О вполне неразложимых неотрицательных матрицах и условии А. Н. Колмогорова

И. А. КРУГЛОВ
Академия криптографии Российской Федерации
e-mail: kruglov-gosha@mail.ru

УДК 519.2

Ключевые слова: дважды стохастические матрицы, вполне неразложимые матрицы.

Аннотация

В работе обсуждаются свойства вполне неразложимых дважды стохастических матриц.

Abstract

I. A. Kruglov, On the completely indecomposable nonnegative matrices and A. N. Kolmogorov's condition, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 167—172.

The paper concerns properties of fully indecomposable doubly stochastic matrices.

В одной из ранних работ А. А. Нечаева [6] рассматривалась следующая задача исследования предельного поведения вероятностных распределений на конечных группах. Предположим, что задана конечная простая однородная неразложимая цепь Маркова с множеством состояний $\{1, 2, \dots, n\}$, $n \geqslant 2$, с матрицей переходных вероятностей $P = [p(i,j)]_{n\times n}$ и начальным распределением $\bar{p}_0$. Пусть также $(G;\cdot)$ — некоторая конечная группа, $\sigma\colon G \to G$ — произвольное *биективное* преобразование множества G, $g_1, g_2, \dots, g_n$ — произвольная последовательность элементов группы G. Случайной реализации $\alpha_1, \alpha_2, \dots, \alpha_k, \dots$ цепочки состояний цепи Маркова соответствует последовательность случайных элементов со значениями в группе G, определяемая по индукции:

$$\xi^{(1)} = g_{\alpha_1}, \quad \xi^{(k+1)} = \sigma\big(\xi^{(k)}\big) \cdot g_{\alpha_{k+1}}, \quad k \geqslant 1. \tag{1}$$

Для приложений в криптографии представляют интерес условия на матрицу P и последовательность $g_1, g_2, \dots, g_n$, при выполнении которых, *независимо от выбора* $\bar{p}_0$ и σ, последовательность распределений случайных элементов $\xi^{(k)}$ при $k \to \infty$ сходится к равномерному распределению на группе G, т. е. для любого $g \in G$

$$\lim_{k\to\infty} \mathsf{P}\big(\xi^{(k)} = g\big) = \frac{1}{|G|}. \tag{2}$$

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 167—172.

Нетрудно убедиться, что необходимым условием для соотношения (2) является следующее: множество $\{g_1, g_2, \ldots, g_n\}$ не содержится в одном (левом) смежном классе по некоторой собственной подгруппе группы G, т. е.

$$G = \langle g_1^{-1} \cdot g_2, \ldots, g_1^{-1} \cdot g_n \rangle. \tag{3}$$

Действительно, в противном случае для подгруппы $H = \langle g_1^{-1} \cdot g_2, \ldots, g_1^{-1} \cdot g_n \rangle$, порождённой подмножеством $\{g_1^{-1} \cdot g_2, \ldots, g_1^{-1} \cdot g_n\}$, имеет место соотношение $H \neq G$. Если мы теперь выберем биективное преобразование $\sigma\colon G \to G$, для которого $\sigma(g) = g \cdot g_1^{-1}$, $g \in G$, то при любом $g \in G \setminus H$ и любом $k \geqslant 2$ согласно (1) получим равенство $\mathsf{P}\big(\xi^{(k)} = g\big) = 0$, и соотношение (2) не будет выполнено.

При исследовании случая, когда матрица P является дважды стохастической, А. А. Нечаев (на основе известной теоремы Биркгофа [8]) использовал возможность разложения вида

$$P = p_1\Pi_1 + \ldots + p_s\Pi_s, \tag{4}$$

в котором $\Pi_1, \ldots, \Pi_s$ — подстановочные матрицы и $p_1, \ldots, p_s$ — положительные вещественные числа, для которых $p_1 + \ldots + p_s = 1$. Разложение (4) не однозначно, полученные результаты не зависят от выбора данного разложения.

Для $l = 1, \ldots, s$ обозначим через π_l подстановку на множестве $\{1, 2, \ldots, n\}$, которой соответствует матрица Π_l. М. М. Глуховым в статье, которая была опубликована в ведомственном научном журнале в 1967 году, введено так называемое *условие E-F-примитивности* систем подстановок. Система подстановок $\pi_1, \ldots, \pi_s$ называется *E-F-примитивной*, если не существует таких подмножеств $E, F \subset \{1, 2, \ldots, n\}$, что $|E| = |F| = m$, $0 < m < n$, и для любых $l = 1, \ldots, s$ и $i \in E$ выполняется $\pi_l(i) \in F$.

