длина и ширина группы, и решения уравнений в группах вида

$$A_1 \cdot X_1 \cdot \ldots \cdot A_l \cdot X_l \cdot A_{l+1} = \sigma.$$

В качестве примера выделяется система образующих элементов симметрической группы подстановок S_n, состоящая из полного цикла g и транспозиции h. В [3] найдено асимптотически точное значение длины группы S_n относительно системы образующих $\{g, h\}$. Данная статья посвящена разработке методов

Фундаментальная и прикладная математика, 2009, том 15, № 1, с. 31—51.

нахождения всех представлений элементов группы S_n в виде произведений, составленных из транспозиции и полного цикла, и, в частности, методов решения уравнений вида

$$g^{y_1} \cdot h \cdot g^{y_2} \cdot h \cdot \ldots \cdot g^{y_l} \cdot h \cdot g^{y_{l+1}} = \sigma, \quad l \in \mathbb{N}, \quad \sigma \in \mathrm{S}_n.$$

1. Кортежи подстановок

Пусть S_n — симметрическая группа подстановок на множестве $\Omega_n = \{0, 1, \ldots, n-1\}$ и $\sigma \in \mathrm{S}_n$. Обозначим через $i\sigma$ образ элемента $i \in \Omega_n$ по подстановке σ. Если $\{i, j, \ldots\} \subset \Omega_n$, то через $\{i, j, \ldots\}\sigma$ обозначим множество $\{i\sigma, j\sigma, \ldots\}$. В этой статье через g и h обозначаются соответственно полный цикл $(0, 1, \ldots, n-1)$ и транспозиция $(0, 1)$ из S_n, а через $\mathbb{N}$ множество натуральных чисел.

В основе предлагаемого здесь метода лежит понятие кортежа, введённое в [3].

Определение 1. Последовательность

$$A_\sigma = (\{a_0, b_0\}, \{a_1, b_1\}, \ldots, \{a_k, b_k\}), \quad k \in \mathbb{N},$$

пар символов из Ω_n называется *кортежем подстановки* $\sigma \in \mathrm{S}_n$ (или, короче, *σ-кортежем*), если найдутся такие $n_0, n_1, \ldots, n_{k+1} \in \Omega_n$, что

$$\sigma = g^{n_0} \cdot h \cdot g^{n_1} \cdot h \cdot \ldots \cdot g^{n_k} \cdot h \cdot g^{n_{k+1}},$$

причём выполняются равенства

$$\{0, 1\}(g^{-n_i} \cdot h \cdot g^{-n_{i-1}} \cdot h \cdot \ldots \cdot h \cdot g^{-n_0} \cdot \sigma) = \{a_i, b_i\}, \quad i = 0, 1, \ldots, k.$$

Последовательность $(n_0, n_1, \ldots, n_k)$ называется *типом кортежа* A_σ, число $k+1$ — *длиной кортежа*, а слово $\Theta(A_\sigma)$ (в алфавите $\{h, g^{-1}\}$), заданное формулой $\Theta(A_\sigma) = hg^{-n_k}hg^{-n_{k-1}}h \ldots hg^{-n_0}$, — *словом, определяющим кортеж* A_σ.

Имеется очевидное взаимно-однозначное соответствие между множеством возможных представлений подстановки $\sigma \in \mathrm{S}_n$ в виде произведений, составленных из транспозиции и полного цикла, и множеством возможных σ-кортежей.

Если

$$W = g^{-s_1}hg^{-s_2}h \ldots hg^{-s_t} -$$

слово в алфавите $\{h, g^{-1}\}$, то через $\overline{W}$ будем обозначать произведение подстановок

$$g^{-s_1} \cdot h \cdot g^{-s_2} \cdot h \cdot \ldots \cdot h \cdot g^{-s_t}.$$

Заметим, что умножение подстановки σ слева на g^{-m} или h равносильно соответственно циклическому сдвигу нижней строки подстановки σ вправо на m шагов или транспонированию в её нижней строке двух элементов, расположенных на первых двух местах. Поэтому при переходе от подстановки σ к подстановке $\bar{\Theta}(A_\sigma) \cdot \sigma$ (где A_σ — σ-кортеж) последовательно производятся указанные преобразования нижней строки подстановки σ, при этом транспозиции

пар символов происходят в соответствии с их расположением в A_σ. Отметим, что σ-кортеж может содержать одинаковые пары символов.

Определение 2. Пусть A_σ — произвольный σ-кортеж и $\tilde{A}_\sigma$ — совокупность всех пар из A_σ с учётом кратностей их вхождения. Назовём мультимножество $\tilde{A}_\sigma$ *носителем σ-кортежа* A_σ.

Непосредственно из определений 1 и 2 следует алгоритм построения всех кортежей с данным носителем. Пусть даны подстановка $\sigma \in \mathrm{S}_n$ и произвольное конечное мультимножество A пар символов из Ω_n, $|A| = k+1$. Для описания всех σ-кортежей с носителем A достаточно найти множество их типов $T(A_\sigma) = \{(n_0, n_1, \ldots, n_k)\}$. Это множество может быть построено с помощью следующего алгоритма.

Алгоритм 1. Строим множество

$$T_0(A_\sigma) = \{n_0 \colon \{0,1\}(g^{-n_0} \cdot \sigma) \in A\}.$$

Если $|A| = 1$ или $T_0(A_\sigma) = \varnothing$, то алгоритм закончен. В этом случае $T(A_\sigma) = T_0(A_\sigma)$. В противном случае строим множество

$$T_1(A_\sigma) = \{(n_0, n_1) \colon n_0 \in T_0(A_\sigma),\ \{0,1\}(g^{-n_1} \cdot h \cdot g^{-n_0} \cdot \sigma) \in A_{n_0}\},$$

где

$$A_{n_0} = A \setminus \big\{\{0,1\}(g^{-n_0} \cdot \sigma)\big\}.$$

Предположим, что построено множество $T_i(A_\sigma)$, $i \geqslant 1$. Тогда если $|A| = i$ или $T_i(A_\sigma) = \varnothing$, то алгоритм закончен. В этом случае $T(A_\sigma) = T_i(A_\sigma)$. В противном случае строим множество

$$T_{i+1}(A_\sigma) = \{(n_0, \ldots, n_{i+1}) \colon (n_0, \ldots, n_i) \in T_i(A_\sigma), \\ \{0,1\}(g^{-n_{i+1}} \cdot h \cdot g^{-n_0} \cdot \sigma) \in A_{n_0,\ldots,n_i}\},$$

где

$$A_{n_0,\ldots,n_i} = A_{n_0,\ldots,n_{i-1}} \setminus \big\{\{0,1\}(g^{-n_i} \cdot h \cdot g^{-n_0} \cdot \sigma)\big\}.$$

Если $|A| = k$ и при некотором $s < k-1$ получается $T_s(A_\sigma) = \varnothing$, то $T(A_\sigma) = \varnothing$. В противном случае $T(A_\sigma) = T_{k-1}(A_\sigma)$.

Теорема 1. *Пусть σ — подстановка из группы S_n. Тогда носитель любого конечного σ-кортежа содержит в качестве подмножества носитель некоторого σ-кортежа без кратных вхождений пар.*

Доказательство. Пусть σ — подстановка из S_n, A_σ — её кортеж и пара $\{i,j\}$ содержится в $\tilde{A}_\sigma$ с кратностью, не меньшей 2. Тогда согласно определению 1 слово $\Theta(A_\sigma)$, определяющее A_σ, можно представить в виде $\Theta(A_\sigma) = W_3 h W_2 h W_1$, где подслова W_1, W_2, W_3 таковы, что

$$\{0,1\}(\overline{W_1} \cdot \sigma) = \{0,1\}(\overline{W_2 h W_1} \cdot \sigma) = \{i,j\}.$$

При этом возможны два случая:

1) $0(\overline{W_1}\cdot\sigma)=i$, $1(\overline{W_1}\cdot\sigma)=j$, $0(\overline{W_2hW_1}\cdot\sigma)=i$, $1(\overline{W_2hW_1}\cdot\sigma)=j$;
2) $0(\overline{W_1}\cdot\sigma)=i$, $1(\overline{W_1}\cdot\sigma)=j$, $0(\overline{W_2hW_1}\cdot\sigma)=j$, $1(\overline{W_2hW_1}\cdot\sigma)=i$.

В случае 1) имеют место равенства $0(\overline{W_2hW_1}\cdot\sigma)=i=0(\overline{W_1}\cdot\sigma)$, откуда следует, что $0\overline{W_2}=1$. Аналогично $1\overline{W_2}=0$. Тогда $\overline{W_2}=\overline{hW_2h}$ и $\bar{\Theta}(A_\sigma)=\overline{W_3W_2W_1}$.

Очевидно, что слово $W_3W_2W_1$ определяет σ-кортеж A'_σ, для которого $\Theta(A'_\sigma)=W_3W_2W_1$, причём $\tilde{A}'_\sigma=(\tilde{A}_\sigma\setminus\{i,j\})\setminus\{i,j\}$. Мы уменьшили на 2 кратность вхождения пары $\{i,j\}$ в $\tilde{A}_\sigma$. Точно так же можно было поступить и с любой другой парой из $\tilde{A}_\sigma$, имеющей кратность, не меньшую 2.

Аналогично строится A'_σ в случае 2). Отсюда следует требуемое утверждение. □

Замечание. Если $\sigma=g^t$, то исключение из $\tilde{A}_\sigma$ кратных вхождений пар может привести к пустому подмножеству $\tilde{A}'_\sigma$.

