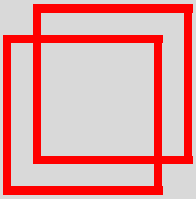
Math-Net.Ru
All Russian mathematical portal

I. A. Kruglov, The estimate of the convergence rate to the uniform distribution for products of elements of finite group controlled by a Markov chain,
Mat. Vopr. Kriptogr., 2014, Volume 5, Issue 1, 85–94

https://www.mathnet.ru/eng/mvk108

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.14.81
May 23, 2025, 08:36:06

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2014 Т. 5 № 1 С. 85–94

УДК: 519.217.2

Оценка скорости сходимости к равномерному распределению для произведений элементов конечной группы, управляемых цепью Маркова

И. А. Круглов

ООО «Центр сертификационных исследований», Москва

Получено 22.IV.2013

Для произведений случайных подстановок, управляемых цепью Маркова, получена верхняя оценка среднеквадратического отклонения матриц вероятностей переходов, порожденных этими произведениями, от стохастической матрицы с одинаковыми элементами.

Ключевые слова: цепи Маркова, группы подстановок, матрицы вероятностей переходов

The estimate of the convergence rate to the uniform distribution for products of elements of finite group controlled by a Markov chain

I. A. Kruglov

LLC "Sertification Research Center", Moscow

Abstract. For products of random substitutions controlled by a Markov chain we obtain an upper bound for the mean-square deviation of transition matrices corresponding to these products from the stochastic matrix with equal elements.

Key words: Markov chain, substitution groups, transition probability matrices

Citation: *Mathematical Aspects of Cryptography*, 2014, vol. 5, no. 1, pp. 85–94 (Russian).

© 2014 И. А. Круглов

Рассмотрим конечную простую однородную цепь Маркова

$$\alpha_1, \alpha_2, \ldots, \alpha_N, \alpha_{N+1}, \ldots$$

со множеством состояний $\{1, 2, \ldots, n\}$, матрицей переходных вероятностей $P = [p(i,j)]_{i,j=1}^{n}$ и вектором начального распределения $\overline{p}_0$. Рассмотрим также произвольную конечную группу G с групповой операцией «$*$» и предположим, что для любых $i, j \in \{1, 2, \ldots, n\}$ задана последовательность $\{\xi_{i,j}^{(N)}\}_{N\geq 1}$ одинаково распределенных случайных элементов со значениями в группе G, распределения которых совпадают с распределением случайного элемента $\xi_{i,j}$, причем случайные элементы $\xi_{i,j}^{(N)}$, $N \geq 1$, $i, j \in \{1, \ldots, n\}$, независимы между собой и не зависят от цепи Маркова $\{\alpha_N\}_{N\geq 1}$. При любом $N \geq 1$ определим произведение случайных элементов

$$\eta^{(N)} = \xi_{\alpha_1,\alpha_2}^{(1)} * \xi_{\alpha_2,\alpha_3}^{(2)} * \ldots * \xi_{\alpha_N,\alpha_{N+1}}^{(N)}.$$

Пусть q — произвольное подстановочное представление группы G подстановками непустого конечного множества S, $m = |S|$ — степень представления q. Для любого случайного элемента ξ со значениями в группе G определена матрица переходных вероятностей (см. [1, § 1])

$$\Pi_{\xi}^{(q)} = \left[p_{\xi}^{(q)}(\alpha, \beta)\right]_{\alpha,\beta\in S},$$

где для любых $\alpha, \beta \in S$

$$p_{\xi}^{(q)}(\alpha, \beta) = \sum_{\tau\in G_{\alpha,\beta}} \mathsf{P}(\xi = \tau), \quad G_{\alpha,\beta} = \left\{\tau \in G | \alpha^{q(\tau)} = \beta\right\}.$$