А. А. Нечаевым была доказана следующая теорема.

Теорема 1 [6]. *Предположим, что система подстановок $\pi_1, \ldots, \pi_s$ из разложения вида* (4) *дважды стохастической матрицы P является E-F-примитивной, члены последовательности $g_1, g_2, \ldots, g_n$ попарно различны и выполнено равенство* (3). *Тогда для любого начального распределения $\bar{p}_0$ цепи Маркова и любого биективного преобразования σ группы G последовательность распределений случайных элементов $\xi^{(k)}$ при $k \to \infty$ сходится к равномерному распределению на группе G.*

Отметим, что В. Н. Сачковым в статье, которая была опубликована также в ведомственном научном журнале в 1964 году, для разложений дважды стохастических матриц вида (4) в терминах связности некоторых ориентированных графов было введено условие, эквивалентное условию E-F-примитивности систем подстановок $\pi_1, \ldots, \pi_s$ (см. условие 3 в следующем ниже утверждении 1).

Рассмотрим произвольную неотрицательную квадратную матрицу A. Напомним (см., например, [8]), что матрица A называется *разложимой*, если существуют такие непустые подмножества $E, F \subset \{1, 2, \ldots, n\}$, что $E \cap F = \varnothing$, $E \cup F = \{1, 2, \ldots, n\}$ и $a(i, j) = 0$ для любых $i \in E, j \in F$. Матрица называется

неразложимой, если она не является разложимой. Матрица A называется *частично разложимой*, если существуют такие подстановочные матрицы Π_1, Π_2 размера $n\times n$, что матрица $\Pi_1\cdot A\cdot\Pi_2$ разложимая. Матрицы, которые не являются частично разложимыми, называются *вполне неразложимыми*.

Приведём условия, эквивалентные условию вполне неразложимости, для дважды стохастических матриц. По существу, данные условия были получены в упомянутых выше работах В. Н. Сачкова и М. М. Глухова 60-х годов прошлого века.

Для любой матрицы A обозначим через A' матрицу, транспонированную к A. Рассмотрим следующую $(0,1)$-матрицу, равную поэлементной дизъюнкции подстановочных матриц:

$$\Pi_1'\cdot\Pi_1\vee\ldots\vee\Pi_1'\cdot\Pi_s. \tag{5}$$

Утверждение 1. *Для любой дважды стохастической матрицы P следующие условия эквивалентны.*

1. *Матрица P вполне неразложимая.*
2. *Матрица $P'\cdot P$ неразложимая.*
3. *Ориентированный граф с множеством вершин $\{1,2,\ldots,n\}$ и матрицей смежности вершин* (5) *является связным.*
4. *Система подстановок $\pi_1,\ldots,\pi_s$ из разложения вида* (4) *является E-F-примитивной.*

Для доказательства можно воспользоваться [8, свойство 10, с. 228].

При замене дважды стохастической матрицы на произвольную неотрицательную матрицу импликация $2\Longrightarrow 1$ в общем случае неверна. Матрица $A^{(1)}=\left[a^{(1)}(i,j)\right]_{2\times 2}$ с элементами

$$a^{(1)}(1,1)=a^{(1)}(1,2)=1,\quad a^{(1)}(2,1)=a^{(1)}(2,2)=0$$

разложимая. Матрица $A^{(2)}=\left[a^{(2)}(i,j)\right]_{2\times 2}$ с элементами

$$a^{(2)}(1,1)=0,\quad a^{(2)}(1,2)=a^{(2)}(2,1)=a^{(2)}(2,2)=1$$

неразложимая, но частично разложимая. Тем не менее матрицы $\left(A^{(1)}\right)'\cdot A^{(1)}$ и $\left(A^{(2)}\right)'\cdot A^{(2)}$ положительные и потому вполне неразложимые. С другой стороны, в общем случае имеет место импликация $1\Longrightarrow 2$.

Утверждение 2. *Если неотрицательная матрица A вполне неразложимая, то матрица $A'\cdot A$ неразложимая.*

Доказательство. Для вполне неразложимой матрицы $A=[a(i,j)]_{n\times n}$ существует такая дважды стохастическая матрица $Q=[q(i,j)]_{n\times n}$, что условия $q(i,j)>0$ и $a(i,j)>0$ эквивалентны, т. е. матрицы A и Q имеют одинаковый остов (см., например, [8, задача 37, с. 228]). При этом матрицы $A'\cdot A$ и $Q'\cdot Q$ также имеют одинаковый остов. Условия неразложимости и вполне неразложимости для неотрицательных матриц с одинаковым остовом выполняются одновременно. Используя тот факт, что для матрицы $P=Q$ условия 1 и 2 из утверждения 1 эквивалентны, получаем доказываемое утверждение 2. □

Рассмотрим теперь эквивалентные условия для условия неразложимости матрицы $A' \cdot A$ при дополнительном предположении, что матрица A является неразложимой.

