Об условиях k-транзитивности произведения регулярных групп подстановок

А. В. ТОКТАРЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: toktarev@gmail.com

УДК 512.542.72

Ключевые слова: произведение регулярных групп подстановок, кратная транзитивность.

Аннотация

В работе анализируется произведение m регулярных групп подстановок $G_1 \cdot \ldots \cdot G_m$, где $m \geqslant 2$ — натуральное число. Каждая из регулярных групп подстановок является подгруппой $\mathrm{S}(\Omega)$ — симметрической группы подстановок степени $|\Omega|$ для некоторого множества Ω. М. М. Глуховым доказано, что для $k = 2$ и $m = 2$, 2-транзитивность произведения $G_1 \cdot G_2$ эквивалентна отсутствию нулей в соответствующей квадратной матрице с количеством строк и столбцов, равным $|\Omega| - 1$. Также М. М. Глуховым приведены необходимые условия 2-транзитивности такого произведения регулярных групп подстановок.

В данной работе рассматривается общий случай для любых натуральных m, k, таких что $m \geqslant 2$, $k \geqslant 2$. Доказано, что k-транзитивность произведения регулярных групп подстановок $G_1 \cdot \ldots \cdot G_m$ эквивалентна отсутствию нулей в квадратной матрице, количество строк и столбцов в которой равно $(|\Omega| - 1)!/(|\Omega| - k)!$. Получена зависимость между количеством дуг орграфа, соответствующего этой матрице, и таким натуральным числом l, что произведение $(PsQt)^l$, где $P, Q \subseteq \mathrm{S}(\Omega)$ — некоторые регулярные группы подстановок, а подстановка st — $(|\Omega| - 1)$-цикл, будет 2-транзитивно. Приведён пример построения таких шифров типа AES, что их раундовые преобразования будут k-транзитивны на некотором количестве раундов.

Abstract

A. V. Toktarev, On K-transitivity conditions of a product of regular permutation groups, Fundamentalnaya i prikladnaya matematika, vol. 21 (2016), no. 3, pp. 217—231.

The paper analyses the product of m regular permutation groups $G_1 \cdot \ldots \cdot G_m$, where $m \geqslant 2$ is natural number. Each of regular permutation groups is the subgroup of symmetric permutation group $S(\Omega)$ of degree $|\Omega|$ for the set Ω. M. M. Glukhov proved that for $k = 2$ and $m = 2$, 2-transitivity of the product $G_1 \cdot G_2$ is equivalent to the absence of zeros in the corresponding square matrix with number of rows and columns equal to $|\Omega| - 1$. Also by M. M. Glukhov necessary conditions of 2-transitivity of such product of regular permutation groups are given.

In this paper, we consider the general case for any natural m and k such that $m \geqslant 2$ and $k \geqslant 2$. It is proved that k-transitivity of product of regular permutation groups $G_1 \cdot \ldots \cdot G_m$ is equivalent to the absence of zeros in the square matrix with number of rows and columns equal to $(|\Omega| - 1)!/(|\Omega| - k)!$. We obtain correlation between the number of arcs corresponding to this matrix and a natural number l such that the product

Фундаментальная и прикладная математика, 2016, том 21, № 3, с. 217—231.

$(PsQt)^l$ is 2-transitive, where $P, Q \subseteq S(\Omega)$ are some regular permutation groups and permutation st is $(|\Omega|-1)$-loop. We provide an example of the building of AES ciphers such that their round transformation are k-transitive on a number of rounds.

Введение

Пусть $\mathbb{N}$ — множество натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Регулярной группой подстановок конечного множества Ω называют любую транзитивную подгруппу G порядка $|\Omega|$ симметрической группы $\mathrm{S}(\Omega)$. Регулярные группы подстановок из $\mathrm{S}(\Omega)$ обладают следующим свойством: в каждой из них для любых $a, b \in \Omega$ существует единственная подстановка, отображающая a в b. Отсюда непосредственно следует, что порядок любой регулярной группы, являющейся подгруппой $\mathrm{S}(\Omega)$, равен $|\Omega|$. В связи с этим элементы регулярной группы G из $\mathrm{S}(\Omega)$ можно занумеровать элементами из Ω так, что $eg_c = c$ при фиксированном e и любом c из Ω. При этом множество Ω с операцией $\cdot$, определённой равенством $x \cdot y = xg_y$, становится группой с единицей e, а G — правым регулярным представлением группы $(\Omega, \cdot)$.

Основным результатом данной работы является нахождение условия k-транзитивности произведений m регулярных групп. Переходом от алгебраического анализа данных свойств к анализу свойств соответствующих графов и матриц удалось свести исследование условия k-транзитивности к исследованию полноты соответствующих графов.

Основные определения и обозначения

Для заданного множества Ω и числа $m \in \mathbb{N}$ через $\Omega^{\{m\}}$ будем обозначать множество всех таких строк $(\alpha_1, \ldots, \alpha_m)$ с элементами из множества Ω, что для любых $i, j \in \{1, \ldots, m\}$, $i \neq j$, выполняется соотношение $\alpha_i \neq \alpha_j$.

Пусть задано число $m \in \mathbb{N}$ и множества $H_1, \ldots, H_m$. Тогда через $H_1 \times \ldots \times H_m$ будем обозначать декартово произведение этих множеств, через $H_1 * \ldots * H_m$ — множество таких строк

$$\big\{(h_1, \ldots, h_m) \mid h_i \in H_i,\ i \in \{1, \ldots, m\}\big\},$$

что для любых $i, j \in \{1, \ldots, m\}$, $i \neq j$, выполняется соотношение $h_i \neq h_j$.

