Дискретная математика и математическая кибернетика

Discrete mathematics and mathematical cybernetics

УДК 519.217.2

О СЛУЧАЙНЫХ БЛУЖДАНИЯХ НА ГРАФАХ КЭЛИ ГРУПП КОМПЛЕКСНЫХ ОТРАЖЕНИЙ

М. М. ВАСЬКОВСКИЙ[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Исследуются асимптотические свойства случайных блужданий на минимальных графах Кэли групп комплексных отражений. Основным результатом является теорема о быстром перемешивании для случайных блужданий на графах Кэли групп комплексных отражений. В частности, ключевую роль играют оценки диаметров и изопериметрических постоянных таких графов, а также известный результат о быстром перемешивании для случайных блужданий на экспандерах. Приводится конструктивный способ доказательства частного случая гипотезы Бабаи о логарифмическом порядке диаметров для графов групп комплексных отражений. На основании оценки диаметров и неравенства Чигера получена нетривиальная оценка снизу для спектральных пробелов минимальных графов Кэли групп комплексных отражений.

Ключевые слова: группы комплексных отражений; графы Кэли; случайные блуждания; экспандеры.

Образец цитирования:
Васьковский ММ. О случайных блужданиях на графах Кэли групп комплексных отражений. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:51–56.
https://doi.org/10.33581/2520-6508-2021-3-51-56

For citation:
Vaskouski MM. Random walks on Cayley graphs of complex reflection groups. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:51–56. Russian.
https://doi.org/10.33581/2520-6508-2021-3-51-56

Автор:
Максим Михайлович Васьковский – доктор физико-математических наук, доцент; заведующий кафедрой высшей математики факультета прикладной математики и информатики.

Author:
Maksim M. Vaskouski, doctor of science (physics and mathematics), docent; head of the department of higher mathematics, faculty of applied mathematics and computer science.
vaskovskii@bsu.by
https://orcid.org/0000-0001-5769-3678

Журнал Белорусского государственного университета. Математика. Информатика. 2021;3:51–56
Journal of the Belarusian State University. Mathematics and Informatics. 2021;3:51–56

RANDOM WALKS ON CAYLEY GRAPHS OF COMPLEX REFLECTION GROUPS

M. M. VASKOUSKI[a]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

Asymptotic properties of random walks on minimal Cayley graphs of complex reflection groups are investigated. The main result of the paper is theorem on fast mixing for random walks on Cayley graphs of complex reflection groups. Particularly, bounds of diameters and isoperimetric constants, a known result on fast fixing property for expander graphs play a crucial role to obtain the main result. A constructive way to prove a special case of Babai's conjecture on logarithmic order of diameters for complex reflection groups is proposed. Basing on estimates of diameters and Cheeger inequality, there is obtained a non-trivial lower bound for spectral gaps of minimal Cayley graphs on complex reflection groups.

Keywords: complex reflection groups; Cayley graphs; random walks; expander graphs.

Введение

В последние десятилетия разработаны глубокие и оригинальные приложения графов-экспандеров в теории алгоритмов и, в частности, в криптографии и теории кодирования [1–3]. В настоящее время нет строгого и общепринятого математического определения экспандера. Под экспандером, как правило, понимают большой разреженный граф или последовательность таких графов, имеющие достаточно хорошие параметры спектрального расширения (в случае последовательностей графов требуется отделенность снизу от нуля изопериметрических постоянных). Графы Кэли на конечных неабелевых группах обычно обладают худшими параметрами спектрального расширения, но имеют несложную комбинаторную структуру и позволяют строить простые алгоритмы маршрутизации, что делает их удобным инструментом при реализации алгоритмов [4]. В настоящей статье исследуется вопрос о времени перемешивания случайных блужданий на графах Кэли групп комплексных отражений. Отметим, что группы комплексных отражений являются естественными обобщениями групп Коксетера [5] и имеют значительные применения, в частности, в дифференциальной геометрии [6]. Свойства случайных блужданий на графах групп Коксетера глубоко исследовались во многих работах, в том числе в публикациях [7; 8]. Однако случайные блуждания на графах групп комплексных отражений до сих пор остаются малоизученными. Поскольку изопериметрические постоянные таких графов не отделены снизу от нуля, то для получения необходимых оценок времени перемешивания случайных блужданий в настоящей статье исследуются диаметры и спектральные пробелы упомянутых графов.

