Math-Net.Ru

Общероссийский математический портал

И. А. Круглов, Скорость сходимости к равномерному распределению в схеме авторегрессии на конечной абелевой группе, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 1, 65–74

DOI: <https://doi.org/10.4213/mvk245>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.85.209

26 апреля 2023 г., 03:44:26

**Скорость сходимости
к равномерному распределению в схеме
авторегрессии на конечной абелевой группе**

И. А. Круглов

Академия криптографии Российской Федерации, Москва

Получено 11.V.2017

Аннотация. Рассматривается схема линейной авторегрессии со случайным управлением на конечной абелевой группе. Доказаны неравенства для среднеквадратического отклонения распределений ее элементов от равномерного распределения.

Ключевые слова: схема авторегрессии на конечной группе, среднеквадратическое отклонение от равномерного распределения

**Rate of convergence to the uniform distribution
for autoregression scheme on the finite Abelian group**

I. A. Kruglov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. The linear autoregression scheme with random control on finite Abelian group is considered. Inequalities for the mean-square deviation of distributions of its elements from the uniform distribution are obtained.

Key words: autoregression scheme on the finite group, mean-square deviation from the uniform distribution

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 1, pp. 65–74 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

В работе исследуется способ образования случайных элементов со значениями в конечных абелевых группах, получивший название схемы линейной авторегрессии со случайным управлением [2].

Пусть $(G, +)$ — конечная абелева группа порядка $|G| \geq 3$ с нейтральным элементом θ , $(\text{Aut } G, \circ)$ — группа автоморфизмов группы G с операцией $\circ$ композиции преобразований, E — тождественный автоморфизм. Образ подмножества $M \subset G$ при действии автоморфизма $A \in \text{Aut } G$ будем обозначать через M^A .

Предположим, что задана последовательность

$$\{(\xi_N, \zeta_N)\}_{N \geq 1} \quad (1)$$

независимых случайных элементов со значениями в декартовом произведении $G \times \text{Aut } G$, члены которой одинаково распределены с некоторым случайным элементом (ξ, ζ) ; случайные элементы ξ и ζ могут быть зависимыми. Предположим также, что задан случайный элемент $\mu^{(0)}$ со значениями в группе G , не зависящий от членов последовательности (1). Определим по индукции последовательность случайных элементов

$$\mu^{(N)} = (\mu^{(N-1)})^{\zeta_N} + \xi_N, \quad N \geq 1. \quad (2)$$

В настоящей работе доказаны оценки сверху в виде неравенств для величин

$$\delta_N^2 = \sum_{\sigma \in G} \left(\mathbf{P}\{\mu^{(N)} = \sigma\} - \frac{1}{|G|} \right)^2, \quad N \geq 1, \quad (3)$$

квадратов среднеквадратических отклонений распределений случайных элементов (2) от равномерного распределения на группе G . Полученные результаты представляют интерес, главным образом, для случая невырожденного распределения ζ . Ранее аналогичные задачи для некоторых частных случаев выбора группы G и распределения (ξ, ζ) решались в работах [2–6].

Введем обозначения. Рассмотрим носитель

$$\Omega(\zeta) = \{A_1, A_2, \dots, A_s\} = \{A \in \text{Aut } G : \mathbf{P}\{\zeta = A\} > 0\}, \quad s \geq 1,$$

распределения случайного элемента ζ . Множество $\Omega(\zeta)$ является системой порождающих элементов некоторой подгруппы $\mathfrak{A}$ группы $\text{Aut } G$.

Обозначим через $(\widehat{G}, \cdot)$ группу неприводимых комплексных характеров группы G с групповой операцией умножения функций, заданных на группе G . Пусть $\chi^{(0)}$ — единичный характер, $\chi^{(0)}(\sigma) = 1$ при любом $\sigma \in G$.