Подмножество R симметрической группы $\mathrm{S}(\Omega)$ называется k-транзитивным, если для любых $(a_1, \ldots, a_k), (b_1, \ldots, b_k) \in \Omega^{\{k\}}$ существует подстановка $r \in R$, такая что для любого $i \in \{1, \ldots, k\}$ выполняется равенство $r(a_i) = b_i$. Очевидно, что если правое регулярное представление R из $\mathrm{S}(\Omega)$ k-транзитивно, то полученная описанной во введении нумерацией соответствующая группа $(\Omega, \cdot)$ также k-транзитивна.

Пусть H — произвольная группа. Положим $H^* = H \setminus \{e\}$, где e — нейтральный элемент группы H.

Пусть группы $G_1, \ldots, G_m$ из $\mathrm{S}(\Omega)$ являются правыми регулярными представлениями соответственно групп $\left(\Omega, \overset{1}{\cdot}\right)$, $\left(\Omega, \overset{2}{\cdot}\right), \ldots,$ $\left(\Omega, \overset{m}{\cdot}\right)$. Не теряя общности, далее будем считать, что все группы $\left(\Omega, \overset{1}{\cdot}\right)$, $\left(\Omega, \overset{2}{\cdot}\right), \ldots,$ $\left(\Omega, \overset{m}{\cdot}\right)$ имеют общую единицу e, а элементы $G_1, \ldots, G_m$ из $\mathrm{S}(\Omega)$ занумерованы по указанному во введении правилу.

Также введём обозначение $\Omega^* = \Omega \setminus \{e\}$.

k-транзитивные свойства произведения m регулярных групп подстановок

Пусть заданы регулярные группы $G_1, \ldots, G_m$ из $\mathrm{S}(\Omega)$. По описанной во введении нумерации этим группам соответствует m групп вида

$$H_1 = \left(\Omega, \overset{1}{\cdot}\right),\ H_2 = \left(\Omega, \overset{2}{\cdot}\right), \ldots,\ H_m = \left(\Omega, \overset{m}{\cdot}\right).$$

Ясно, что для определения того, является ли произведение групп $G_1 \cdot \ldots \cdot G_m$ k-транзитивным, достаточно определить, имеет ли система уравнений

$$\begin{cases} \left(\ldots\left(\left(a_1 \overset{1}{\cdot} z_1\right) \overset{2}{\cdot} z_2\right) \overset{3}{\cdot} \ldots\right) \overset{m}{\cdot} z_m = b_1, \\ \quad \ldots \\ \left(\ldots\left(\left(a_k \overset{1}{\cdot} z_1\right) \overset{2}{\cdot} z_2\right) \overset{3}{\cdot} \ldots\right) \overset{m}{\cdot} z_m = b_k \end{cases}$$

решение для любых строк $(a_1, \ldots a_k) \in \Omega^{\{k\}}$, $(b_1, \ldots, b_k) \in \Omega^{\{k\}}$, где $\left\{z_i \in \Omega \mid i \in \{1, \ldots, m\}\right\}$.

Для упрощения записи далее будем полагать, что запись без скобок

$$a \overset{1}{\cdot} z_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m}{\cdot} z_m = b$$

эквивалентна последовательному умножению, т. е. записи

$$\left(\ldots\left(\left(a \overset{1}{\cdot} z_1\right) \overset{2}{\cdot} z_2\right) \overset{3}{\cdot} \ldots\right) \overset{m}{\cdot} z_m = b.$$

Утверждение 1. *Пусть группы $G_1, \ldots, G_m$ из $\mathrm{S}(\Omega)$ являются правыми регулярными представлениями соответственно групп*

$$H_1 = \left(\Omega, \overset{1}{\cdot}\right),\ H_2 = \left(\Omega, \overset{2}{\cdot}\right), \ldots,\ H_m = \left(\Omega, \overset{m}{\cdot}\right).$$

Тогда для любых строк $(a_1, \ldots a_k) \in \Omega^{\{k\}}$, $(b_1, \ldots, b_k) \in \Omega^{\{k\}}$ система уравнений

$$\begin{cases} a_1 \overset{1}{\cdot} z_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m}{\cdot} z_m = b_1, \\ \quad \ldots \\ a_k \overset{1}{\cdot} z_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m}{\cdot} z_m = b_k \end{cases} \tag{1}$$

имеет хотя бы одно решение тогда и только тогда, когда для всех $i \in \{1, \dots, k-1\}$ *существует хотя бы один набор из* $k-1$ *строк*

$$\begin{gathered}\left(\delta_1^{(2)}, \dots, \delta_1^{(m-1)}\right) \in (\Omega^*)^{\{m-2\}}, \\ \dots \\ \left(\delta_{k-1}^{(2)}, \dots, \delta_{k-1}^{(m-1)}\right) \in (\Omega^*)^{\{m-2\}},\end{gathered}$$

такой что система из $(k-1)\cdot(m-1)$ *уравнений*

$$\begin{cases} \beta_i \overset{m}{\cdot} x_{m-1} = \delta_i^{(m-1)} \overset{m-1}{\cdot} x_{m-1}, \\ \delta_i^{(m-1)} \overset{m-1}{\cdot} x_{m-2} = \delta_i^{(m-2)} \overset{m-2}{\cdot} x_{m-2}, \\ \quad \dots \\ \delta_i^{(2)} \overset{2}{\cdot} x_1 = \alpha_i \overset{1}{\cdot} x_1 \end{cases} \tag{2}$$

имеет хотя бы одно решение относительно неизвестных $(x_1, \dots, x_{m-1}) \in \Omega^{m-1}$, *где*

$$\begin{gathered} a_i \overset{1}{\cdot} a_k^{-1} = \alpha_i, \\ b_i \overset{m}{\cdot} b_k^{-1} = \beta_i. \end{gathered}$$

Доказательство. Введём следующие обозначения:

$$\begin{cases} a_k \overset{1}{\cdot} z_1 = x_1, \\ b_k \overset{m}{\cdot} z_m^{-1} = x_{m-1}, \\ a_i \overset{1}{\cdot} a_k^{-1} = \alpha_i = \delta_i^{(1)}, \\ b_i \overset{m}{\cdot} b_k^{-1} = \beta_i = \delta_i^{(m)}. \end{cases} \tag{3}$$