Для нас представляет больший интерес обращение теоремы 1. Пусть $\bar{\bar{A}}_\sigma$ — класс всех конечных носителей σ-кортежей и $\bar{A}_\sigma$ — его подкласс, состоящий из всех носителей σ-кортежей без кратных вхождений пар. Непосредственно из теоремы 1 вытекает следующее утверждение.

Теорема 2. *Любой элемент из $\bar{\bar{A}}_\sigma$ может быть получен путём добавления кратных вхождений пар к подходящему элементу из $\bar{A}_\sigma$.*

Предположим, что для подстановки $\sigma\in\mathrm{S}_n$ нам удалось неким образом построить (конечный) класс $\bar{A}_\sigma$ носителей σ-кортежей. Тогда путём добавления к элементам из $\bar{A}_\sigma$ кратных пар мы сможем построить множество всех носителей σ-кортежей нужной длины l, применяя к которым алгоритм 1, мы найдём все решения уравнения

$$g^{y_1}\cdot h\cdot g^{y_2}\cdot h\cdot\ldots\cdot g^{y_l}\cdot h\cdot g^{y_{l+1}}=\sigma. \tag{1}$$

Таким образом, чтобы решить уравнение (1), достаточно научиться строить множество $\bar{A}_\sigma$. Для решения этой задачи нам понадобятся множества обобщённых инверсий перестановок.

2. Множества обобщённых инверсий перестановок

Определим процедуру, которую назовём *расстановкой меток в подстановке*. Она состоит в следующем. Поставим в соответствие каждому символу нижней строки подстановки $\sigma\in\mathrm{S}_n$ метку 0 или 1. При этом символу i, для которого $i\sigma=i$, ставится в соответствие лишь метка 0. Если же $i\sigma\neq i$, то символу i можно поставить в соответствие как метку 0, так и метку 1. Если x_i — метка символа $i\in\Omega_n$, то вектор $\vec{x}=(x_0,x_1,\ldots,x_{n-1})$ назовём *вектором меток* в σ.

Для вектора меток $\vec{x}$ в σ через $[i\sigma, i]_{\vec{x}}$ обозначим следующее множество символов нижней строки подстановки:

$$[i\sigma, i]_{\vec{x}} = \begin{cases} \{i\sigma, (i+1)\sigma, \ldots, i\}, & \text{если } x_i = 0 \text{ и } i\sigma \neq i, \\ \{i\sigma, (i-1)\sigma, \ldots, i\}, & \text{если } x_i = 1 \text{ и } i\sigma \neq i, \\ \{i\}, & \text{если } i\sigma = i. \end{cases} \tag{2}$$

В (2) операции сложения и вычитания выполняются по модулю n.

Поставим в соответствие вектору меток $\vec{x}$ в σ множество $D_\sigma(\vec{x})$ пар символов из Ω_n, построенное по следующему правилу. Пара $\{i, j\}$ в том и только том случае принадлежит $D_\sigma(\vec{x})$, когда выполняется хотя бы одно из следующих условий:

1) $[i\sigma, i]_{\vec{x}} \subset [j\sigma, j]_{\vec{x}}$ или $[j\sigma, j]_{\vec{x}} \subset [i\sigma, i]_{\vec{x}}$;
2) $[i\sigma, i]_{\vec{x}} \cap [j\sigma, j]_{\vec{x}} \neq \varnothing$, причём $x_i \neq x_j$.

Множества $[i\sigma, i]_{\vec{x}}$ и $D_\sigma(\vec{x})$ имеют простую геометрическую интерпретацию. Расположим подстановку σ на круге с n точками (соединив начало с концом), верхнюю строку на внутренней части круга, нижнюю на внешней части. Пусть метка 0 соответствует «направлению движения» символа, расположенного на внешней части круга, «на своё место» на внутренней части круга против часовой стрелки. Пусть метка 1 соответствует «направлению движения» символа по часовой стрелке (если $i\sigma = i$, то символ i «неподвижен»). Утверждение $\{i, j\} \in \in D_\sigma(\vec{x})$ равносильно тому, что символы i и j при «движении» на свои места по предписанным им направлениям обязаны встретиться на внешней части круга и поменяться местами друг с другом.

Важная роль в дальнейших рассуждениях отводится вектору меток $\vec{0}$, состоящему из одних нулей. В этом случае $D_\sigma(\vec{0})$ совпадает с множеством

$$\big\{\{i, j\} \colon [i\sigma, i]_{\vec{0}} \supseteq [j\sigma, j]_{\vec{0}} \text{ или } [i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}\big\}.$$

Пусть

$$D_\sigma = \{D_{g^k \cdot \sigma}(\vec{0}) \colon k \in \Omega_n\}.$$

Теорема 3 [3, теорема 2.1]. *Для любой подстановки $\sigma \in \mathrm{S}_n$ множество D_σ состоит из носителей σ-кортежей. Носитель σ-кортежа минимально возможной длины принадлежит множеству D_σ.*

Множество инверсий произвольной перестановки $(i_0, i_1, \ldots, i_{n-1})$ множества Ω_n может быть реализовано как множество $D_\sigma(\vec{x})$ для подстановки

$$\sigma = \begin{pmatrix} 0 & 1 & \ldots & n-1 \\ i_0 & i_1 & \ldots & i_{n-1} \end{pmatrix}$$

и подходящего вектора меток $\vec{x}$. Таковым является, например, вектор $\vec{x}$, в котором метка x_{i_j} равна 0, если символ i_j расположен правее своего места (или находится на своём месте), и равна 1, если символ i_j расположен левее своего места в нижней строке подстановки σ. При «движении пары символов на свои места в предписанных им направлениях» они должны встретиться и поменяться местами друг с другом.

В связи с указанной трактовкой множества инверсий введём понятие множества обобщённых инверсий перестановки.

Определение 3. Будем называть множество $D_\sigma(\vec{x})$, являющееся носителем некоторого кортежа подстановки σ, множеством обобщённых инверсий перестановки, которой является нижняя строка подстановки σ.

Оказывается, что для любой подстановки σ множество $\bar{A}_\sigma$ носителей кортежей без кратных вхождений пар состоит из множеств обобщённых инверсий нижних строк всех подстановок $g^r \cdot \sigma$, $r \in \Omega_n$.

В дальнейшем будем описывать подстановку σ её нижней строкой в виде $[0\sigma, 1\sigma, \ldots, (n-1)\sigma]$.

3. Описание множеств обобщённых инверсий перестановок

Пусть σ — подстановка из S_n, $\vec{x}$ — вектор меток в σ и $\Omega \subset \Omega_n$. Введём обозначение

$$D_\sigma^\Omega(\vec{x}) = \big\{\{\alpha, \beta\} \in D_\sigma(\vec{x})\colon \alpha, \beta \in \Omega\big\}.$$

Лемма 4. *Пусть σ — подстановка из S_n, $\vec{y}$ — произвольный вектор меток в σ и для вектора меток $\vec{x}$ в σ множество $D_\sigma(\vec{x})$ является множеством обобщённых инверсий нижней строки подстановки σ. Если для различных точек $i, j, k \in \Omega_n$ выполняются условия*

$$D_\sigma^{\Omega_1}(\vec{x}) = D_\sigma^{\Omega_1}(\vec{y}), \quad D_\sigma^{\Omega_2}(\vec{x}) = D_\sigma^{\Omega_2}(\vec{y}), \quad D_\sigma^{\Omega_3}(\vec{x}) \neq D_\sigma^{\Omega_3}(\vec{y})$$

или условия

$$D_\sigma^{\Omega_1}(\vec{x}) \neq D_\sigma^{\Omega_1}(\vec{y}), \quad D_\sigma^{\Omega_2}(\vec{x}) \neq D_\sigma^{\Omega_2}(\vec{y}), \quad D_\sigma^{\Omega_3}(\vec{x}) \neq D_\sigma^{\Omega_3}(\vec{y}),$$

где

$$\{\Omega_1, \Omega_2, \Omega_3\} = \big\{\{i, j\},\ \{i, k\},\ \{j, k\}\big\},$$

то $D_\sigma(\vec{y})$ не является носителем σ-кортежа.

Доказательство. Пусть A_σ — это σ-кортеж с носителем $D_\sigma(\vec{x})$ и $\Theta(A_\sigma)$ — слово, определяющее A_σ. Тогда для подходящего $r \in \Omega_n$ выполняется равенство $\bar{\Theta}(A_\sigma) = g^r$.

Предположим, что $D_\sigma(\vec{y})$ является носителем σ-кортежа. Используя условия леммы, легко убедиться в том, что для любого σ-кортежа A'_σ с носителем $D_\sigma(\vec{y})$ символы i, j и k не могут следовать друг за другом в нижней строке подстановки $\bar{\Theta}(A'_\sigma)$ в том же порядке, что и в g^t, для любого $t \in \Omega_n$. Так, если σ имеет вид $[\ldots, i, \ldots, j, \ldots, k, \ldots]$ и $\{i, j\}, \{i, k\} \in D_\sigma(\vec{x})$, но $\{j, k\} \notin D_\sigma(\vec{x})$, то для некоторого $t \in \Omega_n$

$$g^t \cdot \bar{\Theta}(A_\sigma) = [\ldots, i, \ldots, j, \ldots, k, \ldots].$$

Если же $\{i,j\} \notin D_\sigma(\vec{y})$, $\{i,k\} \in D_\sigma(\vec{y})$ и $\{j,k\} \notin D_\sigma(\vec{y})$, то для некоторого $t' \in \Omega_n$

$$g^{t'} \cdot \bar{\Theta}(A'_\sigma) = [\ldots, i, \ldots, k, \ldots, j, \ldots].$$

Эта подстановка не может совпадать со степенью подстановки g. Поэтому $\bar{\Theta}(A'_\sigma) \neq g^s$ при любом $s \in \Omega_n$. Мы получили противоречие с тем, что A'_σ является σ-кортежем. □

Определение 4. Если для подстановки $\sigma \in \mathrm{S}_n$, векторов меток $\vec{x}$, $\vec{y}$ в σ и символов $i,j,k \in \Omega_n$ выполняются условия леммы 4, то будем говорить, что для σ тройка (y_i, y_j, y_k) *не является согласованной* с тройкой (x_i, x_j, x_k). В противном случае тройки будем называть *согласованными*.