Автором в § 3 работы [1] было показано, что при выполнении широких условий последовательность матриц переходных вероятностей $\left\{\Pi_{\eta^{(N)}}^{(q)}\right\}_{N\geq 1}$ сходится при $N \to \infty$ к матрице $\left[\frac{1}{m}\right]$ размеров $m \times m$, все элементы которой равны $\frac{1}{m}$. При этом из доказательства следует, что в случае наличия такой сходимости для величин

$$\varepsilon_N = \max_{\alpha\in S}\left(\sum_{\beta\in S}\left(p_{\xi}^{(q)}(\alpha, \beta) - \frac{1}{m}\right)^2\right)^{\frac{1}{2}}, \quad N \geq 1,$$

справедлива экспоненциальная оценка порядка скорости сходимости к 0 при $N \to \infty$. Оценке порядка скорости сходимости величин ε_N к нулю в одном

частном случае посвящена также работа автора [2]. Однако ее результаты имеют лишь качественный характер.

В настоящей работе получена явная экспоненциальная оценка сверху для величины ε_N в виде неравенства. Найдены дополнительные условия, при выполнении которых основание экспоненты строго меньше единицы. Основные из них состоят в том, что матрица P переходных вероятностей цепи Маркова должна быть дважды стохастической и вполне неразложимой (т. е. при вычеркивании любой строки и любого столбца перманент получающейся матрицы должен быть положительным). Отметим, что впервые такие условия для доказательства сходимости к матрице вида $\left[\frac{1}{m}\right]$ (в том числе и для неоднородных цепей Маркова) были эффективно использованы В. Н. Сачковым [3].

Введем обозначения, необходимые для формулировки основного результата работы. Пусть для любого $\sigma \in G$ и любых $\alpha, \beta \in S$

$$Q_{\alpha,\beta}(\sigma) = \begin{cases} 1, & \alpha^{q(\sigma)} = \beta, \\ 0, & \alpha^{q(\sigma)} \neq \beta. \end{cases}$$

Рассмотрим матричное представление Q группы G, где

$$Q(\sigma) = \left[Q_{\alpha,\beta}(\sigma)\right]_{\alpha,\beta\in S}, \quad \sigma \in G,$$

соответствующее подстановочному представлению q. Выберем произвольное множество $\widehat{\mathsf{G}}^{(q)}$ попарно неэквивалентных неприводимых унитарных матричных представлений группы G над полем комплексных чисел, для которого любая неприводимая компонента представления Q группы G эквивалентна ровно одному представлению из множества $\widehat{\mathsf{G}}^{(q)}$. Для любого случайного элемента ξ со значениями в группе G определена матричная характеристическая функция матрицы переходных вероятностей $\Pi_\xi^{(q)}$ (см. [1]):

$$\Phi_\xi(U) = \sum_{\sigma\in G} \mathsf{P}\,(\xi = \sigma)\, U(\sigma), \quad U \in \widehat{\mathsf{G}}^{(q)}.$$

Рассмотрим произвольное представление $U \in \widehat{\mathsf{G}}^{(q)}$ степени n_U. Определим блочную квадратную матрицу

$$\Phi(U) = \begin{bmatrix} \Phi_{1,1}(U) & \Phi_{1,2}(U) & \dots & \Phi_{1,n}(U) \\ \Phi_{2,1}(U) & \Phi_{2,2}(U) & \dots & \Phi_{2,n}(U) \\ \vdots & \vdots & \vdots & \vdots \\ \Phi_{n,1}(U) & \Phi_{n,2}(U) & \dots & \Phi_{n,n}(U) \end{bmatrix}$$

порядка nn_U с n^2 квадратными блоками порядка n_U, у которой для любых $i, j \in \{1, \ldots, n\}$ на месте i, j стоит блок

$$\Phi_{i,j}(U) = p(i,j)\Phi_{\xi_{i,j}}(U). \tag{1}$$

Для произвольного вектора α унитарного пространства над полем комплексных чисел через $\|\alpha\|$ обозначим его евклидову норму, порожденную скалярным произведением в данном пространстве. При любом $U \in \widehat{\mathsf{G}}^{(q)}$ обозначим через $\|\Phi(U)\|$ эрмитову норму матрицы $\Phi(U)$ как линейного преобразования унитарного пространства вектор-столбцов длины nn_U над полем комплексных чисел. Пусть $U_0 \in \widehat{\mathsf{G}}^{(q)}$ — (одномерное) единичное представление группы G, определяемое соотношением

$$U_0(g) = 1 \quad \forall g \in G.$$

Положим

$$\lambda = \max\left\{\|\Phi(U)\| \colon U \in \widehat{\mathsf{G}}^{(q)}, U \neq U_0\right\}. \tag{2}$$