Также для $l \in \{2, \dots, m-1\}$ положим

$$x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{l-1}{\cdot} z_{l-1} = x_l.$$

Нетрудно убедиться, что для $l \in \{2, \dots, m-1\}$ выполняется соотношение

$$x_{l-1} \overset{l-1}{\cdot} z_{l-1} = x_l.$$

Используя уравнения системы (3), систему (1) можно преобразовать в систему

$$\begin{cases} \left(\delta_1^{(1)} \overset{1}{\cdot} x_1\right) \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = \delta_1^{(m)} \overset{m}{\cdot} x_{m-1}, \\ \quad \dots \\ \left(\delta_i^{(1)} \overset{1}{\cdot} x_1\right) \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = \delta_i^{(m)} \overset{m}{\cdot} x_{m-1}, \\ \quad \dots \\ \left(\delta_{k-1}^{(1)} \overset{1}{\cdot} x_1\right) \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = \delta_{k-1}^{(m)} \overset{m}{\cdot} x_{m-1}, \\ \left(\delta_k^{(1)} \overset{1}{\cdot} x_1\right) \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = \delta_k^{(m)} \overset{m}{\cdot} x_{m-1}. \end{cases} \tag{4}$$

Доказательство проведём индукцией по числу m.

Пусть $m = 2$. Имеем следующую систему уравнений:

$$\begin{cases} a_1 \overset{1}{\cdot} z_1 \overset{2}{\cdot} z_2 = b_1, \\ a_2 \overset{1}{\cdot} z_1 \overset{2}{\cdot} z_2 = b_2, \\ \quad \dots \\ a_k \overset{1}{\cdot} z_1 \overset{2}{\cdot} z_2 = b_k. \end{cases}$$

Используя введённые ранее обозначения, проходим к системе вида

$$\begin{cases} \delta_1^{(1)} \overset{1}{\cdot} x_1 = \delta_1^{(2)} \overset{2}{\cdot} x_1, \\ \delta_2^{(1)} \overset{1}{\cdot} x_1 = \delta_2^{(2)} \overset{2}{\cdot} x_1, \\ \quad \dots \\ \delta_{k-1}^{(1)} \overset{1}{\cdot} x_1 = \delta_{k-1}^{(2)} \overset{2}{\cdot} x_1. \end{cases}$$

Основание индукции доказано.

Пусть утверждение верно для $m-1$. Докажем его для m. Используя введённые ранее обозначения для $i \in \{1, \dots, k-1\}$, проходим к системе из k уравнений

$$\begin{cases} \delta_i^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = \delta_i^{(m)} \overset{m}{\cdot} x_{m-1}, \\ x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = x_{m-1}. \end{cases}$$

Используя ассоциативность умножения в группе H_{m-1}, получаем систему уравнений

$$\begin{cases} \left(\delta_i^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-2}{\cdot} z_{m-2}\right) \overset{m-1}{\cdot} \left(x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-2}{\cdot} z_{m-2}\right)^{-1} = \\ \quad = \left(\delta_i^{(m)} \overset{m}{\cdot} x_{m-1}\right) \overset{m-1}{\cdot} (x_{m-1}^{-1}), \\ x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-1}{\cdot} z_{m-1} = x_{m-1}. \end{cases} \tag{5}$$

Система уравнений (5) имеет решение тогда и только тогда, когда существует такая строка

$$\left(\delta_1^{(m-1)}, \dots, \delta_{k-1}^{(m-1)}\right) \in (H^*{}_{m-1})^{\{k-1\}},$$

что для всех $i \in \{1, \dots, k-1\}$ выполняются соотношения

$$\left(\delta_i^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-2}{\cdot} z_{m-2}\right) \overset{m-1}{\cdot} \left(x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \dots \overset{m-2}{\cdot} z_{m-2}\right)^{-1} = \delta_i^{(m-1)}, \tag{6}$$

$$\delta_i^{(m)} \overset{m}{\cdot} x_{m-1} = \delta_i^{(m-1)} \overset{m-1}{\cdot} x_{m-1}. \tag{7}$$

Используя (6), систему уравнений (5) можно переписать в виде

$$\begin{cases} \delta_1^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = \delta_1^{(m-1)} \overset{m-1}{\cdot} \left(x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2}\right), \\ \quad \ldots \\ \delta_i^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = \delta_i^{(m-1)} \overset{m-1}{\cdot} \left(x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2}\right), \\ \quad \ldots \\ \delta_{k-1}^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = \delta_{k-1}^{(m-1)} \overset{m-1}{\cdot} \left(x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2}\right), \\ \left(x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2}\right) \overset{m-1}{\cdot} z_{m-1} = x_{m-1}. \end{cases} \tag{8}$$

В последнем уравнении при фиксированных $x_1, z_2, \ldots, z_{m-2}, x_{m-1}$ элемент z_{m-1} находится однозначно, поэтому последнее уравнение можно исключить.

Используя соотношение

$$x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = x_{m-2},$$

получаем систему уравнений

$$\begin{cases} \delta_1^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = \delta_1^{(m-1)} \overset{m-1}{\cdot} x_{m-2}, \\ \quad \ldots \\ \delta_i^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = \delta_i^{(m-1)} \overset{m-1}{\cdot} x_{m-2}, \\ \quad \ldots \\ \delta_{k-1}^{(1)} \overset{1}{\cdot} x_1 \overset{2}{\cdot} z_2 \overset{3}{\cdot} \ldots \overset{m-2}{\cdot} z_{m-2} = \delta_{k-1}^{(m-1)} \overset{m-1}{\cdot} x_{m-2}. \end{cases} \tag{9}$$

