Вісник Харківського національного університету імені В.Н. Каразіна
Серія "Математика, прикладна математика і механіка"
Том 86, 2017, с.4–9

Visnyk of V.N.Karazin Kharkiv National University
Ser. “Mathematics, Applied Mathematics and Mechanics”
Vol. 86, 2017, p. 4–9
DOI: 10.26565/2221-5646-2017-86-01

УДК 519.216

Случайные блуждания на конечных группах с классовой вероятностью: алгебраический подход

А. Л. Вишневецкий

Харьковский национальный автомобильно-дорожный университет, ул. Я. Мудрого, 25, 61002, Харьков, Украина
alexwish@mail.ru

Хорошо известны необходимые и достаточные условия сходимости n-кратной свертки вероятности на конечной группе G к равномерной (тривиальной) вероятности на G при $n \to \infty$. Оценке скорости этой сходимости посвящено много работ.
Цель статьи — получение оценок скорости этой сходимости для вероятностей, постоянных на классах сопряженных элементов конечных групп.
Ключевые слова: вероятность, конечная группа, сходимость.

Вишневецький О. Л., **Випадкові блукання на скінченних групах із класовою ймовірністю: алгебраїчний підхід.** Добре відомі необхідні і достатні умови збіжності n-кратної згортки імовірності на скінченній групі G до рівномірної (тривіальної) імовірності на G при $n \to \infty$. Оцінці швидкості цієї збіжності присвячено багато робіт.
Ціль статті — одержання оцінок швидкості цієї збіжності для ймовірностей, постійних на класах спряжених елементів скінченних груп.
Ключові слова: імовірність, скінченна група, збіжність.

A. L. Vyshnevetskiy, **Random walks on finite groups with conjugate class probability: algebraic approach.** Under well known conditions an n-fold convolution of probability on finite group G converges to the uniform probability on G ($n \to \infty$). A lot of works estimate a rate of that convergence. The aim of the article is to obtain estimates of the rate for the probabilities that are constant on classes of conjugate elements of finite groups.
Keywords: probability, finite group, convergency.

2010 Mathematics Subject Classification: 20D99, 60B15, 60B10.

Пусть P – вероятность на конечной группе G порядка $|G|$, $U(g) = \dfrac{1}{|G|}$ – равномерная (тривиальная) вероятность на G, $P^{(n)}$ – n-кратная свертка функции P. Хорошо известны [1] необходимые и достаточные условия, при которых $P^{(n)} \to U$ $(n \to \infty)$. Оценке скорости этой сходимости посвящено много работ (см., например, обзор [2]).

Цель статьи – получение оценок скорости сходимости для конечных групп и вероятностей, постоянных на классах сопряженных элементов. Сходимость в пространстве функций $F(g)$ на группе G понимается относительно норм $\|F\|_1 = \sum\limits_g |F(g)|$ и $\|F\| = \left(|G| \sum\limits_g |F(g)|^2\right)^{1/2}$ (мы пишем $\sum\limits_g$ вместо $\sum\limits_{g \in G}$). В [1, 2] норма $\|\|_1$ имеет коэффициент $\dfrac{1}{2}$.

Пусть $\mathbf{C}G$ – групповая алгебра группы G над полем $\mathbf{C}$ комплексных чисел. Сопоставим вероятности $P(g)$ элемент $p = \sum\limits_g P(g)g$ алгебры $\mathbf{C}G$; этот элемент мы обозначаем той же (но малой) буквой, что и породившая его функция, и называем *вероятностью на $\mathbf{C}G$*. Свертке

$$(P * Q)(h) = \sum_g P(g)Q(g^{-1}h), \quad h \in G$$

функций P и Q соответствует произведение pq вероятностей на $\mathbf{C}G$.

Пусть $L(G)$ – пространство функций над полем $\mathbf{C}$ на группе G, постоянных на ее классах сопряженных элементов (классовые или центральные функции). В дальнейшем, если не оговорено противное, все вероятности являются классовыми. На абелевой группе все вероятности являются классовыми. В пространстве $L(G)$ определено скалярное произведение: если $F_1, F_2 \in L(G)$, то

$$(F_1, F_2) = \frac{1}{|G|} \sum_g F_1(g)\overline{F}_2(g), \tag{1}$$

где черта означает комплексное сопряжение. Множество $Irr(G)$ неприводимых комплексных характеров группы G образует ортонормированный базис в $L(G)$ относительно скалярного произведения (1). Поэтому вероятность $P \in L(G)$ разлагается по базису $Irr(G) = \{\mathbf{1}_G, \chi_1, \ldots, \chi_k\}$, причем ввиду

$$\sum_g P(g) = 1 \tag{2}$$

коэффициент при главном характере $\mathbf{1}_G$ равен $\frac{1}{|G|}$:

$$p = \frac{1}{|G|}\mathbf{1}_G + m_1\chi_1 + \ldots + m_k\chi_k \tag{3}$$

Положим $d_j = \deg \chi_j$, $b = \max\limits_j |b_j|$, где

$$b_j = \frac{|G|m_j}{d_j} \quad (j = 1, \ldots, k). \tag{4}$$

Лемма 1 $b \le 1$

Доказательство. Так как $|\chi_j(g)| \le d_j$, то из (3)

$$|m_j| = |(P,\chi_j)| \le \frac{1}{|G|}\sum_g |P(g)\overline{\chi}_j(g)| =$$
$$= \frac{1}{|G|}\sum_g P(g)|\chi_j(g)| \le \frac{1}{|G|}\sum_g P(g)|\chi_j(g)| \le \frac{1}{|G|}\sum_g P(g)d_j = \frac{d_j}{|G|}.$$