Таким образом, тройки (y_i, y_j, y_k) и (x_i, x_j, x_k) являются согласованными для σ, если выполняются условия

$$D_\sigma^{\Omega_1}(\vec{x}) = D_\sigma^{\Omega_1}(\vec{y}), \quad D_\sigma^{\Omega_2}(\vec{x}) = D_\sigma^{\Omega_2}(\vec{y}), \quad D_\sigma^{\Omega_3}(\vec{x}) = D_\sigma^{\Omega_3}(\vec{y})$$

или условия

$$D_\sigma^{\Omega_1}(\vec{x}) \neq D_\sigma^{\Omega_1}(\vec{y}), \quad D_\sigma^{\Omega_2}(\vec{x}) \neq D_\sigma^{\Omega_2}(\vec{y}), \quad D_\sigma^{\Omega_3}(\vec{x}) = D_\sigma^{\Omega_3}(\vec{y}).$$

Лемма 5. *Пусть $\sigma \in \mathrm{S}_n$ и $\vec{x}$ — вектор меток в σ. Тогда $D_\sigma(\vec{x})$ является множеством обобщённых инверсий нижней строки подстановки σ тогда и только тогда, когда для любых различных символов $i,j,k \in \Omega_n$ тройки (x_i, x_j, x_k) и $(0,0,0)$ являются согласованными для σ.*

Доказательство. Предположим, что $D_\sigma(\vec{x})$ — множество обобщённых инверсий нижней строки подстановки σ, но для символов $i,j,k \in \Omega_n$ тройки (x_i, x_j, x_k) и $(0,0,0)$ не являются согласованными для σ. Тогда по лемме 4 $D_\sigma(\vec{0})$ не является носителем σ-кортежа, что противоречит теореме 3. Отсюда следует необходимость. Убедимся в том, что условия и достаточны.

Рассмотрим такое множество $D_\sigma(\vec{x})$, что для любых различных символов $i,j,k \in \Omega_n$ тройки (x_i, x_j, x_k) и $(0,0,0)$ являются согласованными для σ. Покажем, что $D_\sigma(\vec{x})$ — носитель σ-кортежа. Проведём индукцию по $r = |D_\sigma(\vec{x})|$.

Пусть $r = 0$ и i — произвольный символ из Ω_n, причём $x_{i\sigma} = 0$. Если $x_{(i-1)\sigma} = 1$, то $\{(i-1)\sigma, i\sigma\} \in D_\sigma(\vec{x})$, что противоречит условию $r = 0$. Следовательно, $x_{(i-1)\sigma} = 0$. Аналогично получаем равенство $x_{(i-2)\sigma} = 0$, и т. д. Таким образом, $\vec{x} = \vec{0}$, и согласно теореме 3 $D_\sigma(\vec{0})$ является носителем σ-кортежа. Ясно, что при этом $\sigma = e$. В случае когда $x_{i\sigma} = 1$, рассуждения аналогичны.

Предположим, что утверждение верно, в случае когда $|D_\sigma(\vec{x})| \leqslant r$ и σ — подстановка, для которой $|D_\sigma(\vec{x})| = r+1$.

Если $\vec{x} = \vec{0}$ или $\vec{x} = \vec{1}$, то утверждение следует из теоремы 3. Если $\vec{x} \neq \vec{0}$ и $\vec{x} \neq \vec{1}$, то найдётся такой символ $i \in \Omega_n$, что $x_{(i-1)\sigma} = 1$, $x_{i\sigma} = 0$. При этом $\{(i-1)\sigma, i\sigma\} \in D_\sigma(\vec{x})$. Рассмотрим возможные случаи пересечения множеств $\{i-1, i\}$ и $\{(i-1)\sigma, i\sigma\}$.

I. $\{i-1, i\} \cap \{(i-1)\sigma, i\sigma\} = \varnothing$.

II. $(i-1)\sigma = i-1$, $i\sigma = i$.
III. $(i-1)\sigma = i$, $i\sigma = i-1$.

В случае I рассмотрим подстановку $\sigma_1 = (i, i-1)\cdot\sigma$ и тот же вектор меток $\vec{x}$ в σ_1, что и в σ. Непосредственно из определения множества $D_\sigma(\vec{x})$ следует, что в рассматриваемом случае выполняется равенство

$$D_{\sigma_1}(\vec{x}) = D_\sigma(\vec{x}) \setminus \{(i-1)\sigma, i\sigma\},$$

при этом для любых различных точек $i, j, k \in \Omega_n$ тройки (x_i, x_j, x_k) и $(0,0,0)$ являются согласованными для σ_1, так же как и для σ. Поскольку $|D_{\sigma_1}(\vec{x})| = r$, по предположению индукции $D_{\sigma_1}(\vec{x})$ является носителем σ_1-кортежа. Следовательно, $D_\sigma(\vec{x})$ является носителем σ-кортежа, что и требуется.

Пусть в случае II (как и в случае I) $\sigma_1 = (i, i-1)\cdot\sigma$. Рассмотрим для σ_1 вектор меток $\vec{x}'$, который отличается от $\vec{x}$ лишь тем, что $x'_i = 1$ (напомним, что $x_i = 0$). Легко убедиться, что выполняется равенство

$$D_{\sigma_1}(\vec{x}') = D_\sigma(\vec{x}) \setminus \{(i-1)\sigma, i\sigma\}.$$

Кроме того, очевидно, что если подмножество $\{\alpha, \beta, \gamma\} \subset \Omega_n$ не содержит i, то для подстановки σ_1 тройки $(x'_\alpha, x'_\beta, x'_\gamma)$ и $(0,0,0)$ остаются согласованными, как и для σ. Проверим, что для σ_1 и любых $i, j, k \in \Omega_n$ тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными. С этой целью рассмотрим возможные подслучаи случая II.

II.1. $i \in [j\sigma, j]_{\vec{0}}$, $i \in [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \subseteq [k\sigma, k]_{\vec{0}}$.
II.2. $i \in [j\sigma, j]_{\vec{0}}$, $i \in [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$.
II.3. $i \in [j\sigma, j]_{\vec{0}}$, $i \notin [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$.
II.4. $i \in [j\sigma, j]_{\vec{0}}$, $i \notin [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$.
II.5. $i \notin [j\sigma, j]_{\vec{0}}$, $i \notin [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \subseteq [k\sigma, k]_{\vec{0}}$.
II.6. $i \notin [j\sigma, j]_{\vec{0}}$, $i \notin [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$.

Рассуждения в этих случаях сходны, поэтому рассмотрим лишь случай II.1.

Из условий следуют включения $\{i, j\} \in D_\sigma(\vec{0})$, $\{i, k\} \in D_\sigma(\vec{0})$, $\{j, k\} \in D_\sigma(\vec{0})$, а из условия согласованности троек (x_i, x_j, x_k) и $(0,0,0)$ для σ следует, что возможны четыре подслучая.

II.1.а) $\{i, j\} \in D_\sigma(\vec{x})$, $\{i, k\} \in D_\sigma(\vec{x})$, $\{j, k\} \in D_\sigma(\vec{x})$.
II.1.б) $\{i, j\} \in D_\sigma(\vec{x})$, $\{i, k\} \notin D_\sigma(\vec{x})$, $\{j, k\} \notin D_\sigma(\vec{x})$.
II.1.в) $\{i, j\} \notin D_\sigma(\vec{x})$, $\{i, k\} \in D_\sigma(\vec{x})$, $\{j, k\} \notin D_\sigma(\vec{x})$.
II.1.г) $\{i, j\} \notin D_\sigma(\vec{x})$, $\{i, k\} \notin D_\sigma(\vec{x})$, $\{j, k\} \in D_\sigma(\vec{x})$.

Заметим, прежде всего, что в условиях случая II.1 для σ_1 выполняются соотношения

$$\{i, j\} \notin D_{\sigma_1}(\vec{0}), \quad \{i, k\} \notin D_{\sigma_1}(\vec{0}), \quad \{j, k\} \in D_{\sigma_1}(\vec{0}).$$

Рассмотрим подслучай II.1.а). Из условий следует, что $x_j = x_k = 0$, откуда получаем соотношения

$$\{i, j\} \in D_{\sigma_1}(\vec{x}'), \quad \{i, k\} \in D_{\sigma_1}(\vec{x}'), \quad \{j, k\} \in D_{\sigma_1}(\vec{x}').$$

Следовательно, для σ_1 тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными.

Из условий подслучая II.1.б) следует, что $x_j = 0$, $x_k = 1$, откуда получаем соотношения

$$\{i,j\} \in D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \notin D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \notin D_{\sigma_1}(\vec{x}'),$$

означающие, что для σ_1 тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными.

В условиях случая II.1.в) $x_j = 1$, $x_k = 0$, откуда следует, что

$$\{i,j\} \notin D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \in D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \in D_{\sigma_1}(\vec{x}').$$

Полученные соотношения противоречат условиям, поэтому случай II.1.в) невозможен.

В подслучае II.1.г) $x_j = 1$, $x_k = 1$, откуда следует, что

$$\{i,j\} \notin D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \notin D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \in D_{\sigma_1}(\vec{x}').$$

И в этом случае для σ_1 тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными.