По предположению индукции система уравнений (9) имеет решение тогда и только тогда, когда для всех $i \in \{1, \ldots, k-1\}$ существует хотя бы один такой набор из $k-1$ строк

$$\begin{gathered} \left(\delta_1^{(2)}, \ldots, \delta_1^{(m-2)}\right) \in (\Omega^*)^{\{m-3\}}, \\ \ldots \\ \left(\delta_{k-1}^{(2)}, \ldots, \delta_{k-1}^{(m-2)}\right) \in (\Omega^*)^{\{m-3\}} \end{gathered}$$

что система из $(k-1) \cdot (m-1)$ уравнений

$$\begin{cases} \delta_i^{(m-1)} \overset{m-1}{\cdot} x_{m-1} = \delta_i^{(m-2)} \overset{m-2}{\cdot} x_{m-1}, \\ \quad \ldots \\ \delta_i^{(2)} \overset{m-1}{\cdot} x_1 = \alpha \overset{1}{\cdot} x_1 \end{cases} \tag{10}$$

имеет хотя бы одно решение относительно неизвестных $(x_1, \ldots, x_{m-1}) \in \Omega^{m-1}$, а значит, с учётом соотношения (7) система (5) имеет решение тогда и только

тогда, когда существует хотя бы один такой набор из k строк

$$\begin{gathered}\left(\delta_1^{(2)},\dots,\delta_1^{(m-1)}\right)\in(\Omega^*)^{\{m-2\}},\\ \dots\\ \left(\delta_{k-1}^{(2)},\dots,\delta_{k-1}^{(m-1)}\right)\in(\Omega^*)^{\{m-2\}},\end{gathered}$$

что имеют решение система (10) и система (7). □

Для набора групп $H_1,\dots,H_m$ полученного описанной во введении нумерацией для соответствующих m правых регулярных представлений и фиксированного $k\in\mathbb{N}$ рассмотрим $m-1$ квадратную матрицу $M_1,\dots,M_{m-1}$ с количеством строк и столбцов, равным $(|\Omega|-1)!/(|\Omega|-k)!$, с элементами из множества $\{0,1\}$. Для $s,t\in\{1,\dots,(|\Omega|-1)!/(|\Omega|-k)!\}$ и $l\in\{1,\dots,m-1\}$ каждая строка матрицы M_l с номером s соответствует строке

$$\left(\lambda_1^{(s)},\dots,\lambda_{k-1}^{(s)}\right)\in(\Omega^*)^{\{k-1\}},$$

каждый столбец с номером t соответствует строке

$$\left(\lambda_1^{(t)},\dots,\lambda_{k-1}^{(t)}\right)\in(\Omega^*)^{\{k-1\}}.$$

На пересечении строки с номером s и столбца с номером t стоит 1, если система уравнений

$$\begin{cases}{\lambda_{k-1}}^{(t)}\overset{l}{\cdot}x={\lambda_{k-1}^{(s)}}\overset{l-1}{\cdot}x,\\ \quad\dots\\ {\lambda_1}^{(t)}\overset{l}{\cdot}x={\lambda_1^{(s)}}\overset{l-1}{\cdot}x\end{cases}\tag{11}$$

имеет хотя бы одно решение относительно строки-неизвестной $x\in\Omega$, и 0, если система (11) не имеет решений относительно строки-неизвестной $x\in\Omega$.

Для групп $A'=(\Omega,\cdot)$, $B'=(\Omega,*)$, их соответствующих правых регулярных представлений $A,B\subseteq\mathrm{S}(\Omega)$ и фиксированного $k\in\{2,\dots,|\Omega|\}$ построенную описанным способом матрицу будем обозначать как $M(A,B,k)$ в контексте правых регулярных представлений и $M(A',B',k)$ в контексте описанных групп над Ω.

Утверждение 2. *Система уравнений* (1) *разрешима для любых пар строк* $(a_1,\dots,a_k)\in\Omega^k$, $(b_1,\dots,b_k)\in\Omega^k$ *тогда и только тогда, когда матрица* $M_1\cdot\ldots\cdot M_{m-1}$ *не содержит нулевых элементов.*

Доказательство. Доказательство будем проводить индукцией по числу m.

Докажем утверждение для $m=3$. Для всех $i\in\{1,\dots,k-1\}$ рассмотрим систему из $(k-1)\cdot 2$ уравнений

$$\begin{cases}{\beta_i}\overset{3}{\cdot}x_2=\delta_i^{(2)}\overset{2}{\cdot}x_2,\\ \delta_i^{(2)}\overset{2}{\cdot}x_1=\alpha_i\overset{(1)}{\cdot}x_1.\end{cases}\tag{12}$$

Каждая ячейка матрицы M_1 на пересечении строки $(\alpha_1, \ldots, \alpha_{k-1})$ и столбца $(\delta_1, \ldots, \delta_{k-1})$ содержит 1, если система

$$\begin{cases} \delta_1^{(2)} \overset{2}{\cdot} x_1 = \alpha_1 \overset{(1)}{\cdot} x_1, \\ \quad \ldots \\ \delta_{k-1}^{(2)} \overset{2}{\cdot} x_1 = \alpha_{k-1} \overset{(1)}{\cdot} x_1 \end{cases}$$

разрешима, и 0 в обратном случае.

Каждая ячейка матрицы M_2 на пересечении строки $(\delta_1, \ldots, \delta_{k-1})$ и столбца $(\beta_1, \ldots, \beta_{k-1})$ содержит 1, если система уравнений

$$\begin{cases} \delta_1^{(2)} \overset{2}{\cdot} x_1 = \alpha_1 \overset{(1)}{\cdot} x_1, \\ \quad \ldots \\ \delta_{k-1}^{(2)} \overset{2}{\cdot} x_1 = \alpha_{k-1} \overset{(1)}{\cdot} x_1 \end{cases}$$

разрешима, и 0 в обратном случае.