Для произвольного случайного элемента ξ со значениями в группе G обозначим

$$\Omega(\xi) = \{\sigma \in G \colon \mathsf{P}(\xi = \sigma) > 0\}$$

носитель его распределения. Рассмотрим множество Z последовательностей вида

$$\begin{gathered} z = (j_0 = 1, i_1, j_1, i_2, j_2, \ldots, j_{s-1}, i_s, j_s, \ldots, i_{N-1}, j_{N-1}, i_N, j_N = 1), \\ N \geq 1, \quad i_s, j_s \in \{1, \ldots, n\}, \end{gathered} \tag{3}$$

удовлетворяющих условиям

$$p(i_s, j_{s-1})p(i_s, j_s) > 0 \quad \forall s \in \{1, \ldots, N\}.$$

Для любой последовательности вида (3) определим следующее множество элементов группы G:

$$\begin{gathered} \Omega(z) = \Omega\left(\xi_{i_1,1}\right)^{-1} * \Omega\left(\xi_{i_1,j_1}\right) * \ldots * \Omega\left(\xi_{i_s,j_{s-1}}\right)^{-1} * \Omega\left(\xi_{i_s,j_s}\right) * \ldots \\ \ldots * \Omega\left(\xi_{i_N,j_{N-1}}\right)^{-1} * \Omega\left(\xi_{i_N,1}\right). \end{gathered}$$

Для любых последовательностей $z_1, z_2 \in Z$ рассмотрим последовательность $z \in Z$, полученную путем удаления из z_2 первого элемента, равного 1,

и приписывания результата к z_1 справа. Имеет место равенство множеств $\Omega(z) = \Omega(z_1) * \Omega(z_2)$. Следовательно, объединение множеств

$$H = \bigcup_{z \in Z} \Omega(z)$$

замкнуто относительно групповой операции и поэтому является подгруппой конечной группы G.

Используя введенные обозначения, сформулируем основной результат настоящей работы.

Теорема. *1) Справедливо неравенство*

$$\varepsilon_N \leq \sqrt{n} \|\overline{p}_0\| \lambda^N \quad \forall N \geq 1. \tag{4}$$

2) Если P — вполне неразложимая дважды стохастическая матрица и группа подстановок $q(H)$ транзитивна на множестве S, то

$$0 \leq \lambda < 1. \tag{5}$$

Доказательство. 1) Пусть вектор начальных вероятностей цепи Маркова $\{\alpha_N\}_{N \geq 1}$ имеет вид

$$\overline{p}_0 = (p_0(1), p_0(2), \ldots, p_0(n)), \quad p_0(1) + \ldots + p_0(n) = 1,$$
$$p_0(i) \geq 0 \quad \forall i \in \{1, \ldots, n\}.$$

Для любого представления $U \in \widehat{\mathsf{G}}^{(q)}$ степени n_U определим следующие блочные матрицы $A(U), B(U)$ размеров $n_U \times (nn_U)$, $(nn_U) \times n_U$ соответственно:

$$A(U) = \left[\begin{array}{cccc} p_0(1)E_{n_U} & p_0(2)E_{n_U} & \ldots & p_0(n)E_{n_U} \end{array} \right],$$

$$B(U) = \left[\begin{array}{c} E_{n_U} \\ E_{n_U} \\ \vdots \\ E_{n_U} \end{array} \right],$$

где E_{n_U} — единичная квадратная матрица порядка n_U. Покажем, что для любых $N \geq 1, U \in \widehat{\mathsf{G}}^{(q)}$ имеет место равенство

$$\Phi_{\eta^{(N)}}(U) = A(U)\Phi(U)^N B(U). \tag{6}$$

Для любой последовательности

$$l_1, l_2, \ldots, l_N, l_{N+1} \in \{1, \ldots, n\}$$

условное распределение случайного элемента $\eta^{(N)}$ при условии

$$\alpha_1 = l_1, \alpha_2 = l_2, \ldots, \alpha_N = l_N, \alpha_{N+1} = l_{N+1},$$