Для любого характера $\chi \in \widehat{G}$ и любого автоморфизма $A \in \mathfrak{A}$ функция $\chi_A(\sigma) = \chi(\sigma^A)$, $\sigma \in G$, также является неприводимым характером группы G . Поэтому A индуцирует групповой автоморфизм $\overline{A}: \widehat{G} \rightarrow \widehat{G}$, определяемый равенством $\chi^{\overline{A}} = \chi_A$, $A \in \mathfrak{A}$. При этом $\overline{A \circ B} = \overline{A} \cdot \overline{B}$ для любых $A, B \in \mathfrak{A}$ (здесь " $\cdot$ " — произведение преобразований). Таким образом, множество $\overline{\mathfrak{A}} = \{\overline{A}: A \in \mathfrak{A}\}$ является подгруппой симметрической группы (т. е. группой подстановок) множества $\widehat{G}$. Соответствие $A \mapsto \overline{A}$ определяет изоморфизм группы $(\mathfrak{A}, \circ)$ на группу $(\overline{\mathfrak{A}}, \cdot)$.

Для группы подстановок $\mathfrak{A}$ на множестве G определено разбиение G на попарно не пересекающиеся орбиты $\Theta_0, \Theta_1, \dots, \Theta_l$ группы $\mathfrak{A}$: элементы $g, \sigma \in G$ содержатся в одном множестве Θ_i тогда и только тогда, когда $g = \sigma^A$ для некоторого преобразования $A \in \mathfrak{A}$. При этом можно считать, что $\Theta_0 = \{\theta\}$.

Аналогично определены орбиты $\overline{\Theta}^{(0)}, \overline{\Theta}^{(1)}, \dots, \overline{\Theta}^{(k)}$ группы подстановок $\overline{\mathfrak{A}}$ на множестве $\widehat{G}$, где $\overline{\Theta}^{(0)} = \{\chi^{(0)}\}$. Зафиксируем произвольно характеры $\chi^{(j)} \in \overline{\Theta}^{(j)}$, $j = 1, 2, \dots, k$.

Для любого случайного элемента η со значениями в группе G определено преобразование Фурье его распределения

$$\Phi(\eta, \chi) = \sum_{g \in G} \mathbf{P}\{\eta = g\} \cdot \chi(g), \quad \chi \in \widehat{G}.$$

Рассмотрим случайный элемент $\tilde{\mu}^{(0)}$, равный разности в группе G двух независимых одинаково распределенных случайных элементов, у которых распределения совпадают с распределением $\mu^{(0)}$. Имеем выражение для распределения $\tilde{\mu}^{(0)}$ и его преобразования Фурье:

$$\begin{aligned} \mathbf{P}\{\tilde{\mu}^{(0)} = g\} &= \sum_{\sigma \in G} \mathbf{P}\{\mu^{(0)} = \sigma\} \cdot \mathbf{P}\{\mu^{(0)} = g + \sigma\}, \quad g \in G, \\ \Phi(\tilde{\mu}^{(0)}, \chi) &= |\Phi(\mu^{(0)}, \chi)|^2, \quad \chi \in \widehat{G}. \end{aligned} \quad (4)$$

Положим

$$\epsilon_0 = \frac{1}{|G|} \sum_{j=1}^k |\overline{\Theta}^{(j)}|^{(2)} \cdot \left[\sum_{i=0}^l \mathbf{P}\{\tilde{\mu}^{(0)} \in \Theta_i\} \cdot \frac{1}{|\Theta_i|} \sum_{g \in \Theta_i} \chi^{(j)}(g) \right]. \quad (5)$$

Ниже (см. соотношение (14)) будет показано, что ϵ_0 — неотрицательное вещественное число.

Пусть $p_\nu = \mathbf{P}\{\zeta = A_\nu\}$, $\nu = 1, 2, \dots, s$. Для любого $\nu = 1, 2, \dots, s$ обозначим через $\xi^{(\nu)}$ случайный элемент со значениями в группе G , распределение которого совпадает с условным распределением случайного элемента ξ при условии $\zeta = A_\nu$. Определим неотрицательные вещественные числа