Пусть

$$M_1 = \left[c_{i,j}^{(1)}\right], \quad M_2 = \left[c_{i,j}^{(2)}\right], \quad M_1 \cdot M_2 = \left[c_{i,j}^{(1,2)}\right],$$
$$c_{i,j}^{(1,2)} = \sum_{l=1}^{(n-1)!/(n-k)!} c_{i,l}^{(1)} c_{l,j}^{(2)}. \tag{13}$$

Пусть для любых строк $(\alpha_1, \ldots, \alpha_{k-1})$, $(\beta_1, \ldots, \beta_{k-1})$ существует такая строка $(\delta_1, \ldots, \delta_{k-1})$, что система уравнений (12) разрешима. Отсюда следует, что для любых $i, j \in [1, \ldots, (n-1)!/(n-k)!]$ существует такое $l \in [1, \ldots, (n-1)!/(n-k)!]$, что

$$c_{(i,l)}^{(1)} > 0, \quad c_{l,j}^{(2)} > 0.$$

Отсюда следует что все элементы матрицы $M_1 \cdot M_2$ ненулевые.

Обратно пусть все элементы матрицы $M_1 \cdot M_2$ ненулевые. Тогда из (13) следует, что для любых $i, j \in \mathbb{N}$ существует такое $l \in \mathbb{N}$, что

$$c_{(i,l)}^{(1)} > 0, \quad c_{l,j}^{(2)} > 0.$$

Значит, для любых строк $(\alpha_1, \ldots, \alpha_{k-1})$, $(\beta_1, \ldots, \beta_{k-1})$ существует такая строка $(\delta_1, \ldots, \delta_{k-1})$ что система уравнений (12) разрешима.

Из утверждения 1 следует справедливость базы индукции. Пусть утверждение верно для m, докажем его для $m+1$.

Используя предположение индукции и утверждение 1 получаем, что для любых строк $(\alpha_1, \ldots, \alpha_{k-1})$, $(\beta_1, \ldots, \beta_{k-1})$ система уравнений (2) разрешима тогда и только тогда, когда все элементы матрицы $M_1 \cdot \ldots \cdot M_{m-1} = [c_{i,j}^{1,\ldots,m-1}]$ ненулевые.

Для $i \in \{1, \dots, k-1\}$ рассмотрим систему уравнений

$$m(k-1)\begin{cases} \beta_i \overset{m+1}{\cdot} x_m = \delta_i^{(m-1)} \overset{m}{\cdot} x_m, \\ \delta_i^{(m-1)} \overset{m-1}{\cdot} x_{m-1} = \delta_i^{(m-2)} \overset{m-2}{\cdot} x_{m-1}, \\ \quad \dots \\ \delta_i^{(2)} \overset{2}{\cdot} x_1 = \alpha_i \overset{(1)}{\cdot} x_1. \end{cases} \tag{14}$$

Все элементы матрицы

$$M = M_1 \cdot \dots \cdot M_{m-1} \cdot M_m = \left[c_{i,j}^{(1,\dots,m)}\right] = \left[\sum_{l=1}^{(n-1)!/(n-k)!} c_{i,l}^{(1,\dots,m-1)} c_{l,j}^{(m)}\right]$$

ненулевые, если для любых $i, j \in \mathbb{N}$ существует такое $l \in [1, \dots, (n-1)!/(n-k)!]$, что $c_{(i,l)}^{(1,\dots,m-1)} > 0$, $c_{l,j}^{(m)} > 0$, а значит, для любых строк $(\alpha_1, \dots, \alpha_{k-1})$ и $(\beta_1, \dots, \beta_{k-1})$ существуют строки $\left(\delta_1^{(2)}, \dots, \delta_1^{(m-1)}\right)$, $\left(\delta_1^{(2)}, \dots, \delta_{k-1}^{(m-1)}\right)$, такие что система (14) разрешима.

Обратная импликация очевидна. □

Матрицу $M = M_1 \cdot \dots \cdot M_{l-1}$, соответствующую произведению регулярных групп подстановок $G_1 \cdot \dots \cdot G_l$, где для $s \in \{1, \dots, l-1\}$ выполняется соотношение $M_s = M(G_s, G_{s+1}, k)$, будем обозначать через $M(G_1, \dots, G_l, k)$.

Представление матриц в виде орграфов

Для групп $A' = (\Omega, \cdot)$, $B' = (\Omega, *)$, их соответствующих правых регулярных представлений $A, B \subseteq \mathrm{S}(\Omega)$ и фиксированного $k \in \{2, \dots |\Omega|\}$ рассмотрим орграф с множеством вершин из $(\Omega^*)^{\{k-1\}}$. Будем обозначать этот орграф через $G(A, B, k)$ в контексте правых регулярных преставлений и через $G(A', B', k)$ в контексте описанных групп над Ω. Ясно, что количество вершин в описанном орграфе равно $(|\Omega| - 1)!/(|\Omega| - k)!$.

Для $l \in [1, \dots, (|\Omega| - 1)!/(|\Omega| - k)!]$ каждая вершина этого орграфа имеет номер l и взаимно-однозначно соответствует строке

$$\left(\lambda_1^{(l)}, \dots, \lambda_{k-1}^{(l)}\right) \in (\Omega^*)^{\{k-1\}},$$

которая соответствует столбцу и строке матрицы $M(A, B, k)$ с номером l. Для любых $t, s \in [1, \dots, (|\Omega| - 1)!/(|\Omega| - k)!]$ дуга от вершины строки

$$\left(\delta_1^{(t)}, \dots, \delta_{k-1}^{(t)}\right) \in (\Omega^*)^{\{k-1\}}$$

к вершине строки

$$\left(\delta_1^{(s)}, \dots, \delta_{k-1}^{(s)}\right) \in (\Omega^*)^{\{k-1\}}$$

означает, что элемент матрицы $M(A,B,k)$, находящийся на пересечении строки с номером s и столбца с номером t, больше нуля, другими словами, уравнение

$$\begin{cases} \delta_k^{(t)} \overset{t}{\cdot} x = \delta_k^{(s)} \overset{s}{\cdot} x, \\ \delta_{k-1}^{(t)} \overset{t}{\cdot} x = \delta_{k-1}^{(s)} \overset{s}{\cdot} x, \\ \quad \dots \\ \delta_1^{(t)} \overset{t}{\cdot} x = \delta_1^{(s)} \overset{s}{\cdot} x \end{cases}$$

имеет хотя бы одно решение. Ясно, что для любых двух регулярных групп подстановок A, B матрица $M(A,B,k)$ является матрицей смежности орграфа $G(A,B,k)$.