совпадает с распределением произведения независимых случайных элементов

$$\xi^{(1)}_{l_1,l_2} * \xi^{(2)}_{l_2,l_3} * \ldots * \xi^{(N)}_{l_N,l_{N+1}}.$$

Из формулы полной вероятности и теоремы умножения для матричных характеристических функций (см. [1]) следует равенство

$$\Phi_{\eta^{(N)}}(U) = \sum_{l_1,\ldots,l_{N+1}=1}^{n} p_0(l_1)p(l_1,l_2)\Phi_{\xi^{(1)}_{l_1,l_2}}(U)\times$$
$$\times p(l_2,l_3)\Phi_{\xi^{(2)}_{l_2,l_3}}(U)\ldots p(l_N,l_{N+1})\Phi_{\xi^{(N)}_{l_N,l_{N+1}}}(U).$$

Правая часть последнего равенства, в соответствии с соотношением (1) и правилами умножения блочных матриц, совпадает с правой частью равенства (6).

Для любых $N \geq 1, U \in \widehat{\mathsf{G}}^{(q)}$ из соотношения (6) и свойства мультипликативности эрмитовой нормы линейных отображений унитарных пространств следует неравенство

$$\left\|\Phi_{\eta^{(N)}}(U)\right\| \leq \|A(U)\| \cdot \|\Phi(U)\|^N \cdot \|B(U)\|. \tag{7}$$

Можно показать, что при любом $U \in \widehat{\mathsf{G}}^{(q)}$

$$\|A(U)\| = \|\overline{p}_0\|, \quad \|B(U)\| = n^{\frac{1}{2}}. \tag{8}$$

Обозначим через k_U кратность неприводимой компоненты $U \in \widehat{\mathsf{G}}^{(q)}$ представления Q. Доказываемое соотношение (4) следует из соотношений (7), (2), (8), равенства для степени представления Q

$$m = \sum_{U \in \widehat{\mathsf{G}}^{(q)}} n_U \, k_U,$$

и следующего неравенства, доказанного в [4]:

$$\varepsilon_N^2 \le \frac{1}{m} \sum_{U \in \widehat{\mathsf{G}}^{(q)}, U \ne U_0} n_U k_U \|\Phi_{\eta^{(N)}}(U)\|^2.$$

2) Для любой комплексной матрицы C обозначим через $C^\top$ транспонированную матрицу к матрице C и для любого представления $U \in \widehat{\mathsf{G}}^{(q)}$ обозначим через $\Phi(U)^*$ сопряженную матрицу к матрице $\Phi(U)$, где

$$\Phi(U)^* = \overline{\Phi(U)}^\top,$$

черта сверху обозначает взятие комплексно сопряженных элементов к элементам матрицы. Известно (см., например, [5]), что величина $\|\Phi(U)\|^2$ равна максимальному из модулей собственных чисел матрицы

$$\Lambda(U) = \Phi(U)^* \Phi(U). \tag{9}$$

Следовательно, для доказательства неравенства (5) достаточно показать, что для любого представления $U \in \widehat{\mathsf{G}}^{(q)}, U \ne U_0$, все собственные числа матрицы $\Lambda(U)$ по модулю строго меньше 1.

Введем матрицу $R = P^\top P = [r(i,j)]$. Из условия пункта 2) теоремы на матрицу P и результатов работы [3] следует, что R — (вполне) неразложимая дважды стохастическая матрица.