$$\begin{aligned} \delta_1 &= \max_{j=1, \dots, k} \max_{\chi \in \overline{\Theta}^{(j)}} \sum_{\psi \in \overline{\Theta}^{(j)}} \left| \sum_{\nu, \gamma: \psi = \chi^{(\overline{A}_\nu)^{-1} \overline{A}_\gamma} p_\nu \cdot p_\gamma \cdot \overline{\Phi((\xi^{(\nu)})^{A_\nu^{-1}}, \chi)} \cdot \Phi((\xi^{(\gamma)})^{A_\gamma^{-1}}, \chi) \right|, \\ \delta_2 &= \max_{j=1, \dots, k} \max_{\chi \in \overline{\Theta}^{(j)}} \sum_{\psi \in \overline{\Theta}^{(j)}} \left| \sum_{\nu, \gamma: \psi = \chi^{\overline{A}_\nu \cdot (\overline{A}_\gamma)^{-1}} p_\nu \cdot p_\gamma \cdot \Phi(\xi^{(\nu)}, \chi) \cdot \overline{\Phi((\xi^{(\gamma)})^{A_\nu \circ A_\gamma^{-1}}, \chi)} \right|. \end{aligned} \quad (6)$$

Здесь черта сверху обозначает комплексное сопряжение, пустая сумма считается равной нулю.

Теорема. При $m = 1, 2$ выполнены неравенства

$$\delta_N^2 \leq \epsilon_0 \cdot \delta_m^N, \quad N \geq 1. \quad (7)$$

Доказательство. Согласно равенству Парсевалья

$$\delta_N^2 = \frac{1}{|G|} \sum_{\chi \neq \chi_0} |\Phi(\mu^{(N)}, \chi)|^2 = \frac{1}{|G|} \sum_{j=1}^k \sum_{\chi \in \overline{\Theta}^{(j)}} |\Phi(\mu^{(N)}, \chi)|^2, \quad N \geq 1. \quad (8)$$

Оценим слагаемые в правой части равенства (8). Зафиксируем произвольно $j \in \{1, 2, \dots, k\}$ и характер $\chi \in \overline{\Theta}^{(j)}$, пусть $n_j = |\overline{\Theta}^{(j)}|$. Для любого автоморфизма $A \in \mathfrak{A}$ и любого случайного элемента η со значениями в группе G имеем равенства

$$\begin{aligned} \Phi(\eta^A, \chi) &= \sum_{g \in G} \mathbf{P}\{\eta^A = g\} \cdot \chi(g) = \sum_{g \in G} \mathbf{P}\{\eta = g^{A^{-1}}\} \cdot \chi(g) = \\ &= \sum_{\sigma \in G} \mathbf{P}\{\eta = \sigma\} \cdot \chi(\sigma^A) = \sum_{\sigma \in G} \mathbf{P}\{\eta = \sigma\} \cdot \chi_A(\sigma). \end{aligned}$$

Таким образом,

$$\Phi(\eta^A, \chi) = \Phi(\eta, \chi^{\overline{A}}), \quad \Phi(\eta^{A \circ B}, \chi) = \Phi(\eta, \chi^{\overline{A \cdot B}}), \quad A, B \in \mathfrak{A}. \quad (9)$$

Из соотношения (2) по индукции следует равенство

$$\mu^{(N)} = (\mu^{(0)})^{\zeta_N \circ \dots \circ \zeta_1} + \xi_1^{\zeta_N \circ \dots \circ \zeta_2} + \dots + \xi_{N-2}^{\zeta_N \circ \zeta_{N-1}} + \xi_{N-1}^{\zeta_N} + \xi_N.$$

Так как группа G коммутативна, случайный элемент $\mu^{(0)}$ и члены последовательности (1) независимы в совокупности, а члены последовательности (1) — одинаково распределенные случайные элементы, то распределение случайного элемента $\mu^{(N)}$ совпадает с распределением суммы

$$\xi_1 + \xi_2^{\zeta_1} + \xi_3^{\zeta_1 \circ \zeta_2} + \dots + \xi_N^{\zeta_1 \circ \dots \circ \zeta_{N-1}} + (\mu^{(0)})^{\zeta_1 \circ \dots \circ \zeta_N}. \quad (10)$$