Рассмотрим m групп

$$H_1 = \left(\Omega, \overset{1}{\cdot}\right),\ H_2 = \left(\Omega, \overset{2}{\cdot}\right), \dots,\ H_m = \left(\Omega, \overset{m}{\cdot}\right).$$

Ясно, что матрицей смежности орграфа

$$G(H_1,H_2,k) \cdot \ldots \cdot G(H_{m-1},H_m,k)$$

будет матрица

$$M(H_1,H_2,k) \cdot \ldots \cdot M(H_{m-1},H_m,k).$$

Таким образом, из утверждения 2 следует, что произведение $H_1 \cdot \ldots \cdot H_m$ будет k-транзитивно тогда и только тогда, когда матрица

$$M(H_1,H_2,k) \cdot \ldots \cdot M(H_{m-1},H_m,k)$$

не содержит нулевых элементов, откуда следует, что в орграфе

$$G(H_1,H_2,k) \cdot \ldots \cdot G(H_{m-1},H_m,k)$$

для любых двух вершин a, b существует дуга (a,b).

Таким образом, для ответа на вопрос, является ли произведение m регулярных групп подстановок k-транзитивным, достаточно проверить, отсутствуют ли нули в соответствующей матрице $M(H_1,H_2,k) \cdot \ldots \cdot M(H_{m-1},H_m,k)$ или проверить полноту орграфа $G(H_1,H_2,k) \cdot \ldots \cdot G(H_{m-1},H_m,k)$.

k-транзитивность множества подстановок, порождённого двумя регулярными группами подстановок и двумя подстановками

Рассмотрим две регулярные группы подстановок $P,Q \subseteq \mathrm{S}(\Omega)$ и две подстановки $s,t \in \mathrm{S}(\Omega)$. Для $l \in \mathbb{N}$ рассмотрим множество подстановок вида

$$V_l = \underbrace{(PsQt)\,(PsQt)\dots(PsQt)}_{l} = (PsQt)^l.$$

Рассмотрим произведение

$$V_l' = [P(sQs^{-1})]\big[(st)P(st)^{-1}\big((st)s\big)Q\big((st)s\big)^{-1}\big]\dots \\ \dots\big[(st)^{l-1}P\big((st)^{l-1}\big)^{-1}\big((st)^{l-1}s\big)Q\big((st)^{l-1}s\big)^{-1}\big].$$

Очевидно, что для любого $l \in \mathbb{N}$ все множества вида $(st)^{l-1}P\big((st)^{l-1}\big)^{-1}$ и $\big((st)^{l-1}s\big)Q\big((st)^{l-1}s\big)^{-1}$ являются регулярными группами подстановок. Также очевидно, что справедливо равенство $V_l = V_l'(st)^l$. Очевидно, что множество V k-транзитивно тогда и только тогда, когда множество V' k-транзитивно, а значит, для определения того, является ли множество V k-транзитивным, достаточно проверить, k-транзитивно ли множество V', которое является произведением некоторого количества регулярных групп подстановок.

Утверждение 3. *Для любых двух регулярных групп подстановок $P, Q \subseteq \subseteq \mathrm{S}(\Omega)$, подстановок $s, t \in \mathrm{S}(\Omega)$, $k \in \{2, \dots, |\Omega|\}$, $l \in \mathbb{N}$ имеют место следующие изоморфизмы орграфов*:

$$G\big((st)^{l-1}P\big((st)^{l-1}\big)^{-1}, \big((st)^{l-1}s\big)Q\big((st)^{l-1}s\big)^{-1}, k\big) \simeq \\ \simeq G\big((st)^{l}P\big((st)^{l}\big)^{-1}, \big((st)^{l}s\big)Q\big((st)^{l}s\big)^{-1}, k\big),$$

$$G\Big(\big((st)^{l-1}s\big)Q\big((st)^{l-1}s\big)^{-1}, (st)^{l}P\big((st)^{l}\big)^{-1}, k\Big) \simeq \\ \simeq G\Big(\big((st)^{l}s\big)Q\big((st)^{l}s\big)^{-1}, (st)^{l+1}P\big((st)^{l+1}\big)^{-1}, k\Big),$$

при этом изоморфизмом является подстановка $(st)^{-1}$.

Доказательство. Для некоторого $m \in \mathbb{N}$ рассмотрим произведение $2m$ регулярных групп подстановок:

$$[P(sQs^{-1})]\big[(st)P(st)^{-1}\big((st)s\big)Q\big((st)s\big)^{-1}\big]\dots \\ \dots\big[(st)^{m-1}P\big((st)^{m-1}\big)^{-1}\big((st)^{m-1}s\big)Q\big((st)^{m-1}s\big)^{-1}\big].$$

Для любых $k \in \{2, \dots, |\Omega|\}$, $i \in \{1, \dots, k-1\}$ система уравнений (2) будет состоять из $(2m-1)(k-1)$ уравнений и иметь вид

$$\begin{cases} s\big((st)^{m-1}(\beta_i)\big) * x_{2m-1} = s\big((st)^{m-1}\big(\delta_i^{(2m-1)}\big) \cdot x_{2m-1}\big), \\ \quad \dots \\ st\Big((st)^{l}\big(\delta_i^{(2l+3)}\big)\Big) \cdot x_{2l+2} = t\Big(s\Big((st)^{l}\big(\delta_i^{(2l+2)}\big)\Big) * x_{2l+2}\Big), \\ s\Big((st)^{l}\big(\delta_i^{(2l+2)}\big)\Big) * x_{2l+1} = s\big((st)^{l}\big(\delta_i^{(2l+1)}\big) \cdot x_{2l+1}\big), \\ \quad \dots \\ st\big(\delta_i^{(3)}\big) \cdot x_2 = t\big(s\big(\delta_i^{(2)}\big) * x_2\big), \\ s\big(\delta_i^{(2)}\big) * x_1 = s(\alpha_i \cdot x_1). \end{cases} \tag{15}$$