Итак, в случае 1 для любых $i,j,k \in \Omega_n$ тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными для σ_1. По предположению индукции $D_{\sigma_1}(\vec{x}')$ является носителем σ_1-кортежа, следовательно, и $D_\sigma(\vec{x})$ является носителем σ-кортежа.

Точно так же рассматриваются и все другие подслучаи случая II.

Рассмотрим случай III.

Пусть $\sigma_1 = (i-1, i) \cdot \sigma$ и $\vec{x}'$ — вектор меток для σ_1, который отличается от $\vec{x}$ лишь тем, что $x'_i = 0$ (напомним, что $x_i = 1$). Как и в предыдущих случаях, выполняется соотношение

$$D_{\sigma_1}(\vec{x}') = D_\sigma(\vec{x}) \setminus \{(i-1)\sigma, i\sigma\}.$$

Кроме того, если множество $\{\alpha, \beta, \gamma\}$ не содержит элемента i, то для σ_1 тройки $(x'_\alpha, x'_\beta, x'_\gamma)$ и $(0,0,0)$ остаются согласованными, как и для σ. Проверим, что для σ_1 и различных $i,j,k \in \Omega_n$ тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными. С этой целью рассмотрим возможные подслучаи случая III.

III.1. $i-1, i \in [j\sigma, j]_{\vec{0}}$, $i-1, i \in [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \subseteq [k\sigma, k]_{\vec{0}}$.
III.2. $i-1, i \in [j\sigma, j]_{\vec{0}}$, $i-1, i \in [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$.
III.3. $i-1, i \in [j\sigma, j]_{\vec{0}}$, $i-1, i \notin [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$.
III.4. $i-1, i \in [j\sigma, j]_{\vec{0}}$, $i-1, i \notin [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$.
III.5. $i-1, i \notin [j\sigma, j]_{\vec{0}}$, $i-1, i \notin [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \subseteq [k\sigma, k]_{\vec{0}}$.
III.6. $i-1, i \notin [j\sigma, j]_{\vec{0}}$, $i-1, i \notin [k\sigma, k]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$.

Рассуждения в этих случаях сходны, поэтому рассмотрим лишь случай III.1.

Из условий случая следуют соотношения

$$\{i,j\} \notin D_\sigma(\vec{0}), \quad \{i,k\} \notin D_\sigma(\vec{0}), \quad \{j,k\} \in D_\sigma(\vec{0}),$$

а из условия согласованности троек (x_i, x_j, x_k) и $(0,0,0)$ для σ следует, что возможны четыре подслучая.

III.1.а) $\{i,j\} \notin D_\sigma(\vec{x})$, $\{i,k\} \notin D_\sigma(\vec{x})$, $\{j,k\} \in D_\sigma(\vec{x})$.
III.1.б) $\{i,j\} \notin D_\sigma(\vec{x})$, $\{i,k\} \in D_\sigma(\vec{x})$, $\{j,k\} \notin D_\sigma(\vec{x})$.

III.1.в) $\{i,j\} \in D_\sigma(\vec{x})$, $\{i,k\} \notin D_\sigma(\vec{x})$, $\{j,k\} \notin D_\sigma(\vec{x})$.
III.1.г) $\{i,j\} \in D_\sigma(\vec{x})$, $\{i,k\} \in D_\sigma(\vec{x})$, $\{j,k\} \in D_\sigma(\vec{x})$.

В случае III.1 для σ_1 выполняются соотношения

$$\{i,j\} \in D_{\sigma_1}(\vec{0}), \quad \{i,k\} \in D_{\sigma_1}(\vec{0}), \quad \{j,k\} \in D_{\sigma_1}(\vec{0}).$$

В случае III.1.а) $x_j = x_k = 1$, поэтому

$$\{i,j\} \notin D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \notin D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \in D_{\sigma_1}(\vec{x}').$$

Тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными.

В случае III.1.б) $x_j = 1$, $x_k = 0$, поэтому

$$\{i,j\} \notin D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \in D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \in D_{\sigma_1}(\vec{x}').$$

Эти соотношения противоречат условиям. Случай III.1.б) невозможен.

В случае III.1.в) $x_j = 0$, $x_k = 1$, поэтому

$$\{i,j\} \in D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \notin D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \notin D_{\sigma_1}(\vec{x}').$$

Тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными.

В случае III.1.г) $x_j = x_k = 0$, поэтому

$$\{i,j\} \in D_{\sigma_1}(\vec{x}'), \quad \{i,k\} \in D_{\sigma_1}(\vec{x}'), \quad \{j,k\} \in D_{\sigma_1}(\vec{x}').$$

Тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными.

Точно так же рассматриваются и все другие подслучаи случая III.

Во всех рассмотренных случаях для любых $i,j,k \in \Omega_n$ тройки (x'_i, x'_j, x'_k) и $(0,0,0)$ являются согласованными для σ_1. По предположению индукции $D_{\sigma_1}(\vec{x}')$ является носителем σ_1-кортежа, следовательно, и $D_\sigma(\vec{x})$ является носителем σ-кортежа. Лемма доказана. □

Рассмотрим более подробно условия, при которых $D_\sigma(\vec{x})$ является множеством обобщённых инверсий нижней строки подстановки σ.

Для любой подстановки $\sigma \in \mathrm{S}_n$ и каждых трёх символов $i,j,k \in \Omega_n$ построим булеву функцию $f^\sigma_{i,j,k}$ от переменных x_i, x_j, x_k следующим образом:

$$f^\sigma_{i,j,k}(x_i,x_j,x_k) = \\ = \begin{cases} 1, & \text{если } (x_i,x_j,x_k) \text{ и } (0,0,0) \text{ являются согласованными для } \sigma, \\ 0 & \text{в противном случае.} \end{cases}$$

Непосредственно из леммы 5 вытекает лемма 6.

Лемма 6. *Для любой подстановки $\sigma \in \mathrm{S}_n$ и вектора меток $\vec{x} \in \{0,1\}^n$ в σ множество $D_\sigma(\vec{x})$ является множеством обобщённых инверсий нижней строки σ тогда и только тогда, когда $\vec{x}$ удовлетворяет системе уравнений*

$$\begin{cases} f^\sigma_{i,j,k}(x_i,x_j,x_k) = 1, \\ \{i,j,k\} \in \bar{\Omega}^3_n, \end{cases} \tag{3}$$

где $\bar{\Omega}^3_n$ — множество неупорядоченных троек различных символов из Ω_n.

Получим явный вид системы уравнений (3). Для этого заметим, что для любой подстановки $\sigma \in \mathrm{S}_n$ и любых $i, j, k \in \Omega_n$ выполняется лишь одно из следующих соотношений:

1) $[i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}} \subseteq [k\sigma, k]_{\vec{0}}$;
2) $[i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$, $[i\sigma, i]_{\vec{0}} \subseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$, $k \in \{j+1, j+2, \ldots, i-1\}$;
3) $[i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$, $[i\sigma, i]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [i\sigma, i]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [j\sigma, j]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$;
4) $[i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$, $[i\sigma, i]_{\vec{0}} \nsubseteq [k\sigma, k]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}} \nsubseteq [i\sigma, i]_{\vec{0}}$;
5) ни одно из множеств $[i\sigma, i]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}}$, $[k\sigma, k]_{\vec{0}}$ не содержит другого.

Лемма 7. *Для любой подстановки $\sigma \in \mathrm{S}_n$ и любых различных символов $i, j, k \in \Omega_n$ функция $f^{\sigma}_{i,j,k}(x_i, x_j, x_k)$ имеет вид*

$$f^{\sigma}_{i,j,k}(x_i, x_j, x_k) = \begin{cases} x_i \cdot x_j \oplus x_i \cdot x_k \oplus x_j \cdot x_k \oplus x_j \oplus 1 & \text{в случае 1)}, \\ x_i \cdot x_j \oplus x_i \cdot x_k \oplus 1 & \text{в случае 2)}, \\ x_i \cdot x_j \oplus x_i \oplus 1 & \text{в случае 3)}, \\ x_i \cdot x_j \oplus x_j \cdot x_k \oplus x_i \oplus x_k \oplus 1 & \text{в случае 4)}, \\ 1 & \text{в случае 5)}. \end{cases}$$

Для доказательства нужно лишь, исходя из определения, построить $f^{\sigma}_{i,j,k}$ в каждом из случаев 1)—5). Например, табличное задание функции $f^{\sigma}_{i,j,k}$ в случае 1) имеет вид

(x_i, x_j, x_k)	$\{i, j\}$	$\{i, k\}$	$\{j, k\}$	Значение
000	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	1
001	$\in D_\sigma(\vec{x})$	$\notin D_\sigma(\vec{x})$	$\notin D_\sigma(\vec{x})$	1
010	$\notin D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	0
011	$\notin D_\sigma(\vec{x})$	$\notin D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	1
100	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	1
101	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	$\notin D_\sigma(\vec{x})$	0
110	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	1
111	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	$\in D_\sigma(\vec{x})$	1

Отсюда получаем многочлен Жегалкина:

$$f^{\sigma}_{i,j,k}(x_i, x_j, x_k) = x_i \cdot x_j \oplus x_i \cdot x_k \oplus x_j \cdot x_k \oplus x_j \oplus 1.$$

Точно так же поступаем и в остальных случаях.

