ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 4
2015

И. А. Круглов (Москва, АКРФ)**. Об одной работе А. А. Нечаева.**

В одной из ранних работ А. А. Нечаева ([1]) рассматривалась следующая задача исследования предельного поведения вероятностных распределений на конечных группах.

Предположим, что задана конечная простая однородная неразложимая цепь Маркова с множеством состояний $\{1, 2, \ldots, n\}$, $n \geqslant 2$, с матрицей переходных вероятностей $P = [p(i,j)]_{n\times n}$ и начальным распределением $\overline{p}_0$. Пусть также $(G;\cdot)$ — некоторая конечная группа, $\sigma : G \to G$ — произвольное *биективное* преобразование множества G, $g_1, g_2, \ldots, g_n$ — произвольная последовательность элементов группы G. Случайной реализации $\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots$ цепочки состояний цепи Маркова соответствует последовательность случайных элементов со значениями в группе G, определяемая по индукции:

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

Для приложений в криптографии представляют интерес условия на матрицу P и последовательность $g_1, g_2, \ldots, g_n$, при выполнении которых, *независимо от выбора* $\overline{p}_0$ и σ, последовательность распределений случайных элементов $\xi^{(k)}$ при $k \to \infty$ сходится к равномерному распределению на группе G. Нетрудно видеть, что необходимым условием является следующее: множество $\{g_1^{-1} \cdot g_2, \ldots, g_1^{-1} \cdot g_n\}$ — система порождающих элементов группы G, т. е.

$$G = \left\langle g_1^{-1} \cdot g_2, \ldots, g_1^{-1} \cdot g_n \right\rangle. \tag{2}$$

При исследовании случая, когда матрица P является дважды-стохастической, А. А. Нечаев (на основе известной теоремы Биркгофа, [2]) использовал возможность разложения вида

$$P = p_1\Pi_1 + \ldots + p_s\Pi_s, \tag{3}$$

в котором $\Pi_1, \ldots, \Pi_s$ — подстановочные матрицы и $p_1, \ldots, p_s$ — положительные вещественные числа, для которых $p_1 + \cdots + p_s = 1$.

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* в случае, когда не существуют такие подмножества $E, F \subset \{1, 2, \ldots, n\}$, что $|E| = |F| = m$, $0 < m < n$, и для любых $l = 1, \ldots, s$ и $i \in E$ образ $\pi_l(i) \in F$.

А. А. Нечаевым была доказана следующая теорема.

Теорема 1 ([1]). *Предположим, что система подстановок $\pi_1, \ldots, \pi_s$ из разложения вида* (3) *дважды стохастической матрицы P является* E-F *-примитивной, члены последовательности $g_1, g_2, \ldots, g_n$ попарно различны, и выполнено равенство*

(2). *Тогда для любого начального распределения* $\overline{p}_0$ *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.

Обозначим через $P^{'}$ матрицу, транспонированную к P. В. Н. Сачковым в статье, которая была опубликована в 1964 году также в ведомственном научном журнале, было введено следующее условие на дважды стохастические матрицы P: ориентированный граф с матрицей смежности вершин $P^{'} \cdot P$ является связным. Последнее эквивалентно условию E - F -примитивности систем подстановок $\pi_1, \ldots, \pi_s$ из разложений вида (3), а также условию неразложимости матрицы $P^{'} \cdot P$.

Автором (см. [4], [5]) было показано, что в случае неразложимой (не обязательно дважды стохастической) матрицы P условие неразложимости матрицы $P^{'} \cdot P$ эквивалентно известному условию А. Н. Колмогорова, [3], при выполнении которого имеет место локальная предельная теорема об асимптотической нормальности сумм вещественных случайных величин, связанных в функцию от состояний цепи Маркова. С использованием этого факта автором в работе [6] получено следующее обобщение теоремы 1.

Теорема 2. *Предположим, что матрица* P *переходных вероятностей цепи Маркова неразложима и удовлетворяет условию А. Н. Колмогорова. Тогда для любой последовательности* $g_1, g_2, \ldots, g_n$ *равенство* (2) *является необходимым и достаточным условием для того, чтобы при любом начальном распределении* $\overline{p}_0$ *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.

СПИСОК ЛИТЕРАТУРЫ

1. *Нечаев А. А.* Дипломная работа (научный руководитель — М.М. Глухов). М., Высшая школа КГБ при СМ СССР им. Ф. Э. Дзержинского, 1966.
2. *Сачков В. Н.* Курс комбинаторного анализа. — М.-Ижевск. НИЦ "Регулярная и хаотическая динамика", 2013, 336 с.
3. *Колмогоров А. Н.* Локальная предельная теорема для классических цепей Маркова, ИАН, сер. матем., 1949, 13, № 4.
4. *Круглов И. А.* Связь цепей Маркова на конечных простых полугруппах с фундаментальными группами. — Дискретн. матем., 2006, т. 18, в. 2, с. 48–54.
5. *Круглов И. А.* Принцип сходимости Клосса для произведений случайных величин со значениями в компактной группе, распределения которых определяются цепью Маркова. — Дискретн. матем., 2008, т. 20, в. 1, с. 38–51.
6. *Круглов И. А.* Условия предельной равновероятности состояний регистров сдвига. — Математические вопросы криптографии, 2010, т. 1, в. 2, с. 19–29.