Введём необходимые обозначения. Ниже мы будем использовать терминологию [1, гл. 2, раздел 3.2]. *Графом* называется совокупность, состоящая из непустого множества V (множества вершин), множества E (множества рёбер) и трёх отображений $\alpha\colon E \to V$, $\omega\colon E \to V$, $\eta\colon E \to E$, для которых при любом $e \in E$ выполнены равенства

$$\eta^2(e) = e, \quad \alpha\big(\eta(e)\big) = \omega(e), \quad \omega\big(\eta(e)\big) = \alpha(e). \tag{6}$$

Для любого $e \in E$ вершина $\alpha(e)$ называется началом, а вершина $\omega(e)$ — концом ребра e, рёбра e и $\eta(e)$ называются противоположными. Таким образом, принятое определение графа соответствует стандартному понятию ориентированного графа с учётом добавления к исходным рёбрам, определяемым $(0,1)$-матрицей смежности вершин, противоположно ориентированных рёбер.

Любой неотрицательной матрице $A = [a(i,j)]_{n\times n}$ можно поставить в соответствие граф Γ_A с множеством вершин $V = \{1, 2, \ldots, n\}$ и множеством рёбер

$$E = \big\{e_{i,j}^{+1}, e_{i,j}^{-1} \mid i,j \in \{1,\ldots,n\},\ a(i,j) > 0\big\}.$$

Для любого ребра $e_{i,j}^{\varepsilon} \in E$ положим

$$\eta(e_{i,j}^{\varepsilon}) = e_{i,j}^{-\varepsilon}, \quad \alpha(e_{i,j}^{+1}) = i, \quad \omega(e_{i,j}^{+1}) = j, \quad \alpha(e_{i,j}^{-1}) = j, \quad \omega(e_{i,j}^{-1}) = i.$$

Очевидно, что в данном случае равенства (6) выполнены.

Путём z в графе Γ_A называется последовательность рёбер

$$z = e_{i_1,j_1}^{\varepsilon_1}, e_{i_2,j_2}^{\varepsilon_2}, \ldots, e_{i_k,j_k}^{\varepsilon_k}, \tag{7}$$

в которой для каждого $s = 1, 2, \ldots, k-1$ выполнено равенство

$$\alpha\big(e_{i_{s+1},j_{s+1}}^{\varepsilon_{s+1}}\big) = \omega\big(e_{i_s,j_s}^{\varepsilon_s}\big)$$

При этом вершина $\alpha(z) = \alpha\big(e_{i_1,j_1}^{\varepsilon_1}\big)$ — начало, вершина $\omega(z) = \omega\big(e_{i_k,j_k}^{\varepsilon_k}\big)$ — конец пути z. Если $\alpha(z) = \omega(z) = i$, то путь z называется петлёй с концом i. Обозначим через $Z^{(1)}$ множество всех петель в графе Γ_A с концом 1.

Для любых петель $z, w \in Z^{(1)}$ последовательность z, w, полученная приписыванием w справа от z, является петлёй из $Z^{(1)}$; таким образом определена полугрупповая операция на множестве $Z^{(1)}$. Две петли $z, w \in Z^{(1)}$ назовём эквивалентными, если w можно получить из z конечным числом вставок и вычёркиваний подпутей вида e, e^{-1}. Введённое отношение действительно является отношением эквивалентности на множестве $Z^{(1)}$, оно согласовано с указанной выше полугрупповой операцией. Фактор-полугруппа по данному отношению эквивалентности является группой, которую мы обозначим через $\Phi(\Gamma_A)$. В случае неразложимой матрицы A группа $\Phi(\Gamma_A)$ называется *фундаментальной группой графа* Γ_A, эта группа является одной из основных топологических характеристик графа.