Для любых $i, j \in \{1, \dots, n\}$, удовлетворяющих условию $r(i,j) > 0$, рассмотрим непустое множество

$$L_{i,j} = \{l \in \{1, \dots, n\} \colon p(l,i)p(l,j) > 0\},$$

а также случайный элемент $\zeta_{i,j}$ со значениями в группе G с распределением

$$\mathsf{P}\left(\zeta_{i,j} = \sigma\right) = \frac{1}{r(i,j)} \sum_{l \in L_{i,j}} p(l,i)p(l,j)\mathsf{P}\left((\xi_{l,i}^{(1)})^{-1} * \xi_{l,j}^{(2)} = \sigma\right) \quad \forall \sigma \in G \tag{10}$$

и носителем распределения

$$\Omega\left(\zeta_{i,j}\right) = \bigcup_{l \in L_{i,j}} \left(\Omega\left(\xi_{l,i}\right)^{-1} * \Omega\left(\xi_{l,j}\right)\right). \tag{11}$$

Из соотношений (1), (10), свойства унитарности представлений U и теоремы умножения для матричных характеристических функций для любых $i, j \in \in \{1, \ldots, n\}$ и $U \in \widehat{\mathsf{G}}^{(q)}$ следуют равенства

$$r(i,j)\Phi_{\zeta_{i,j}}(U) = \sum_{l=1}^{n} p(l,i)\Phi_{\xi_{l,i}}(U)^* p(l,j)\Phi_{\xi_{l,j}}(U) = \sum_{l=1}^{n} \Phi_{l,i}(U)^* \Phi_{l,j}(U). \quad (12)$$

Вследствие соотношений (9) и (12) матрица $\Lambda(U)$ является блочной матрицей

$$\Lambda(U) = \begin{bmatrix} \Lambda_{1,1}(U) & \Lambda_{1,2}(U) & \ldots & \Lambda_{1,n}(U) \\ \Lambda_{2,1}(U) & \Lambda_{2,2}(U) & \ldots & \Lambda_{2,n}(U) \\ \vdots & \vdots & \vdots & \vdots \\ \Lambda_{n,1}(U) & \Lambda_{n,2}(U) & \ldots & \Lambda_{n,n}(U) \end{bmatrix}$$

с n^2 квадратными блоками порядка n_U, у которой для любых $i, j \in \{1, \ldots, n\}$ на месте i, j стоит блок

$$\Lambda_{i,j}(U) = r(i,j)\Phi_{\zeta_{i,j}}(U).$$

Необходимые и достаточные условия существования у таких блочных матриц собственных чисел, по модулю равных 1, получены автором в лемме из § 3 работы [1]. Эти условия сформулированы в терминах свойств некоторой подгруппы группы G, которая, в свою очередь, описывается в терминах ненулевых элементов матрицы R и множеств $\Omega(\zeta_{i,j})$ для $i, j \in \{1, \ldots, n\}$, удовлетворяющих неравенству $r(i,j) > 0$. Используя равенства (11), можно показать, что в нашем случае эта подгруппа совпадает с определенной выше подгруппой H.

Таким образом, по лемме из § 3 работы [1] для любого представления $U \in \widehat{\mathsf{G}}^{(q)}$ матрица $\Lambda(U)$ имеет собственное число, по модулю большее или равное 1, тогда и только тогда, когда U является неприводимой компонентой индуцированного представления группы G единичным представлением ее подгруппы H. Это условие по теореме взаимности Фробениуса равносильно наличию единичной неприводимой компоненты у ограничения представления U на подгруппу H. Следовательно, количество представлений $U \in \widehat{\mathsf{G}}^{(q)}$ с рассматриваемым свойством матрицы $\Lambda(U)$ не превосходит числа единичных компонент ограничения представления Q на подгруппу H, т. е. числа орбит группы подстановок $q(H)$ на множестве S. Это число равно единице, так как по условию 2) формулировки теоремы группа подстановок $q(H)$ транзитивна на множестве S. Итак, матрица $\Lambda(U)$ может иметь собственное число,

по модулю большее или равное 1, не более чем для одного представления $U \in \widehat{\mathsf{G}}^{(q)}$.

С другой стороны, единичное представление $U_0 \in \widehat{\mathsf{G}}^{(q)}$, а матрица $\Lambda(U_0) = R$ имеет собственное число, равное 1. Следовательно, для любого представления $U \in \widehat{\mathsf{G}}^{(q)}$, $U \neq U_0$, все собственные числа матрицы $\Lambda(U)$ строго меньше 1. Согласно соотношению (2), имеет место двойное неравенство (5). Теорема доказана.