Для любой последовательности $i_1, i_2, \dots, i_N \in \{1, 2, \dots, s\}$ условное распределение случайного элемента (10) при условии $\zeta_1 = A_{i_1}, \zeta_2 = A_{i_2}, \dots, \zeta_N = A_{i_N}$ есть распределение суммы

$$\xi_1^{(i_1)} + (\xi_2^{(i_2)})^{A_{i_1}} + (\xi_3^{(i_3)})^{A_{i_1} \circ A_{i_2}} + \dots + (\xi_N^{(i_N)})^{A_{i_1} \circ \dots \circ A_{i_{N-1}}} + (\mu^{(0)})^{A_{i_1} \circ \dots \circ A_{i_N}},$$

в которой случайные элементы $\xi_1^{(i_1)}, \dots, \xi_N^{(i_N)}, \mu^{(0)}$ независимы, и для любого $j = 1, 2, \dots, N$ распределение $\xi_j^{(i_j)}$ совпадает с распределением случайного элемента $\xi^{(i_j)}$. Из формулы полной вероятности и теоремы умножения для преобразования Фурье суммы независимых случайных элементов следует, что

$$\begin{aligned} \Phi(\mu^{(N)}, \chi) = & \sum_{i_1, i_2, \dots, i_N=1}^s p_{i_1} \Phi(\xi^{(i_1)}, \chi) \cdot p_{i_2} \Phi((\xi^{(i_2)})^{A_{i_1}}, \chi) \cdot p_{i_3} \Phi((\xi^{(i_3)})^{A_{i_1} \circ A_{i_2}}, \chi) \cdot \\ & \dots \cdot p_{i_N} \Phi((\xi^{(i_N)})^{A_{i_1} \circ \dots \circ A_{i_{N-1}}}, \chi) \cdot \Phi((\mu^{(0)})^{A_{i_1} \circ \dots \circ A_{i_N}}, \chi). \end{aligned}$$

Используя равенство (9), получим:

$$\begin{aligned} \Phi(\mu^{(N)}, \chi) = & \sum_{i_1, i_2, \dots, i_N=1}^s p_{i_1} \Phi(\xi^{(i_1)}, \chi) \cdot p_{i_2} \Phi(\xi^{(i_2)}, \chi^{\bar{A}_{i_1}}) \cdot p_{i_3} \Phi(\xi^{(i_3)}, \chi^{\bar{A}_{i_1} \cdot \bar{A}_{i_2}}) \cdot \\ & \dots \cdot p_{i_N} \Phi(\xi^{(i_N)}, \chi^{\bar{A}_{i_1} \cdot \dots \cdot \bar{A}_{i_{N-1}}}) \cdot \Phi(\mu^{(0)}, \chi^{\bar{A}_{i_1} \cdot \dots \cdot \bar{A}_{i_N}}). \quad (11) \end{aligned}$$

Упорядочим элементы орбиты $\bar{\Theta}^{(j)}$ некоторым образом, начиная с χ . Рассмотрим квадратную матрицу порядка n_j

$$\Delta_\chi = [\lambda(\chi_1, \chi_2)],$$

строки и столбцы которой занумерованы элементами орбиты $\bar{\Theta}^{(j)}$, причем для любых $\chi_1, \chi_2 \in \bar{\Theta}^{(j)}$ элементы этой матрицы задаются выражением

$$\lambda(\chi_1, \chi_2) = \sum_{k: \chi_2 = \chi_1^{\bar{A}_k}} p_k \Phi(\xi^{(k)}, \chi_1)$$

(пустая сумма равна нулю).