Лемма 8. *Для любой подстановки $\sigma \in \mathrm{S}_n$ и любых различных символов $i, j, k \in \Omega_n$ функция $\bar{f}^{\sigma}_{i,j,k}$ является суммой форм $x_\alpha \cdot x_\beta \oplus x_\alpha$, где $\bar{f}$ — отрицание f, $\alpha, \beta \in \{i, j, k\}$, причём $x_\alpha \cdot x_\beta \oplus x_\alpha$ входит слагаемым в $\bar{f}^{\sigma}_{i,j,k}$ тогда и только тогда, когда выполняется одно из следующих условий*:

1) $\alpha \leqslant \alpha\sigma^{-1} < \beta\sigma^{-1} < \beta$;

2) $\beta < \alpha \leqslant \alpha\sigma^{-1} < \beta\sigma^{-1}$;
3) $\alpha\sigma^{-1} < \beta\sigma^{-1} < \beta < \alpha$;
4) $\beta\sigma^{-1} < \beta < \alpha \leqslant \alpha\sigma^{-1}$.

Доказательство. Ясно, что $\{\alpha, \beta\} \in D_\sigma(\vec{0})$ и $[\alpha\sigma, \alpha]_{\vec{0}} \subseteq [\beta\sigma, \beta]_{\vec{0}}$ тогда и только тогда, когда выполняется одно из условий 1)—4). Остаётся проверить, что функция $\bar{f}^\sigma_{i,j,k}$, составленная по правилу, указанному в формулировке, совпадает с функцией $\bar{f}^\sigma_{i,j,k}$, указанной в лемме 7. □

Вид системы уравнений (3) можно упростить. Для этого рассмотрим следующую систему, состоящую из $|D_\sigma(\vec{0})|$ уравнений:

$$\begin{cases} x_i \cdot \bar{x}_j = 0, \\ \{i, j\} \in D_\sigma(\vec{0}),\ [i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}. \end{cases} \tag{4}$$

Теорема 9. *Для любой подстановки $\sigma \in \mathrm{S}_n$ и вектора меток $\vec{x} \in \{0,1\}^n$ в σ множество $D_\sigma(\vec{x})$ является множеством обобщённых инверсий нижней строки σ тогда и только тогда, когда $\vec{x}$ удовлетворяет системе уравнений* (4).

Доказательство. Покажем, что системы уравнений (3) и (4) равносильны.

Из лемм 7 и 8 следует, что любое уравнение системы (3) является суммой некоторых уравнений системы (4). Покажем, что каждое уравнение системы (4) содержится среди уравнений системы (3). Для этого, согласно лемме 7, надо показать, что если $[i\sigma, i]_{\vec{0}} \subseteq [j\sigma, j]_{\vec{0}}$, то найдётся такое $k \in \Omega_n$, что множество $[k\sigma, k]_{\vec{0}}$ не содержит множеств $[i\sigma, i]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}}$ и не содержится в них.

Пусть

$$i\sigma^{-1} = r, \quad j\sigma^{-1} = s,$$
$$\Delta_1 = \{i+1, i+2, \ldots, s\}, \quad \Delta_2 = \{(i+1)\sigma, (i+2)\sigma, \ldots, (s-1)\sigma\}.$$

Если $s = i+1$, то $\Delta_1 = \{i+1\}$, $\Delta_2 = \varnothing$. Поскольку $|\Delta_1| > |\Delta_2|$, найдётся $k \in \Delta_1 \setminus \Delta_2$. Легко проверить, что для такого k множество $[k\sigma, k]_{\vec{0}}$ не содержит множеств $[i\sigma, i]_{\vec{0}}$, $[j\sigma, j]_{\vec{0}}$ и не содержится в них. □

Теорема 10. *Для любой подстановки $\sigma \in \mathrm{S}_n$ класс носителей σ-кортежей без кратных пар совпадает с объединением классов всех множеств обобщённых инверсий нижних строк подстановок $g^k \cdot \sigma$ по всем $k \in \Omega_n$.*

Доказательство. Покажем, что для любого σ-кортежа A_σ без кратных пар найдутся $k \in \Omega_n$ и решение $\vec{x}$ системы уравнений (4) применительно к подстановке $g^k \cdot \sigma$, такие что $\tilde{A}_\sigma = D_{g^k \cdot \sigma}(\vec{x})$. Проведём индукцию по $r = |\tilde{A}_\sigma|$.

Как показано в [3, теорема 2.2], в случае когда $r = 0$, найдётся $t \in \Omega_n$, для которого $\sigma = g^t$. Тогда $\tilde{A}_\sigma = D_\sigma(\vec{0})$. Предположим, что утверждение верно, если $r \leqslant m$.

Пусть σ — подстановка и $A_\sigma = (\{\alpha, \beta\}, \ldots)$ — её кортеж с носителем $\tilde{A}_\sigma$, $|\tilde{A}_\sigma| = m+1$. Пусть $i\sigma = \alpha$, $(i+1)\sigma = \beta$ и $\sigma_1 = (i, i+1) \cdot \sigma$. Тогда $\tilde{A}_{\sigma_1} = \tilde{A}_\sigma \setminus \{\alpha, \beta\}$ является носителем σ_1-кортежа, и по предположению индукции

найдётся $s \in \Omega_n$, для которого $\tilde{A}_{\sigma_1} = D_{g^s \cdot \sigma_1}(\vec{x})$, причём $\vec{x}$ является решением системы уравнений (4) применительно к подстановке $\sigma_2 = g^s \cdot \sigma_1$. Пусть $j\sigma_2 = \beta$, $(j+1)\sigma_2 = \alpha$ и $\Delta = \{j, j+1\} \cap \{\alpha, \beta\}$. Рассмотрим ряд случаев.

I. Пусть $\Delta = \varnothing$. Возможны следующие подслучаи.

I.1. $\{\alpha, \beta\} \in D_{\sigma_2}(\vec{0})$.

I.2. $\{\alpha, \beta\} \notin D_{\sigma_2}(\vec{0})$.

Из условия случая I.1 следует, что система уравнений (4) применительно к σ_2 содержит уравнение $x_\beta \cdot \bar{x}_\alpha = 0$, причём x_α и x_β удовлетворяют этому уравнению. Поэтому могут иметь место следующие три случая:

I.1.а) $x_\alpha = x_\beta = 1$;

I.1.б) $x_\alpha = 1$, $x_\beta = 0$;

I.1.в) $x_\alpha = x_\beta = 0$.

На самом деле случаи I.1.а) и I.1.в) невозможны, поскольку в их условиях $\{\alpha, \beta\} \in D_{\sigma_2}(\vec{x})$, что противоречит тому, что A_σ не содержит кратных пар. Остаётся случай I.1.б). В этом случае для подстановки $\sigma_2' = (j, j+1) \cdot \sigma_2$ и вектора меток $\vec{x}$ выполняется равенство

$$D_{\sigma_2'}(\vec{x}) = D_{\sigma_2}(\vec{x}) \cup \{\alpha, \beta\}, \tag{5}$$

причём $\vec{x}$ удовлетворяет системе уравнений (4) применительно к подстановке $\sigma_2' = g^s \cdot \sigma$. Последнее следует из того, что в рассматриваемых условиях система (4) применительно к σ_2 отличается от системы (4) применительно к σ_2' лишь тем, что первая содержит уравнение $x_\beta \cdot \bar{x}_\alpha = 0$, а вторая нет. Поэтому если из системы изъять одно уравнение, то решение исходной системы останется решением и меньшей системы. Мы доказали утверждение в случае I.1.

В случае I.2 из условия $\{\alpha, \beta\} \notin D_{\sigma_2}(\vec{x})$ следует, что возможны лишь два варианта:

I.2.а) $x_\alpha = x_\beta = 0$;

I.2.б) $x_\alpha = x_\beta = 1$.

В случае I.2.а) для подстановки $\sigma_2' = g^s \cdot \sigma$ выполняется равенство (5), причём система уравнений (4) применительно к σ_2 отличается от системы уравнений (4) применительно к σ_2' лишь тем, что к первой системе добавляется уравнение $x_\beta \cdot \bar{x}_\alpha = 0$, которому x_α и x_β удовлетворяют. В этом случае утверждение также доказано.

Совершенно аналогично обстоит дело и в случае I.2.б). При этом рассматриваемые значения $x_\alpha = x_\beta = 1$ также удовлетворяют уравнению $x_\beta \cdot \bar{x}_\alpha = 0$.

II. Пусть $|\Delta| = 1$, причём $j = \beta$, $(j+1)\sigma_2 \neq j+1$.

В этом случае $\{\alpha, \beta\} \in D_{\sigma_2}(\vec{0})$ и $\{\alpha, \beta\} \notin D_{\sigma_2}(\vec{x})$. Легко проверить, что этим условиям удовлетворяют лишь $x_\alpha = 1$ и $x_\beta = 0$. Требуемое утверждение следует из тех же рассуждений, что и в случае I.1.

III. Пусть $|\Delta| = 1$, причём $j+1 = \alpha$, $j\sigma_2 \neq j$.

В этом случае $x_\alpha = 0$, и поскольку $\{\alpha, \beta\} \notin D_{\sigma_2}(\vec{x})$, то $x_\beta = 0$. Отсюда следует, что $\{\alpha, \beta\} \notin D_{\sigma_2}(\vec{0})$. Рассмотрим подстановку $\sigma_2' = (j, j+1) \cdot \sigma_2$ и

вектор меток $\vec{x}'$, который отличается от $\vec{x}$ лишь тем, что $x'_\alpha = 1$ (напомним, что $x'_\alpha = 0$).