Приведем условия, при выполнении которых проверка соотношения (5) несколько упрощается. Предположим, что имеет место соотношение

$$\bigcap_{j\in\{1,\ldots,n\}:\, p(i,j)>0} \Omega\left(\xi_{i,j}\right) \neq \oslash \quad \forall i \in \{1,\ldots,n\}. \tag{13}$$

В частности, условие (13) выполняется в случае, когда распределения сомножителей в произведениях $\eta^{(N)}$ определяются состояниями (а не переходами) цепи Маркова $\{\alpha_N\}_{N\geq 1}$, т. е. при выполнении соотношений

$$\xi_{i,j} = \xi_i \quad \forall i,j \in \{1,\ldots,n\}$$

для некоторых случайных элементов $\xi_1,\ldots,\xi_n$ со значениями в группе G.

Зафиксируем произвольные элементы

$$\sigma_{i,j} \in \Omega(\xi_{i,j}) \quad \forall i,j \in \{1,\ldots,n\}$$

и рассмотрим следующее множество элементов группы G:

$$\Omega = \bigcup_{i,j\in\{1,\ldots,n\}:\, p(i,j)>0} \sigma_{i,j}^{-1} * \Omega\left(\xi_{i,j}\right).$$

Следствие. *Если P — вполне неразложимая дважды стохастическая матрица и множество подстановок $q(\Omega)$ порождает транзитивную группу подстановок на множестве S, то верно неравенство* (5).

Доказательство. Согласно п. 2) теоремы достаточно показать, что группа подстановок $q(H)$ транзитивна на множестве S. Как уже упоминалось, R — вполне неразложимая дважды стохастическая матрица. Из соотношений (11) и (13) следует, что

$$e_G \in \Omega\left(\zeta_{i,j}\right) \quad \forall i,j \in \{1,\ldots,n\}\colon r(i,j) > 0.$$

Из результатов работы [6] следует, что при этих условиях множество

$$\bigcup_{i,j\in\{1,\ldots,n\}:\ r(i,j)>0} \Omega\left(\zeta_{i,j}\right)$$

является системой порождающих элементов подгруппы H группы G. Однако при любом $j \in \{1, \ldots, n\}$ имеет место неравенство $r(j, j) > 0$, и, согласно соотношению (11),

$$\sigma_{i,j}^{-1} * \Omega\left(\xi_{i,j}\right) \subseteq \Omega\left(\zeta_{j,j}\right) \quad \forall i, j \in \{1, \ldots, n\} : p(i, j) > 0.$$

Следовательно, $\Omega \subseteq H$, и по условию следствия группа подстановок $q(H)$ транзитивна на множестве S. Следствие доказано.

Список литературы

1. *Горчинский Ю. Н., Круглов И. А., Капитонов В. М.* Вопросы теории распределений на конечных группах // В сб.: Труды по дискретной математике, т. 1. — 1997. — С. 85–112.
2. *Круглов И. А.* Оценка среднеквадратического уклонения от равновероятной матрицы для матриц переходных вероятностей произведений случайных величин со значениями в конечных группах, распределения которых определяются цепью Маркова // Обозр. прикл. и промышл. матем.— 2006. — Т. 13. Вып. 3. — С. 507–509.
3. *Сачков В. Н.* Вероятностные преобразователи и правильные мультиграфы.1 // В сб.: Труды по дискретной математике, т. 1. — 1997. — С. 227–250.
4. *Горчинский Ю. Н., Капитонов В. М.* О средних квадратических уклонениях в строках матриц переходных вероятностей на конечных группах подстановок // В сб.: Труды по дискретной математике, т. 2. — 1998. — С. 88–100.
5. *Гантмахер Ф. Р.* Теория матриц. — М.: Наука, 1988.
6. *Круглов И. А.* Принцип сходимости Б. М. Клосса для произведений случайных величин со значениями в компактной группе, распределения которых определяются цепью Маркова // Дискретная математика. — 2008. — Т. 20. Вып. 1. — С. 38–51.