Для $l \in \{1, \dots, m-2\}$ ясно, что если уравнение

$$s\big((st)^l(\alpha)\big) * x = s\big((st)^l(\beta) \cdot x\big)$$

имеет решение для пары (α, β) тогда и только тогда, когда уравнение

$$s\big((st)^{l+1}(\alpha)\big) * x = s\big((st)^{l+1}(\beta) \cdot x\big)$$

имеет решение для пары $\big((st)^{-1}(\alpha), (st)^{-1}(\beta)\big)$. Значит, для любого $l \in \in \{1, \dots, m-2\}$ выполняется соотношение для матриц

$$M\big((st)^l P\big((st)^l\big)^{-1}, \big((st)^l s\big) Q\big((st)^l s\big)^{-1}, k\big) = \\ = M\big((st)^{l-1} P\big((st)^{l-1}\big)^{-1}, \big((st)^{l-1} s\big) Q\big((st)^{l-1} s\big)^{-1}, k\big) \cdot M_{(st)}^{-1},$$

где $M_{(st)}^{-1}$ — подстановочная матрица, соответствующая подстановке $(st)^{-1}$. Так как число m выбиралось произвольно, получаем, что для любого $l \in \mathbb{N}$ орграф

$$G\big((st)^l P\big((st)^l\big)^{-1}, \big((st)^l s\big) Q\big((st)^l s\big)^{-1}, k\big)$$

получается из орграфа

$$G\big((st)^{l-1} P\big((st)^{l-1}\big)^{-1}, \big((st)^{l-1} s\big) Q\big((st)^{l-1} s\big)^{-1}, k\big)$$

отображением множества вершин подстановкой $(st)^{-1}$. Значит, имеет место изоморфизм орграфов

$$G\big((st)^{l-1} P\big((st)^{l-1}\big)^{-1}, \big((st)^{l-1} s\big) Q\big((st)^{l-1} s\big)^{-1}, k\big) \simeq \\ \simeq G\big((st)^l P\big((st)^l\big)^{-1}, \big((st)^l s\big) Q\big((st)^l s\big)^{-1}, k\big).$$

Аналогично доказывается изоморфизм орграфов

$$G\Big(\big((st)^{l-1} s\big) Q\big((st)^{l-1} s\big)^{-1}, (st)^l P\big((st)^l\big)^{-1}, k\Big) \simeq \\ \simeq G\Big(\big((st)^l s\big) Q\big((st)^l s\big)^{-1}, (st)^{l+1} P\big((st)^{l+1}\big)^{-1}, k\Big). \quad \square$$

Пусть G — произвольный орграф. Тогда через $c(G)$ будем обозначать количество компонент связности в нём, а через $r(G)$ — количество дуг в орграфе G.

Для фиксированных $l \in \mathbb{N}$, $k \in \{2, \dots, |\Omega|\}$ введём следующее обозначение:

$$G_{l,k} = G\big((st)^{l-1} P\big((st)^{l-1}\big)^{-1}, \big((st)^{l-1} s\big) Q\big((st)^{l-1} s\big)^{-1}, k\big) * \\ * G\Big(\big((st)^{l-1} s\big) Q\big((st)^{l-1} s\big)^{-1}, (st)^l P\big((st)^l\big)^{-1}, k\Big).$$

Утверждение 4. *Для любых двух регулярных групп подстановок $P, Q \subseteq \subseteq \mathrm{S}(\Omega)$ и подстановок $s, t \in \mathrm{S}(\Omega)$, таких что st — это $(|\Omega|-1)$-цикл, оставляющий на месте нейтральный элемент, справедливы следующие свойства*:

1) *множество подстановок $(PsQt)^l$ 2-транзитивно для*

$$l = \min(|\Omega^*|^2 - r(G), |\Omega^*| - 2) + 1,$$

где $G = G_{1,2}$;

2) *для любого* $k \in \{2, \dots, |\Omega|\}$ *если множество подстановок* $PsQt$ *содержит* $(|\Omega| - k + 2)$*-цикл, то группа* $\langle PsQt \rangle$ k*-транзитивна.*

Доказательство. Рассмотрим произведение регулярных групп подстановок

$$P(sQs^{-1})\big((st)P(st)^{-1}\big).$$

Система уравнений (2) будет иметь вид

$$\begin{cases} st(\beta) \cdot x_2 = t(s(\delta) * x_2), \\ s(\delta) * x_1 = s(\alpha \cdot x_1). \end{cases} \tag{16}$$

Рассмотрим орграфы

$$H_1 = G(P, sQs^{-1}, 2), \quad H_2 = G(P, sQs^{-1}, 2).$$

Рассмотрим множество подстановок $T \subseteq \mathrm{S}(\Omega)$. Обозначим через $G(T)$ такой орграф с вершинами из Ω^*, что любые две вершины α, β соединены дугой тогда и только тогда, когда существует такая подстановка $\varphi \in T$, что $\varphi(\alpha) = \beta$. Ясно что имеют место соотношения

$$G_1 = G(\{p_\delta s q_\delta^{-1} s^{-1} \mid \delta \in \Omega\}), \quad G_2 = G(\{s q_\delta t p_\delta^{-1} (st)^{-1} \mid \delta \in \Omega\}).$$

Пусть

$$H = \{p_\delta s q_\delta^{-1} q_\gamma t p_\gamma^{-1} (st)^{-1} \mid \delta, \gamma \in \Omega\}.$$