Заметим, что системы уравнений (4) применительно к подстановкам σ_2 и σ'_2 имеют единственное отличие: если $x_\alpha \cdot \bar{x}_{\gamma_1} = 0, \ldots, x_\alpha \cdot \bar{x}_{\gamma_k} = 0$ — все уравнения системы для σ_2, содержащие x_α, то $\bar{x}_\alpha \cdot x_\gamma = 0$, $\gamma \in \Omega_n \setminus \{\gamma_1, \ldots, \gamma_k, \beta\}$ — все уравнения системы для σ'_2, содержащие x_α. Поэтому если $x_\alpha = x_\beta = 0$ удовлетворяют системе для σ_2, то $x_\alpha = 1$, $x_\beta = 0$ удовлетворяют системе для σ'_2. Отсюда следует утверждение в случае III.

IV. $\beta = j + 1$, $\alpha = j$.

Очевидно, что в этом случае $x_\alpha = x_\beta$, так как иначе $\{\alpha, \beta\} \in D_{\sigma_2}(\vec{x})$.

Обратим внимание на то, что в рассматриваемом случае в нижней строке подстановки $\sigma'_2 = (j, j+1) \cdot \sigma_2$ символы α и β расположены «на своих местах». В силу того что множество $\tilde{A}_{\sigma_2} = \tilde{A}_\sigma \setminus \{\alpha, \beta\}$ не содержит кратных пар и является носителем σ_2-кортежа, символы α и β вновь могут оказаться «на своих местах» в нижней строке подстановки $\bar{\Theta}(A_{\sigma_2}) = g^r$, $r \in \Omega_n$, лишь тогда, когда выполняется равенство

$$\{\gamma \in \Omega_n \colon \{\alpha, \gamma\} \in \tilde{A}_\sigma\} \cup \{\delta \in \Omega_n \colon \{\beta, \gamma\} \in \tilde{A}_\sigma\} = \Omega_n.$$

Заметим также, что при этом ни для одного $k \in \Omega_n$ невозможно одновременное включение $\{\alpha, k\}, \{\beta, k\} \in \tilde{A}_\sigma$. В самом деле, если $x_\alpha = x_\beta = 0$, то $\{\alpha, k\}, \{\beta, k\} \in \tilde{A}_\sigma$ лишь тогда, когда $x_k = 1$, причём в системе уравнений (4) применительно к σ_2 содержится уравнение $x_k \cdot \bar{x}_\alpha = 0$. Но это невозможно, так как x_k и x_α не удовлетворяют этому уравнению, что противоречит предположению индукции. К аналогичному выводу приходим и в случае, когда $x_\alpha = x_\beta = 1$.

Пусть $x_\alpha = x_\beta = 0$. Рассмотрим тогда подстановку $\sigma_3 = g \cdot \sigma_2$ и её вектор меток $\vec{x}'$, который отличается от $\vec{x}$ лишь тем, что символы k, такие что $k\sigma_2 = k$ (и поэтому имеющие метки $x_k = 0$), получают метки $x'_k = 1$. Заметим, что в рассматриваемых условиях не существует такого t, для которого $(t+1)\sigma_2 = t$, причём $x_t = 1$. В этом случае мы получаем включения $\{\alpha, t\}, \{\beta, t\} \in D_{\sigma_2}(\vec{x})$, которые противоречат сказанному выше. Пользуясь теперь определением множества $D_\sigma(\vec{x})$, убеждаемся в справедливости равенства $D_{\sigma_2}(\vec{x}) = D_{\sigma_3}(\vec{x}')$. Убедимся также в том, что вектор меток $\vec{x}'$ удовлетворяет системе уравнений (4) применительно к подстановке σ_3.

Рассмотрим пары символов $t, k \in \Omega_n$, такие что $t\sigma_2 \neq t$, $k\sigma_2 \neq k$. Тогда $x'_t = x_t$, $x'_k = x_k$ и

$$\{t, k\} \in D_{\sigma_2}(\vec{0}) \iff \{t, k\} \in D_{\sigma_3}(\vec{0}).$$

Поэтому множества уравнений систем (4) для σ_2 и σ_3, в которых встречаются лишь такие переменные x_t и x_k, одинаковы. Пусть теперь для некоторого $k \in \Omega_n$ выполняется равенство $k\sigma_2 = k$. Если уравнение системы (4) для σ_2 (для σ_3) содержит переменную x_k, то это уравнение имеет вид $x_k \cdot \bar{x}_t = 0$ (соответственно $\bar{x}_k \cdot x_s = 0$). Поэтому если $\vec{x}$ удовлетворяет системе (4) для σ_2, то $\vec{x}'$ удовлетворяет системе (4) для σ_3.

Рассмотрим подстановку $\sigma_3' = (j, j+1) \cdot \sigma_3$ и её вектор меток $\vec{x}''$, который отличается от $\vec{x}'$ лишь тем, что $x_j'' = 1$. Легко убедиться в том, что выполняются равенства

$$D_{\sigma_3'}(\vec{x}'') = D_{\sigma_3}(\vec{x}') \cup \{\alpha, \beta\} = D_{\sigma_2}(\vec{x}) \cup \{\alpha, \beta\} = \tilde{A}_\sigma.$$

Кроме того, $\vec{x}''$ удовлетворяет системе (4) применительно к подстановке σ_3'. Это следует из того, что если уравнение системы для σ_3 содержит переменную x_j, то это уравнение имеет вид $x_j \cdot \bar{x}_t = 0$. Если же уравнение системы для σ_3' содержит переменную x_j, то это уравнение имеет вид $\bar{x}_j \cdot x_k = 0$.

Рассмотренные случаи I—IV исчерпывают все возможные случаи расположения символов α и β в нижней строке подстановки σ_2. В каждом из этих случаев мы реализовали множество $\tilde{A}_\sigma$ как множество обобщённых инверсий $D_{g^k \cdot \sigma}(\vec{x})$ нижней строки подстановки $g^k \cdot \sigma$ для подходящего $k \in \Omega_n$. На этом доказательство теоремы закончено. □

Выясним, сколько различных множеств обобщённых инверсий даёт система уравнений (4). Непосредственно из определения множества $D_\sigma(\vec{x})$ вытекает следующая лемма.

Лемма 11. *Справедливо равенство*

$$D_\sigma(\vec{x}) = \big\{\{i,j\}\colon \text{либо } \{i,j\} \in D_\sigma(\vec{0}) \text{ и } x_i = x_j, \text{ либо } \{i,j\} \notin D_\sigma(\vec{0}) \text{ и } x_i = \bar{x}_j\big\}.$$

Лемма 12. *Если $D_\sigma(\vec{x}_1) = D_\sigma(\vec{x}_2)$, где $\vec{x}_1$, $\vec{x}_2$ — решения системы уравнений* (4)*, то $\vec{x}_1 \oplus \vec{x}_2 = \vec{1}$.*

Достаточно заметить, что если

$$\vec{x}_1 = (\ldots, x_i, \ldots, x_j, \ldots), \quad \vec{x}_2 = (\ldots, x_i, \ldots, \bar{x}_j, \ldots),$$

то $D_\sigma(\vec{x}_1) \neq D_\sigma(\vec{x}_2)$. Последнее соотношение следует из леммы 11.

Заметим, что $x_i^{(0)}$ и $x_j^{(0)}$ из $\{0,1\}$ удовлетворяют уравнению $x_i \cdot \bar{x}_j = 0$ тогда и только тогда, когда $x_i^{(0)} \leqslant x_j^{(0)}$. Система уравнений (4) индуцирует отношение ε частичного порядка на Ω_n: $i \varepsilon j$ тогда и только тогда, когда уравнение $x_i \cdot \bar{x}_j = 0$ входит в (4). Пусть Γ_σ — ориентированный граф отношения ε, $P(\sigma)$ — число решений системы (4), $K(\sigma)$ — число компонент связности графа Γ_σ, $N(\sigma)$ — число множеств обобщённых инверсий $D_\sigma(\vec{x})$ нижней строки подстановки σ, для которых $\vec{x}$ удовлетворяет системе уравнений (4).

Теорема 13. *Для любой подстановки $\sigma \in \mathrm{S}_n$ выполняется равенство*

$$N(\sigma) = \begin{cases} P(\sigma), & \text{если найдётся } i \in \Omega_n, \text{ для которого } i\sigma = i, \\ P(\sigma) - 2^{K(\sigma)-1}, & \text{если } i\sigma \neq i \text{ для всех } i \in \Omega_n. \end{cases} \tag{6}$$

Доказательство. Пары чисел $x_i^{(0)}$, $x_j^{(0)}$ и $\bar{x}_i^{(0)}$, $\bar{x}_j^{(0)}$ из $\{0,1\}$ одновременно удовлетворяют уравнению $x_i \cdot \bar{x}_j = 0$ тогда и только тогда, когда $x_i^{(0)} = x_j^{(0)}$. Поэтому если решения $\vec{x}_1$ и $\vec{x}_2$ системы уравнений (4) удовлетворяют условию

$\vec{x}_1 \oplus \vec{x}_2 = \vec{1}$, то координаты вектора $\vec{x}_k$, $k = 1, 2$, входящие в компоненту связности графа Γ_σ, совпадают друг с другом. Метка единичного цикла может быть равной лишь 0. Поэтому из лемм 11 и 12 следует (6). □

Теорема 13 позволяет вычислять общее число носителей кортежей без кратных пар для некоторых подстановок. Пусть, например, $\sigma = g^k$, $k \in \Omega_n$. Для этой подстановки система (4) состоит из пустого множества уравнений, и следовательно, любой вектор $\vec{x} \in \{0,1\}^n$ является её решением. Тогда согласно теореме 13 $P(g^k) = 2^n$, $K(g^k) = n$, и с учётом леммы 12 число множеств обобщённых инверсий нижней строки подстановки σ равно 2^{n-1}. Теперь заметим, что для любого $\vec{x} \in \{0,1\}^n$ и любых i и j из $\Omega_n \setminus \{0\}$ выполняется равенство $D_{g^i}(\vec{x}) = D_{g^j}(\vec{x})$. Отсюда и из теоремы 10 следует, что число носителей кортежей без кратных пар подстановки σ равно 2^{n-1}.