Поэтому из (4) $|b_j| \le 1$ и, следовательно, $b \le 1$.

Пусть $\operatorname{supp}(P) = \{g \in G,\ P(g) \ne 0\}$ — носитель вероятности P. Оценку леммы 1 можно усилить для вероятностей, у которых носитель $\operatorname{supp}(P) = G$.

Теорема 1 $b \le 1 - \min\limits_g P(g)$.

Доказательство. Положим $l = \min\limits_g P(g)$, $l_0 = (1-l)^{-1}$.
Функция $P_1 = l_0(P - lU)$ является вероятностью на G. Для любого неглавного характера $\chi_j \in Irr(G)$ имеем

$$m_j(P_1) = (P_1,\chi_j) = l_0(P - lU,\chi_j) = l_0(P,\chi_j) = l_0 m_j,$$

где $m_j(P_1)$ – коэффициенты разложения (3) для P_1 ($j = 1,\ldots,k$). Поэтому $b_j(P_1) = l_0 b_j(P)$ и

$$b(P_1) = l_0 b(P). \tag{5}$$

Так как $b(P_1) \le 1$ (лемма 1), то $b(P) \le l_0^{-1} = 1 - l$.

В дальнейшем будем считать, что числа b_j занумерованы так, что $b = |b_1| = \ldots = |b_t|$ и $|b_j| < b$ при $j > t$. Пусть $D = \left(\sum\limits_{j=1}^{t} d_j^2\right)^{1/2}$.

Теорема 2 $Db^n \le \|P^{(n)} - U\| \le Db^n + a^n\left(|G| - 1 - D^2\right)^{1/2}$, *где* $0 \le a < b$, *a и b не зависят от n.*

Доказательство. Пусть p, u — вероятности на алгебре $\mathbf{C}G$, соответствующие вероятностям P, U. Если $e_j = \dfrac{d_j}{|G|}\sum\limits_g \chi_j(g)g \quad (j = 1,\ldots,k)$, то из (3) и (4) следует

$$p = \tfrac{1}{|G|}\sum_g \mathbf{1}_G\, g + m_1\sum_g \chi_1(g)g + \ldots + m_k\sum_g \chi_k(g)g = u + \sum_{j=1}^{k} \tfrac{|G|m_j}{d_j}\, e_j =$$
$$= u + \sum_{j=1}^{k} b_j e_j.$$

Так как $u, e_1, \ldots, e_k$ – ортогональные идемпотенты центра алгебры $\mathbf{C}G$, то $p^n = u + \sum\limits_{j=1}^{k} b_j^n e_j$,

$$p^n - u = \sum_{j=1}^{k} b_j^n e_j = \sum_{j=1}^{k} b_j^n \sum_{g} \frac{d_j}{|G|} \chi_j(g)\, g = \sum_{g} \left(\sum_{j=1}^{k} \frac{d_j b_j^n}{|G|} \chi_j(g) \right) g,$$

или, возвращаясь к функциям на группе G,

$$p^n - U = \sum_{j=1}^{k} \frac{d_j b_j^n}{|G|} \chi_j.$$

Так как $\|\chi_j\|^2 = |G| \sum\limits_{g} |\chi_j(g)|^2 = |G|^2$, то функции $\dfrac{\chi_j}{|G|}$ $(j = 1, \ldots, k)$ образуют ортонормированное множество относительно нормы $\| \cdot \|$. Поэтому

$$\|P^{(n)} - U\|^2 = \sum_{j=1}^{k} |b_j^{2n}| d_j^2 = b^{2n} D^2 + \sum_{j>t} |b_j^{2n}| d_j^2 \leq b^{2n} D^2 + a^{2n} \sum_{j>t} d_j^2,$$

где $a = \max\limits_{j>t} |b_j|$, $\; 0 \leq a < b$.

Так как $0 \leq \sum\limits_{j>t} d_j^2 = \left(\sum\limits_{j=1}^{k} d_j^2 - D^2 \right) = \left(|G| - 1 - D^2 \right)$, то

$$D^2 b^{2n} \leq \|P^{(n)} - U\|^2 \leq D^2 b^{2n} + a^{2n} \left(|G| - 1 - D^2 \right),$$

откуда следует утверждение теоремы.

Следствие 1.