Кроме того, введем вектор-столбец $\mu^{(0)}(\chi)^\downarrow$ размерности n_j , элементы которого занумерованы элементами орбиты $\overline{\Theta}^{(j)}$, причем для любого характера $\chi_1 \in \overline{\Theta}^{(j)}$ элемент с номером χ_1 равен $\Phi(\mu^{(0)}, \chi_1)$. Наконец, обозначим через $\vec{e}$ вектор-строку длины n_j , у которой первый элемент равен единице, а все остальные равны нулю. В этих обозначениях равенство (11) можно записать следующим образом:

$$\Phi(\mu^{(N)}, \chi) = \vec{e} \cdot \Delta_\chi^N \cdot \mu^{(0)}(\chi)^\downarrow. \quad (12)$$

Воспользуемся сведениями из теории матриц, изложение которых можно найти в [6]. Обозначим через $\|y^\downarrow\|$ евклидову норму комплексного n_j -мерного вектора $y^\downarrow$, а через $\|\overline{\Delta}_\chi\|$ — эрмитову норму матрицы Δ_χ , подчиненную евклидовой норме комплексного пространства n_j -мерных векторов. Тогда

$$\|\Delta_\chi\| = \max_{\|\vec{z}\|=1, \|y^\downarrow\|=1} |\vec{z} \cdot \overline{\Delta}_\chi \cdot y^\downarrow|.$$

Кроме того, имеет место свойство полумультимпликативности эрмитовой нормы матриц

$$\|\Delta_1 \cdot \Delta_2\| \leq \|\Delta_1\| \cdot \|\Delta_2\|.$$

Поэтому из равенства (12) следует оценка

$$|\Phi(\mu^{(N)}, \chi)| \leq \|\Delta_\chi\|^N \cdot \|\mu^{(0)}(\chi)^\downarrow\|. \quad (13)$$

Покажем, что

$$\|\mu^{(0)}(\chi)^\downarrow\|^2 = n_j \sum_{i=0}^l \mathbf{P}\{\tilde{\mu}^{(0)} \in \Theta_i\} \cdot \frac{1}{|\Theta_i|} \sum_{g \in \Theta_i} \chi^{(j)}(g). \quad (14)$$

Используя (4), получим

$$\|\mu^{(0)}(\chi)^\downarrow\|^2 = \sum_{\psi \in \overline{\Theta}^{(j)}} \Phi(\tilde{\mu}^{(0)}, \psi) = \sum_{\psi \in \overline{\Theta}^{(j)}} \sum_{g \in G} \mathbf{P}\{\tilde{\mu}^{(0)} = g\} \cdot \psi(g).$$

Следовательно,

$$\|\mu^{(0)}(\chi)^\downarrow\|^2 = \sum_{g \in G} \mathbf{P}\{\tilde{\mu}^{(0)} = g\} \cdot \sum_{\psi \in \overline{\Theta}^{(j)}} \psi(g). \quad (15)$$

Обозначим через $\overline{\mathfrak{A}}_j$ стабилизатор элемента $\chi^{(j)}$ в группе подстановок $\overline{\mathfrak{A}}$. Имеем соотношение для индекса подгруппы $\overline{\mathfrak{A}}_j$

$$|\overline{\mathfrak{A}} : \overline{\mathfrak{A}}_j| = |\overline{\mathfrak{A}}| : |\overline{\mathfrak{A}}_j| = n_j.$$

Если $\bar{B}_1, \bar{B}_2, \dots, \bar{B}_{n_j}$ — представители правых смежных классов группы $\bar{\mathfrak{A}}$ по подгруппе $\bar{\mathfrak{A}}_j$, то

$$\bar{\Theta}^{(j)} = \left\{ (\chi^{(j)})^{\bar{B}_1}, (\chi^{(j)})^{\bar{B}_2}, \dots, (\chi^{(j)})^{\bar{B}_{n_j}} \right\}.$$

Для любого элемента $g \in G$

$$\begin{aligned} \sum_{\psi \in \bar{\Theta}^{(j)}} \psi(g) &= \sum_{t=1}^{n_j} (\chi^{(j)})^{\bar{B}_t}(g) = \\ &= \sum_{t=1}^{n_j} \frac{1}{|\bar{\mathfrak{A}}_j|} \sum_{\bar{C} \in \bar{\mathfrak{A}}_j} (\chi^{(j)})^{\bar{C} \cdot \bar{B}_t}(g) = \frac{n_j}{|\bar{\mathfrak{A}}|} \sum_{\bar{A} \in \bar{\mathfrak{A}}} (\chi^{(j)})^{\bar{A}}(g). \end{aligned}$$