4. Пример

Решим уравнение

$$g^{y_1} \cdot h \cdot g^{y_2} \cdot h \cdot \ldots \cdot g^{y_6} \cdot h \cdot g^{y_7} = (0)(1,5)(2,4)(3) \tag{7}$$

в группе S_6.

I. Найдём множество носителей всех σ-кортежей длины 6, где

$$\sigma = (0)(1,5)(2,4)(3).$$

Для этого построим все множества обобщённых инверсий нижних строк подстановок $g^k \cdot \sigma$, $k \in \Omega_6$.

1. Согласно теореме 9 все множества обобщённых инверсий нижней строки подстановки σ исчерпываются множествами вида $D_\sigma(\vec{x})$, где вектор меток $\vec{x}$ является решением системы уравнений (4). Для подстановки σ система (4) имеет вид

$$\begin{cases} x_0 \cdot \bar{x}_4 = 0, \\ x_0 \cdot \bar{x}_5 = 0, \\ \bar{x}_1 \cdot x_2 = 0, \\ \bar{x}_1 \cdot x_3 = 0, \\ \bar{x}_2 \cdot x_3 = 0, \\ \bar{x}_4 \cdot x_5 = 0, \end{cases} \tag{8}$$

где $x_i \in \{0,1\}$, $i = 0, 1, \ldots, 5$, причём $x_j = 0$, если $j\sigma = j$. Решения системы (8), а также соответствующие множества $D_\sigma(\vec{x})$ сведём в табл. 1.

2. Непосредственно проверяется, что для подстановок $g^2 \cdot \sigma$ и $g^4 \cdot \sigma$ (имеющих единичные циклы) картина полностью аналогичная. Нижние строки этих подстановок имеют по 9 множеств обобщённых инверсий тех же мощностей, что и указанные в табл. 1, причём множества мощности 6 совпадают для σ, $g^2 \cdot \sigma$ и

Таблица 1

	x_0	x_1	x_2	x_3	x_4	x_5	$D_\sigma(x_0,x_1,x_2,x_3,x_4,x_5)$	$\lvert D_\sigma(\vec{x})\rvert$
1	0	0	0	0	0	0	$\{0,1\}$, $\{0,5\}$, $\{1,5\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$	6
2	0	0	0	0	0	1	$\{0,1\}$, $\{2,3\}$, $\{2,4\}$, $\{2,5\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$	7
3	0	0	1	0	0	0	$\{0,1\}$, $\{0,2\}$, $\{0,5\}$, $\{1,2\}$, $\{1,5\}$, $\{2,5\}$, $\{3,4\}$	7
4	0	0	1	0	0	1	$\{0,1\}$, $\{0,2\}$, $\{1,2\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$	6
5	0	0	1	1	0	0	$\{0,1\}$, $\{0,2\}$, $\{0,3\}$, $\{0,5\}$, $\{1,2\}$, $\{1,3\}$, $\{1,5\}$, $\{2,3\}$, $\{2,5\}$, $\{3,5\}$	10
6	0	0	1	1	0	1	$\{0,1\}$, $\{0,2\}$, $\{0,3\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{4,5\}$	7
7	1	0	0	0	0	1	$\{0,2\}$, $\{0,3\}$, $\{0,4\}$, $\{0,5\}$, $\{2,3\}$, $\{2,4\}$, $\{2,5\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$	10
8	1	0	1	0	0	1	$\{0,3\}$, $\{0,4\}$, $\{0,5\}$, $\{1,2\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$	7
9	1	0	1	1	0	1	$\{0,4\}$, $\{0,5\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{4,5\}$	6

$g^4\cdot\sigma$. Кроме того, состав множеств обобщённых инверсий нижних строк остальных подстановок $g^k\cdot\sigma$ совпадает с составом множеств обобщённых инверсий для одной из рассмотренных трёх перестановок. Отсюда следует, что σ-кортежи, соответствующие решениям уравнения (7), имеют один из трёх возможных носителей:

$$\{0,1\},\ \{0,5\},\ \{1,5\},\ \{2,3\},\ \{2,4\},\ \{3,4\},$$
$$\{0,1\},\ \{0,2\},\ \{1,2\},\ \{3,4\},\ \{3,5\},\ \{4,5\},$$
$$\{0,4\},\ \{0,5\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{4,5\}.$$

3. Остаётся применить для этих носителей алгоритм 1 для построения множества типов соответствующих σ-кортежей, дающих решения уравнения. Непосредственно проверяется, что каждый из указанных носителей даёт 80 различных σ-кортежей. Поэтому общее число решений уравнения (7) равно 240. Заметим, что все эти решения можно получить из 80 решений, которые даёт лишь один носитель $D_\sigma(\vec{0})$. Для этого нужно домножить каждое произведение в (7) слева и справа на g или g^{-1}. Это следует из очевидных соотношений $g\cdot\sigma\cdot g=\sigma$ и $g^{-1}\cdot\sigma\cdot g^{-1}=\sigma$.

4. Все решения y_1, y_2, y_3, y_4, y_5, y_6, y_7 уравнения (7) сведём в табл. 2 в лексикографическом порядке.

Таблица 2

	y_1	y_2	y_3	y_4	y_5	y_6	y_7		y_1	y_2	y_3	y_4	y_5	y_6	y_7		y_1	y_2	y_3	y_4	y_5	y_6	y_7
1	0	1	2	1	2	3	3	2	0	1	2	1	5	3	0	3	0	1	2	3	4	5	3
4	0	1	3	2	3	1	2	5	0	1	3	5	1	2	0	6	0	1	3	5	3	4	2
7	0	1	5	3	1	5	3	8	0	1	5	4	5	1	2	9	0	2	1	2	1	2	2
10	0	2	1	2	3	4	4	11	0	2	1	5	3	1	4	12	0	2	3	1	3	5	2
13	0	2	3	4	3	2	2	14	0	2	3	4	5	4	4	15	0	3	1	3	2	3	0
16	0	3	1	3	2	3	3	17	0	3	1	5	4	5	0	18	0	3	2	1	2	1	1
19	0	3	2	3	1	3	4	20	0	3	2	3	4	3	1	21	0	3	4	3	2	3	3
22	0	3	4	3	5	3	0	23	0	3	4	5	4	5	0	24	0	3	5	1	2	1	4
25	0	3	5	3	1	3	1	26	0	3	5	3	4	3	4	27	0	4	3	2	1	2	0
28	0	4	3	2	3	4	2	29	0	4	3	5	3	1	2	30	0	4	5	1	3	5	0
31	0	4	5	4	3	2	0	32	0	4	5	4	5	4	2	33	0	5	1	2	1	5	2
34	0	5	1	3	5	1	1	35	0	5	3	1	3	2	2	36	0	5	3	1	5	4	4
37	0	5	3	4	3	5	1	38	0	5	4	3	2	1	1	39	0	5	4	5	1	3	4
40	0	5	4	5	4	3	1	41	1	1	2	1	2	3	4	42	1	1	2	1	5	3	1
43	1	1	2	3	4	5	4	44	1	1	3	2	3	1	3	45	1	1	3	5	1	2	1
46	1	1	3	5	3	4	3	47	1	1	5	3	1	5	4	48	1	1	5	4	5	1	3
49	1	2	1	2	1	2	3	50	1	2	1	2	3	4	5	51	1	2	1	5	3	1	5
52	1	2	3	1	3	5	3	53	1	2	3	4	3	2	3	54	1	2	3	4	5	4	5
55	1	3	1	3	2	3	1	56	1	3	1	3	5	3	4	57	1	3	1	5	4	5	1
58	1	3	2	1	2	1	2	59	1	3	2	3	1	3	5	60	1	3	2	3	4	3	2
61	1	3	4	3	2	3	4	62	1	3	4	3	5	3	1	63	1	3	4	5	4	5	4
64	1	3	5	1	2	1	5	65	1	3	5	3	1	3	2	66	1	3	5	3	4	3	5
67	1	4	3	2	1	2	1	68	1	4	3	2	3	4	3	69	1	4	3	5	3	1	3
70	1	4	5	1	3	5	1	71	1	4	5	4	3	2	1	72	1	4	5	4	5	4	3
73	1	5	1	2	1	5	3	74	1	5	1	3	5	1	2	75	1	5	3	1	3	2	3
76	1	5	3	1	5	4	5	77	1	5	3	4	3	5	2	78	1	5	4	3	2	1	2
79	1	5	4	5	1	3	5	80	1	5	4	5	4	3	2	81	2	1	2	1	2	3	5
82	2	1	2	1	5	3	2	83	2	1	2	3	4	5	5	84	2	1	3	2	3	1	4
85	2	1	3	5	1	2	2	86	2	1	3	5	3	4	4	87	2	1	5	3	1	5	5
88	2	1	5	4	5	1	4	89	2	2	1	2	1	2	4	90	2	2	1	2	3	4	0
91	2	2	1	5	3	1	0	92	2	2	3	1	3	5	4	93	2	2	3	4	3	2	4
94	2	2	3	4	5	4	0	95	2	3	1	3	2	3	2	96	2	3	1	3	5	3	5
97	2	3	1	5	4	5	2	98	2	3	2	1	2	1	3	99	2	3	2	3	1	3	0
100	2	3	2	3	4	3	3	101	2	3	4	3	2	3	5	102	2	3	4	3	5	3	2
103	2	3	4	5	4	5	5	104	2	3	5	1	2	1	0	105	2	3	5	3	1	3	0
106	2	3	5	3	4	3	0	107	2	4	3	2	1	2	2	108	2	4	3	2	3	4	4
109	2	4	3	5	3	1	4	110	2	4	5	1	3	5	2	111	2	4	5	4	3	2	2