1) $P^{(n)} \overrightarrow{\overrightarrow{\scriptstyle n\to\infty}}\, U$ по любой норме тогда и только тогда, когда $b < 1$.

2) Для достаточно больших n существует число $a_0 \in [0; 1)$, не зависящее от n, такое что

$$Db^n \leq \|P^{(n)} - U\| \leq (D + a_0^n)\, b^n \tag{6}$$

и

$$|G|^{-\frac{1}{2}} Db^n \leq \|P^{(n)} - U\|_1 \leq (D + a_0^n)\, b^n \tag{7}$$

Доказательство.

1) В конечномерном пространстве любая норма эквивалентна норме $\| \cdot \|$.

2) В доказательстве нуждается только (7). Если из $m \geq 2$ вещественных чисел $a_1 \ldots a_m$ хотя бы два не равны нулю, то в силу неравенств между средними

$$\sum_{i=1}^{m} a_i^2 < \left(\sum_{i=1}^{m} |a_i| \right)^2 \leq m \sum_{i=1}^{m} a_i^2. \tag{8}$$

Ввиду (2) значения двух вероятностей на G не могут отличаться ровно на одном элементе. Поэтому при $m = |G|$ в качестве $a_1, \dots, a_m$ можно взять значения функции $\left(P^{(n)} - U\right) g$, $g \in G$. Извлекая в (8) квадратный корень, получим

$$|G|^{-\frac{1}{2}} \|P^{(n)} - U\| < \|P^{(n)} - U\|_1 \leq \|P^{(n)} - U\|.$$

Поэтому (7) следует из (6).

Ввиду неравенств (6) и (7) число b играет важную роль в оценке скорости сходимости $P^{(n)}$ к U. Приведем оценки для величины b.

Теорема 3 $\left(\dfrac{\|P\|^2 - 1}{|G| - 1}\right)^{\frac{1}{2}} \leq b \leq \dfrac{\left(\|P\|^2 - 1\right)^{\frac{1}{2}}}{D}$.

Доказательство. Возьмем скалярный квадрат равенства (3) относительно скалярного произведения (1):

$$\frac{1}{|G|} \sum_g P^2(g) = \frac{1}{|G|^2} + \sum_{j=1}^{k} m_j^2.$$

Умножая на $|G|^2$ и используя (4), получаем $\|P\|^2 - 1 = \sum\limits_{j=1}^{k} b_j^2 d_j^2$. Так как

$$b^2 \sum_{j=1}^{t} d_j^2 \leq \sum_{j=1}^{k} b_j^2 d_j^2 \leq b^2 \sum_{j=1}^{k} d_j^2 = b^2(|G| - 1),$$

и $D^2 = \sum\limits_{j=1}^{k} d_j^2$, то $b^2 D^2 \leq \|P\|^2 - 1 \leq b^2(|G| - 1)$. Поэтому $\|P\|^2 - 1 > 0$ и $\dfrac{\|P\|^2 - 1}{|G| - 1} \leq b^2 \leq \dfrac{\|P\|^2 - 1}{D^2}$, что завершает доказательство.

Можно оценить b снизу с помощью числа $s = |\mathrm{supp(P)}|$.

Следствие 2.

$$b \geq \left(\frac{1}{s} - \frac{1}{|G|}\right)^{\frac{1}{2}} \tag{9}$$

. Доказательство. Так как $s^{-1} \geq |G|^{-1}$, то из (2) и (8) получаем, что $\|P\|^2 |G|^{-1} \geq s^{-1}$. Поэтому

$$\frac{\|P\|^2 - 1}{|G| - 1} \geq \frac{\|P\|^2 - 1}{|G|} \geq \frac{1}{s} - \frac{1}{|G|}.$$

Замечания.

1. В силу (9) вероятности с малым носителем не могут быстро сходиться к U.

2. С помощью (9) можно получить нетривиальную оценку для b даже при $s = |G|$. Для этого нужно применить (9) к вероятности P_1 (см. доказательство теоремы 1), у которой $\mathrm{supp}(P) \neq G$.

Следствие 3. Если вероятность P равномерно распределена на нормальном s-элементном множестве, то $\dfrac{|G|s^{-1} - 1}{|G| - 1} \leq b^2 \leq \dfrac{|G|s^{-1} - 1}{D^2}$.

Доказательство. Для равномерного распределения $P(g) = s^{-1}$ $(g \in \mathrm{supp} P)$, поэтому

$$\|P\|^2 = |G| \sum_g P^2(g) = |G| s \cdot s^{-2} = |G| s^{-1}.$$

ЛИТЕРАТУРА

1. P. Diaconis, Group Representations in Probability and Statistics. Institute of Mathematical Statistics, 1988. – 198 p.

2. L. Saloff-Coste, Random walks on finite groups. In Probability on Discrete Structures. / H. Kesten, editor, Springer, 2004. – P. 263–340.

Статья получена: 13.08.2017; принята: 16.10.2017.
Article history: Received: 13 August 2017; Accepted: 16 October 2017.