Таким образом,

$$\sum_{\psi \in \bar{\Theta}^{(j)}} \psi(g) = \frac{n_j}{|\bar{\mathfrak{A}}|} \sum_{A \in \bar{\mathfrak{A}}} \chi^{(j)}(g^A). \quad (16)$$

Аналогично соотношению (16) для любых $i = 0, 1, \dots, l$ и $g \in \Theta_i$ можно доказать справедливость равенства

$$\sum_{A \in \bar{\mathfrak{A}}} \chi^{(j)}(g^A) = \frac{|\bar{\mathfrak{A}}|}{|\Theta_i|} \sum_{\sigma \in \Theta_i} \chi^{(j)}(\sigma). \quad (17)$$

Учитывая (16), (17) в сумме (15) и группируя ее слагаемые по орбитам Θ_i , $i = 0, 1, \dots, l$, получим равенство (14).

Далее, величина $\|\Delta_\chi\|^2$ есть максимальное (вещественное) собственное значение матрицы

$$D_\chi = [d(\chi_1, \chi_2)] = (\Delta_\chi)^* \cdot \Delta_\chi,$$

здесь « $*$ » — знак сопряжения матриц. Для любых $\chi_1, \chi_2 \in \bar{\Theta}^{(j)}$ элемент $d(\chi_1, \chi_2) \neq 0$ тогда и только тогда, когда существуют такие $\nu, \gamma \in \{1, 2, \dots, s\}$, что $\chi_2 = \chi_1^{\bar{A}_\nu^{-1} \cdot \bar{A}_\gamma}$. При выполнении этого условия

$$d(\chi_1, \chi_2) = \sum_{\nu, \gamma: \chi_2 = \chi_1^{(\bar{A}_\nu)^{-1} \cdot \bar{A}_\gamma}} p_\nu \cdot p_\gamma \cdot \overline{\Phi((\xi^{(\nu)})^{A_\nu^{-1}}, \chi_1)} \cdot \Phi((\xi^{(\gamma)})^{A_\nu^{-1}}, \chi_1).$$

По теореме Гершгорина величина $\|\bar{\Delta}_\chi\|^2$ не превосходит максимальной суммы модулей элементов строк матрицы D_χ . Из равенства (6) следует оценка

$$\|\Delta_\chi\|^2 \leq \delta_1. \quad (18)$$

Кроме того, величина $\|\Delta_\chi\|^2 = \|(\Delta_\chi)^*\|^2$ есть максимальное (вещественное) собственное значение матрицы

$$\Delta_\chi \cdot (\Delta_\chi)^*.$$

Для ненулевого элемента этой матрицы, соответствующего $\chi_1, \chi_2 \in \bar{\Theta}^{(j)}$, имеет место выражение

$$\sum_{\nu, \gamma: \chi_2 = \chi_1^{\bar{A}_\nu \cdot (\bar{A}_\gamma)^{-1}}} p_\nu \cdot p_\gamma \cdot \Phi(\xi^{(\nu)}, \chi_1) \cdot \overline{\Phi((\xi^{(\gamma)})^{A_\nu \circ A_\gamma^{-1}}, \chi_1)}.$$

Поэтому аналогично неравенству (18) можно доказать неравенство

$$\|\Delta_\chi\|^2 \leq \delta_2. \quad (19)$$

Из соотношений (5), (8), (13), (14), (18), (19) следует доказываемое неравенство (7).

Теорема доказана. $\square$

Отметим, что при $s = 1$, т.е. в случае вырожденного распределения случайного элемента ζ , выполнены равенства

$$\delta_1 = \delta_2 = \max_{\chi \neq \chi^0} |\Phi(\xi, \chi)|^2$$

и оценка (7) сводится к известным ранее.