	y_1	y_2	y_3	y_4	y_5	y_6	y_7		y_1	y_2	y_3	y_4	y_5	y_6	y_7		y_1	y_2	y_3	y_4	y_5	y_6	y_7
112	2	4	5	4	5	4	4	113	2	5	1	2	1	5	4	114	2	5	1	3	5	1	3
115	2	5	3	1	3	2	4	116	2	5	3	1	5	4	0	117	2	5	3	4	3	5	4
118	2	5	4	3	2	1	3	119	2	5	4	5	1	3	0	120	2	5	4	5	4	3	3
121	3	1	2	1	2	3	0	122	3	1	2	1	5	3	3	123	3	1	2	3	4	5	0
124	3	1	3	2	3	1	5	125	3	1	3	5	1	2	3	126	3	1	3	5	3	4	5
127	3	1	5	3	1	5	0	128	3	1	5	4	5	1	5	129	3	2	1	2	3	4	1
130	3	2	1	2	1	2	5	131	3	2	1	5	3	1	1	132	3	2	3	1	3	5	5
133	3	2	3	4	3	2	5	134	3	2	3	4	5	4	1	135	3	3	1	3	2	3	3
136	3	3	1	3	5	3	0	137	3	3	1	5	4	5	3	138	3	3	2	1	2	1	4
139	3	3	2	3	1	3	1	140	3	3	2	3	4	3	4	141	3	3	4	3	2	3	0
142	3	3	4	3	5	3	3	143	3	3	4	5	4	5	0	144	3	3	5	1	2	1	1
145	3	3	5	3	1	3	1	146	3	3	5	3	4	3	1	147	3	4	3	2	1	2	3
148	3	4	3	2	3	4	5	149	3	4	3	5	3	1	5	150	3	4	5	1	3	5	3
151	3	4	5	4	3	2	3	152	3	4	5	4	5	4	5	153	3	5	1	2	1	5	5
154	3	5	1	3	5	1	4	155	3	5	3	1	3	2	5	156	3	5	3	1	5	4	1
157	3	5	3	4	3	5	5	158	3	5	4	3	2	1	4	159	3	5	4	5	1	3	1
160	3	5	4	5	4	3	4	161	4	1	2	1	2	3	1	162	4	1	2	1	5	3	4
163	4	1	2	3	4	5	1	164	4	1	3	2	3	1	0	165	4	1	3	5	1	2	4
166	4	1	3	5	3	4	0	167	4	1	5	3	1	5	2	168	4	1	5	4	5	1	0
169	4	2	1	2	1	2	0	170	4	2	1	2	3	4	2	171	4	2	1	5	3	1	2
172	4	2	3	1	3	5	0	173	4	2	3	4	3	2	0	174	4	2	3	4	5	4	2
175	4	3	1	3	2	3	4	176	4	3	1	3	5	3	1	177	4	3	1	5	4	5	4
178	4	3	2	1	2	1	5	179	4	3	2	3	1	3	2	180	4	3	2	3	4	3	5
181	4	3	4	3	2	3	1	182	4	3	4	3	5	3	4	183	4	3	4	5	4	5	4
184	4	3	5	1	2	1	2	185	4	3	5	3	1	3	2	186	4	3	5	3	4	3	2
187	4	4	3	2	1	2	4	188	4	4	3	2	3	4	0	189	4	4	3	5	3	1	0
190	4	4	5	1	3	5	4	191	4	4	5	4	3	2	4	192	4	4	5	4	5	4	0
193	4	5	1	2	1	5	0	194	4	5	1	3	5	1	5	195	4	5	3	1	3	2	0
196	4	5	3	1	5	4	2	197	4	5	3	4	3	5	0	198	4	5	4	3	2	1	5
199	4	5	4	5	1	3	2	200	4	5	4	5	4	3	5	201	5	1	2	1	2	3	2
202	5	1	2	1	5	3	5	203	5	1	2	3	4	5	2	204	5	1	3	2	3	1	1
205	5	1	3	5	1	2	5	206	5	1	3	5	3	4	1	207	5	1	5	3	1	5	2
208	5	1	5	4	5	1	1	209	5	2	1	2	1	2	1	210	5	2	1	2	3	4	3
211	5	2	1	5	3	1	3	212	5	2	3	1	3	5	1	213	5	2	3	4	3	2	1
214	5	2	3	4	5	4	3	215	5	3	1	3	2	3	5	216	5	3	1	3	5	3	2
217	5	3	1	5	4	5	5	218	5	3	2	1	2	1	0	219	5	3	2	3	1	3	3
220	5	3	2	3	4	3	0	221	5	3	4	3	2	3	2	222	5	3	4	3	5	3	5
223	5	3	4	5	4	5	5	224	5	3	5	1	2	1	3	225	5	3	5	3	1	3	0
226	5	3	5	3	4	3	3	227	5	4	3	2	1	2	5	228	5	4	3	2	3	4	1

	y_1	y_2	y_3	y_4	y_5	y_6	y_7		y_1	y_2	y_3	y_4	y_5	y_6	y_7		y_1	y_2	y_3	y_4	y_5	y_6	y_7
229	5	4	3	5	3	1	1	230	5	4	5	1	3	5	5	231	5	4	5	4	3	2	5
232	5	4	5	4	5	4	1	233	5	5	1	2	1	5	1	234	5	5	1	3	5	1	0
235	5	5	3	1	3	2	1	236	5	5	3	1	5	4	3	237	5	5	3	4	3	5	0
238	5	5	4	3	2	1	0	239	5	5	4	5	1	3	3	240	5	5	4	5	4	3	0

Отметим, что приведённый пример был посчитан вручную, в то время как полный перебор предполагает проверку 6^7 вариантов векторов $(y_1, \ldots, y_7)$. Это требует выполнения $6^8 \cdot 13 \approx 2{,}2 \cdot 10^7$ операций нахождения образа символа по подстановке и не представляется возможным.

При увеличении l в (7) с 7 до 8 число решений уравнения с той же правой частью увеличивается до 588. Каждому решению уравнения отвечает носитель σ-кортежа длины 7. Нетрудно убедиться в том, что подстановка имеет лишь 6 таких носителей (табл. 3).

Таблица 3

$D_\sigma(0,0,1,0,0,0)$	$\{0,1\}$, $\{0,2\}$, $\{0,5\}$, $\{1,2\}$, $\{1,5\}$, $\{2,5\}$, $\{3,4\}$
$D_\sigma(0,0,0,0,0,1)$	$\{0,1\}$, $\{2,3\}$, $\{2,4\}$, $\{2,5\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$
$D_\sigma(0,0,1,1,0,1)$	$\{0,1\}$, $\{0,2\}$, $\{0,3\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{4,5\}$
$D_\sigma(1,0,1,0,0,1)$	$\{0,3\}$, $\{0,4\}$, $\{0,5\}$, $\{1,2\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$
$D_{g^4\cdot\sigma}(0,0,1,1,0,1)$	$\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$, $\{0,5\}$
$D_{g^2\cdot\sigma}(1,1,0,1,0,0)$	$\{0,1\}$, $\{1,4\}$, $\{1,5\}$, $\{0,4\}$, $\{0,5\}$, $\{4,5\}$, $\{2,3\}$

Применяя к этим носителям алгоритм 1, получаем все решения уравнения. Каждый из этих носителей даёт 98 решений.

При увеличении l до 9 каждому решению уравнения с той же правой частью отвечает носитель σ-кортежа длины 8. Поскольку носители σ-кортежей без кратных пар могут иметь длины 6, 7 или 10, любой носитель σ-кортежа длины 8 получается добавлением кратного вхождения некоторой пары к одному из трёх носителей длины 6. Таким образом, получается ровно 45 носителей длины 8. Непосредственно проверяется, что эти носители дают в общей сложности 10158 решений уравнения.

Эти примеры иллюстрируют порядок роста числа решений уравнения (1) с ростом l. Соответственно возрастает и трудоёмкость предложенного метода.

Сравнительно несложно выяснить, имеет ли уравнение (1) решения. Для этого достаточно найти величину

$$L = \min\{|D_{g^k\cdot\sigma}(\vec{0})| \colon k \in \Omega_n\}$$

и проверить, выполняется ли неравенство $L \leqslant l$ и содержится ли в множестве $\{D_{g^k\cdot\sigma}(\vec{0}) \colon k \in \Omega_n\}$ множество, мощность которого имеет ту же чётность, что

и l. Как показано в [3], вычисление величины L требует $O(n^3)$ операций типа сложения или сравнения чисел.

Автор выражает глубокую признательность М. М. Глухову за ряд ценных предложений и замечаний, высказанных при подготовке статьи.

Литература

[1] Глухов М. М., Зубов А. Ю. О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор) // Математические вопросы кибернетики. Вып. 8. — М.: Наука; Физматлит, 1999. — С. 5—32.

[2] Глухов М. М., Погорелов Б. А. О некоторых применениях групп в криптографии // Математика и безопасность информационных технологий. Материалы конференции. МГУ, 28—29 октября 2004 г. — М.: МЦНМО, 2005. — С. 19—31.

[3] Зубов А. Ю. О диаметре группы S_n относительно системы образующих, состоящей из полного цикла и транспозиции // Труды по дискретной математике. РАН, Академия криптографии РФ. Том 2. — М.: ТВП, 1998. — С. 112—150.