Из определения произведения орграфов следует, что $H_1 H_2 = G(H)$. Ясно, что H содержит единичный элемент, а значит, в орграфе $G(H)$ для каждой вершины существует петля. Ясно, что

$$\{p_\alpha (st) p_\alpha^{-1} (st)^{-1} \mid \alpha \in \Omega\} \subseteq H.$$

Отсюда в силу регулярности группы подстановок P для любого $\alpha \in \Omega$ существует такая подстановка $p \in P$, что $p(\alpha) = e$. Так как подстановка st — это цикл длины $|\Omega| - 1$, не содержащий e, имеет место соотношение

$$p_\alpha (st) p_\alpha^{-1} (st)^{-1}(\alpha) = (st)^{-1}(\alpha).$$

Значит, в орграфе $H_1 H_2$ две вершины $\alpha, \beta \in \Omega^*$ соединены дугой, если $(st)^{-1}(\alpha) = \beta$. Отсюда следует, что орграф $H_1 H_2$ связный. Отсюда в силу утверждения 3 и сказанного выше получаем, что для любого $l \in \mathbb{N}$ орграф

$$G_l = G\big((st)^{l-1} P \big((st)^{l-1}\big)^{-1}, \big((st)^{l-1} s\big) Q \big((st)^{l-1} s\big)^{-1}, 2\big) * \\ * G\Big(\big((st)^{l-1} s\big) Q \big((st)^{l-1} s\big)^{-1}, (st)^l P \big((st)^l\big)^{-1}, 2\Big)$$

связный, содержит цикл со всеми элементами из множества Ω^* и петли для каждой вершины.

Пусть r_i — число дуг в графе G, исходящих из вершины с номером i. Очевидно, что для любых натуральных $i \in [1, \dots, |\Omega| - 1]$ и $l \geqslant 2$ имеет место соотношение

$$r_i \geqslant \min(r_i + 1, |\Omega| - 1).$$

Пусть

$$r_{\min} = \min_{i\in[1,\ldots,|\Omega|-1]} r_i.$$

Тогда

$$r_{\min} \geqslant r(G) - |\Omega^*|(|\Omega^*| - 1).$$

Отсюда следует, что

$$l_{\max} = |\Omega^*| - r_{\min} \leqslant |\Omega^*| - r(G) + |\Omega^*|(|\Omega^*| - 1).$$

Получаем, что орграф

$$G_1 G_2 \ldots G_{\min(|\Omega^*|^2 - r(G), |\Omega^*|-2)}$$

полный, а значит, множество

$$(PsQt)^{\min(|\Omega^*|^2 - r(G), |\Omega^*|-2)+1}$$

2-транзитивно. Пункт 1) доказан.

Из пункта 1) непосредственно следует, что группа $\langle PsQt\rangle$ примитивна. Используя теорему Маргграффа [2] и условия пункта 2), получаем, что группа $\langle PsQt\rangle$ k-транзитивна. □

k-транзитивные свойства некоторых алгоритмов шифрования

Описанная выше конструкция произведения m регулярных групп подстановок является основой для ряда алгоритмов шифрования. Дальнейшие рассуждения будем вести для симметрической группы множества двоичных строк $\Omega = \mathrm{GF}(2)^m$, где m — размер блока алгоритма шифрования. Рассмотрим разновидности алгоритмов шифрования типа AES. Далее будем полагать, что Q — это регулярная группа с операцией побитового сложения по модулю 2, P — это регулярная группа с операцией сложения по модулю 2^m , а s — некоторая подстановка из $\mathrm{S}(\Omega)$.

Рассмотрим подстановку вида

$$\varphi = \begin{pmatrix} 2^m-1 & 2^m-2 & \ldots & 2^{m-1} & 2^{m-1}-1 & \ldots & 1 \\ 1 & 3 & \ldots & 2^m-1 & 2 & \ldots & 2^m-2 \end{pmatrix}.$$

Пусть

$$s = \varphi\begin{pmatrix}0 & 1 & 2 & 3 & \ldots & 2^m-1\end{pmatrix}\varphi^{-1},\ t = \varphi\begin{pmatrix}1 & 0 & 2 & 3 & 4 & \ldots & 2^m-1\end{pmatrix}\varphi^{-1}.$$

Тогда

$$st = \begin{pmatrix}2^m-1 & \ldots & 2 & 1\end{pmatrix}\begin{pmatrix}0\end{pmatrix}.$$

В силу того что

$$\begin{pmatrix}0 & 1 & \ldots & 2^m-1\end{pmatrix} \in P,$$

получаем, что

$$\begin{pmatrix} 0 & 1 & \dots & 2^m-1 \end{pmatrix} \begin{pmatrix} 2^m-1 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 2^m-1 & 0 \end{pmatrix}.$$

Из утверждения 4 получаем, что произведение $\langle PsQt \rangle$ $|\Omega|$-транзитивно, что равносильно тому, что $\langle PsQt \rangle = \mathrm{S}(\Omega)$.

Заключение

В работе получен результат, который позволит определять условия k-транзитивности шифрсистем, представляющих собой комбинацию преобразований из регулярных групп подстановок. Также результат может быть использован для получения шифрсистем с заранее определёнными свойствами кратной транзитивности.

Автор благодарит кандидата физико-математических наук, доцента Пудовкину Марину Александровну, доктора физико-математических наук, профессора Глухова Михаила Михайловича и доктора физико-математических наук, профессора Михалёва Александра Васильевича за внимание и поддержку при написании работы.

Литература

[1] Глухов М. М. О 2-транзитивных произведениях регулярных групп подстановок // Тр. по дискр. матем. — 2000. — Т. 3. — С. 37—52.

[2] Levingston R., Taylor D. E. The theorem of Marggraff on primitive permutation groups which contain a cycle // Bull. Austral. Math. Soc. — 1976. — Vol. 15, no. 1. — P. 125—128.