Сделаем ряд замечаний относительно величины ϵ_0 из равенства (5). При любом распределении $\mu^{(0)}$ выполнены неравенства

$$\epsilon_0 \leq \frac{1}{|G|} \sum_{j=1}^k |\bar{\Theta}^{(j)}|^{(2)} \leq \max_{j=1, \dots, k} |\bar{\Theta}^{(j)}|.$$

Если $\mathbf{P}\{\mu^{(0)} = \theta\} = 1$, то первое из указанных неравенств обращается в равенство. Если G — элементарная абелева p -группа (p — простое), а группа автоморфизмов $\mathfrak{A}$ транзитивна на множестве ненулевых элементов группы G , то $k = 1$ и

$$\epsilon_0 = (|G| - 1) \sum_{g \neq \theta} \left(\mathbf{P}\{\mu^{(0)} = g\} - \frac{1}{|G|} \right)^2.$$

Укажем достаточные условия, при выполнении которых оценки (7) содержательны, т.е. $\delta_m < 1$. Введем дополнительные обозначения.

Зафиксируем произвольно элементы носителей распределений $g_\nu \in \Omega(\xi_\nu)$, $\nu = 1, 2, \dots, s$. Без ограничения общности будем считать, что

$$p_1 = \min_{\nu=1,2,\dots,s} p_\nu$$

и что для числа $\nu_0 \in \{0, 1, \dots, s\}$ выполнены условия

$$|\Omega(\xi^{(\nu)})| > 1, \quad \nu = 1, 2, \dots, \nu_0, \quad |\Omega(\xi^{(\nu)})| = 1, \quad \nu = \nu_0 + 1, \nu_0 + 2, \dots, s.$$

В случае когда $\nu_0 \geq 1$, для $\nu = 1, 2, \dots, \nu_0$ обозначим через H_ν подгруппу группы G , порожденную множеством $\Omega(\xi^{(\nu)}) - g_\nu$, через $\hat{H}_\nu$ — группу ее комплексных характеров, через $\varphi_0^{(\nu)}$ — единичный характер H_ν . Положим

$$\varepsilon_\nu = \max \{ |\Phi(\xi^{(\nu)} - g_\nu, \varphi)| : \varphi \in \hat{H}_\nu, \varphi \neq \varphi_0^{(\nu)} \}, \quad \nu = 1, 2, \dots, \nu_0, \quad (20)$$

$$\varepsilon = \min_{\nu=1,2,\dots,\nu_0} p_\nu (1 - \varepsilon_\nu).$$

Следствие. *Предположим, что хотя бы одно из множеств*

$$\bigcup_{\nu,\gamma=1}^s (\Omega(\xi^{(\gamma)}) - g_\gamma)^{A_\nu^{-1}} \quad (21)$$

или

$$\bigcup_{\nu,\gamma=1}^s (\Omega(\xi^{(\gamma)}) - g_\gamma)^{A_\nu \circ A_\gamma^{-1}} \quad (22)$$

является системой порождающих элементов группы G . Тогда $\nu_0 \geq 1$, $\varepsilon > 0$ и выполнены неравенства

$$\delta_N^2 \leq \varepsilon_0 \cdot (1 - p_1 \cdot \varepsilon)^N, \quad N \geq 1. \quad (23)$$

Доказательство. Будем предполагать, что множество (21) является системой порождающих элементов группы G ; для случая когда данному условию удовлетворяет множество (22), доказательство аналогично.

Если $\nu_0 = 0$, то $\Omega(\xi^{(\gamma)}) = \{g_\gamma\}$ при любом $\gamma = 1, 2, \dots, s$ и множество (21) равно $\{\theta\}$, что противоречит предположению о множестве (21). Для $\nu = 1, 2, \dots, \nu_0$ подгруппа $H_\nu \neq \{\theta\}$. Для любого характера $\varphi \in \hat{H}_\nu \setminus \{\varphi_0^{(\nu)}\}$ множество $\Omega(\xi^{(\nu)}) - g_\nu$ не содержится в одном смежном классе группы H_ν по ее подгруппе, равной аннулятору

$$\text{Ann}(\varphi) = \{g \in H_\nu : \varphi(g) = 1\}.$$

Отсюда следует неравенство $\varepsilon_\nu < 1$. Таким образом, $\varepsilon > 0$.