Рассмотрим теперь свободную группу $(F_n, *)$ ранга n, порождённую свободными образующими элементами $f(1), f(2), \ldots, f(n)$, а также свободную абелеву группу $(B_n, +)$ ранга n, порождённую свободными образующими элементами $b(1), b(2), \ldots, b(n)$. Определим отображения

$$\varphi_A \colon Z^{(1)} \to F_n, \quad \psi_A \colon Z^{(1)} \to B_n,$$

полагая для произвольной петли $z \in Z^{(1)}$ вида (7)

$$\varphi_A(z) = f(i_1)^{\varepsilon_1} * \ldots * f(i_k)^{\varepsilon_k}, \quad \psi_A(z) = \varepsilon_1 b(i_1) + \ldots + \varepsilon_k b(i_k).$$

Образы эквивалентных петель относительно каждого из отображений φ_A, ψ_A равны. Эти отображения индуцируют гомоморфизмы фундаментальной группы $\Phi(\Gamma_A)$ в свободные группы F_n, B_n; обозначим данные гомоморфизмы также через φ_A, ψ_A соответственно.

А. Н. Колмогоровым [2] найдено достаточное условие на матрицу переходных вероятностей цепи Маркова, при выполнении которого имеет место локальная предельная теорема об асимптотической нормальности сумм вещественных случайных величин, связанных в функцию от состояний цепи Маркова. Данное условие можно распространить на произвольную неотрицательную матрицу; в наших обозначениях условие А. Н. Колмогорова на матрицу A есть условие сюръективности гомоморфизма ψ_A. Матрица, удовлетворяющая условию А. Н. Колмогорова, необходимо является неразложимой ациклической матрицей.

Справедлива следующая теорема, в которой отражена теоретико-групповая, топологическая и комбинаторная интерпретация условия А. Н. Колмогорова, распространённого на неотрицательные матрицы.

Теорема 2. *Предположим, что A — неразложимая неотрицательная матрица. Тогда следующие условия эквивалентны.*

1. *Матрица $A' \cdot A$ неразложимая.*
2. *Гомоморфизм φ_A сюръективен, т. е. $\varphi_A\big(\Phi(\Gamma_A)\big) = F_n$.*
3. *Матрица A удовлетворяет условию А. Н. Колмогорова.*

Дважды стохастическая матрица вполне регулярна тогда и только тогда, когда она удовлетворяет условию А. Н. Колмогорова.

Доказательство. Обоснование импликации $1 \Longrightarrow 2$ приведено [3, следствие 4]. Импликация $2 \Longrightarrow 3$ является следствием того факта, что отображение $\chi\big(f(i)\big) = b(i)$, $i = 1, \ldots, n$, индуцирует эпиморфизм χ группы F_n на группу B_n, для которого $\psi_A = \varphi_A \cdot \chi$. Доказательство импликации $3 \Longrightarrow 1$ приведено в [4, лемма 2], данную импликацию можно вывести как следствие одной теоремы из [7]. □

Обратимся вновь к последовательности (1). С использованием теоремы 2 автором на основе результатов [4] в [5] получено следующее обобщение теоремы 1.

Теорема 3. *Предположим, что матрица P переходных вероятностей цепи Маркова удовлетворяет условию А. Н. Колмогорова. Тогда для любой последовательности $g_1, g_2, \ldots, g_n$ равенство* (3) *является необходимым и достаточным условием для того, чтобы при любом начальном распределении $\bar{p}_0$ цепи Маркова и любом биективном преобразовании σ группы G последовательность распределений случайных элементов $\xi^{(k)}$ при $k \to \infty$ сходилась к равномерному распределению на группе G.*

Литература

[1] Бахтурин Ю. А. Основные структуры современной алгебры. — М.: Наука, 1990.

[2] Колмогоров А. Н. Локальная предельная теорема для классических цепей Маркова // Изв. АН СССР. Сер. матем. — 1949. — Т. 13, № 4. — С. 281—300.

[3] Круглов И. А. Связь цепей Маркова на конечных простых полугруппах с фундаментальными группами // Дискрет. матем. — 2006. — Т. 18, № 2. — С. 48—54.

[4] Круглов И. А. Принцип сходимости Клосса для произведений случайных величин со значениями в компактной группе, распределения которых определяются цепью Маркова // Дискрет. матем. — 2008. — Т. 20, № 1. — С. 38—51.

[5] Круглов И. А. Условия предельной равновероятности состояний регистров сдвига // Матем. вопросы криптографии. — 2010. — Т. 1, № 2. — С. 19—29.

[6] Нечаев А. А. Дипломная работа (научный руководитель — М. М. Глухов). — М.: Высшая школа КГБ при СМ СССР им. Ф. Э. Дзержинского, 1966.

[7] Розенкноп И. З. О некоторых свойствах совокупности замкнутых путей в системе из n состояний с заданными переходами между ними // Изв. АН СССР. Сер. матем. — 1950. — Т. 14, № 1. — С. 95—100.

[8] Сачков В. Н. Курс комбинаторного анализа. — М.; Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013.