Зафиксируем произвольный характер $\chi \in \widehat{\mathbf{G}} \setminus \{\chi_0\}$; его аннулятор $\text{Ann}(\chi)$ — собственная подгруппа группы G . Предположим, что для любых $\gamma, \nu = 1, 2, \dots, s$ имеет место равенство $|\Phi((\xi^{(\gamma)})^{A_\nu^{-1}}, \chi)| = 1$. В этом случае множество (21) содержится в подгруппе $\text{Ann}(\chi)$, что противоречит предположению. Таким образом, существует пара $\gamma, \nu \in \{1, 2, \dots, s\}$ (зависящая от выбора χ), для которой $|\Phi((\xi^{(\gamma)})^{A_\nu^{-1}}, \chi)| < 1$. Величина $|\Phi((\xi^{(\gamma)})^{A_\nu^{-1}}, \chi)|$ совпадает со значением $|\Phi(\xi^{(\gamma)} - g_\gamma, \varphi)|$, где $\varphi \in \widehat{H}_\gamma$ — ограничение характера $(\chi)^{\overline{A}_\nu^{-1}}$ на подгруппу H_γ . При этом $\varphi \neq \varphi_0^{(\gamma)}$, поскольку $\Phi(\xi^{(\gamma)} - g_\gamma, \varphi_0^{(\gamma)}) = 1$. Согласно (20) справедлива оценка $|\Phi((\xi^{(\gamma)})^{A_\nu^{-1}}, \chi)| \leq \varepsilon_\gamma$. Следовательно,

$$\sum_{\psi \in \overline{\Theta}^{(j)}} \left| \sum_{\nu, \gamma: \psi = \chi^{(\overline{A}_\nu)^{-1} \cdot \overline{A}_\gamma} p_\nu \cdot p_\gamma \cdot \overline{\Phi((\xi^{(\nu)})^{A_\nu^{-1}}, \chi)} \cdot \Phi((\xi^{(\gamma)})^{A_\nu^{-1}}, \chi) \right| \leq$$

$$\leq 1 - p_\nu \cdot p_\gamma \cdot (1 - \varepsilon_\gamma) \leq 1 - p_1 \cdot \varepsilon. \quad (24)$$

Учитывая произвольность выбора характера $\chi \in \widehat{\mathbf{G}} \setminus \{\chi_0\}$, из соотношений (24), (6) получаем оценку

$$\delta_1 \leq 1 - p_1 \cdot \varepsilon. \quad (25)$$

Соотношение (23) следует из (25) и (7). $\square$

Список литературы

- [1] Горчинский Ю. Н., Круглов И. А., Капитонов В. М., “Вопросы теории распределений на конечных группах”, *Труды по дискретной математике*, **1** (1997), 85–112.
- [2] Круглов И. А., “Случайные последовательности вида $X_{t+1} = a_t \cdot X_t + b_t \pmod{n}$ с зависимыми коэффициентами a_t, b_t ”, *Дискретная математика*, **17**:2 (2005), 49–55.
- [3] Hildebrand M., “Random processes of the form $X_{n+1} = a_n \cdot X_n + b_n \pmod{p}$ ”, *Ann. Probab.*, **21** (1993), 710–720.
- [4] Hildebrand M., “Random processes of the form $X_{n+1} = a_n \cdot X_n + b_n \pmod{p}$, where b_n takes on a single value”. In: “*Random Discrete Structures*”, IMA Vol. Math. Appl., **76**, 1996, 153–174.
- [5] Bianco S., *Random processes of the form $X_{n+1} = A_n \cdot X_n + B_n \pmod{p}$ in two dimensions*, Ph.D., State Univ. of New York at Albany, 2012, 37 p.
- [6] Круглов И. А. “Сходимость матриц переходных вероятностей некоторых цепей Маркова на конечной абелевой группе к равномерной матрице”, *Математические вопросы криптографии*, **8**:1 (2017), 31–50.
- [7] Гантмахер Ф. Р., *Теория матриц*, М.: Наука, 1966, 576 с.