Основные результаты

Рассмотрим семейство неприводимых групп комплексных отражений $G(m, p, n)$, $m, p, n \in \mathbb{N}$, $n > 2$, $p \mid m$. Каждая из групп $G(m, 1, n)$ является полупрямым произведением абелевой группы порядка m^n и симметрической группы S_n. В частности, $G(1, 1, n) = S_n$. При $p > 1$ группа $G(m, p, n)$ – это подгруппа индекса p группы $G(m, 1, n)$. Элементами группы $G(m, p, n)$ являются матрицы $w \in \mathbb{C}^{n \times n}$, у которых на позициях $(k, \tau(k))$, $k \in \{1, \ldots, n\}$, стоят элементы ξ^{a_k}, где $\tau \in S_n$; $(a_1, \ldots, a_n) \in \mathbb{Z}_m^n$; $\sum_{k=1}^{n} a_k = 0 \pmod{p}$; ξ – некоторый первообразный комплексный корень из единицы степени m, а на остальных позициях стоят нули. Будем обозначать такую матрицу w символом $\xi^{(a_1, \ldots, a_n)} \otimes \tau$. Поскольку существует взаимно однозначное соответствие между матрицами $w = \xi^{(a_1, \ldots, a_n)} \otimes \tau$ и перестановками $(w_1, \ldots, w_n)$, где $w_k = \tau(k)\xi^{a_k}$, $k \in \{1, \ldots, n\}$, то в дальнейшем элементы группы $G(m, p, n)$ будем кодировать перестановками указанного вида. Порядок группы $G(m, p, n)$ равен $\frac{m^n n!}{p}$.

Определение. Пусть Γ – конечная группа, T – система образующих группы Γ, удовлетворяющая условиям $\mathrm{id} \notin T$ и $T = T^{-1}$, т. е. $s^{-1} \in T$ для любого $s \in T$. *Граф Кэли* $\mathrm{Cay}(\Gamma, T)$ – это неориентированный граф со множеством вершин $V = \Gamma$ и множеством ребер $E = \{(x, y) \mid x, y \in \Gamma,\ yx^{-1} \in T\}$. Граф Кэли $\mathrm{Cay}(\Gamma, T)$ называется *минимальным*, если порождающее множество T минимально, т. е. для любого $s \in T$ множество $T' = T \setminus \{s, s^{-1}\}$ не является системой образующих группы Γ.

Определим следующие элементы группы $G(m, p, n)$: $s_i = \xi^{(0,\ldots,0)} \otimes (i, i+1)$, $i \in \{1, \ldots, n-1\}$, $t_1 = \xi^{(m-1,1,0,\ldots,0)} \otimes (1, 2)$, $t = \xi^{(p,0,\ldots,0)} \otimes \mathrm{id}$. Рассмотрим семейство минимальных графов Кэли $A(m, p, n)$ на группах $G(m, p, n)$ с порождающими множествами $T(m, p, n)$, где $T(m, p, n) = \{s_1, \ldots, s_{n-1}\}$ при $p = m = 1$; $T(m, p, n) = \{s_1, \ldots, s_{n-1}, t, t^{-1}\}$ при $p = 1, m > 1$; $T(m, p, n) = \{s_1, \ldots, s_{n-1}, t_1, t, t^{-1}\}$ при $1 < p < m$; $T(m, p, n) = \{s_1, \ldots, s_{n-1}, t_1\}$ при $p = m > 1$ [9]. Отметим, что каждый граф $A(m, p, n)$ является связным, регулярным и вершинно-транзитивным. Обозначим через $d_{m,p,n}$ степень вершины данного графа.

Пусть $G = (V, E)$ – конечный связный k-регулярный граф. Определим на этом графе стандартное вероятностное пространство $(\Omega, \mathcal{F}, \mathbb{P})$ и рассмотрим случайное блуждание X_t, $t = 0, 1, 2, \ldots$, на графе G такое, что $\mathbb{P}(X_t = w \,|\, X_{t-1} = w_0) = \frac{1}{k}$ при $w \in N(w_0)$, где $N(w_0)$ – множество смежных вершин с вершиной w_0 в графе G; $\mathbb{P}(X_t = w \,|\, X_{t-1} = w_0) = 0$ при $w \in V \setminus N(w_0)$.

В дальнейшем будем опираться на следующий известный результат о времени перемешивания случайных блужданий на экспандерах.

Предложение 1 [1]. *Пусть $G = (V, E)$ – конечный связный k-регулярный граф, для которого нетривиальные собственные значения λ матрицы смежности удовлетворяют неравенству $|\lambda| \le c$ при некотором $c < k$, а S – произвольное подмножество вершин графа G, $v \in V$. Тогда для любого $t \ge t_0 := \ln\left(\frac{2|V|}{|S|^{1/2}}\right)\left(\ln\frac{k}{c}\right)^{-1}$ выполняется двойное неравенство*

$$\frac{|S|}{2|V|} \le \mathbb{P}(X_t \in S \,|\, X_0 = v) \le \frac{3|S|}{2|V|}.$$

Пусть $G = (V, E)$ – конечный граф, S – непустое подмножество множества вершин V графа G. Подмножество ребер $\partial_E S = \{(u, v) \in E \,|\, u \in S, v \in V \setminus S\}$ называется *реберной границей* множества S, а подмножество вершин $\partial_V S = \{v \in V \setminus S \,|\, \exists u \in S : (u, v) \in E\}$ – *вершинной границей* множества S. *Постоянной Чигера* графа G именуется величина $h_E(G) = \min\limits_{0 < |S| \le |V|/2} \frac{|\partial_E S|}{S}$, *матрицей Лапласа* графа G – матрица $L = D - A$, где D – диагональная матрица, состоящая из степеней вершин графа G; A – матрица смежности графа G. *Спектральным пробелом* графа G называется наименьшее положительное собственное значение матрицы Лапласа графа G. Через $\mathrm{diam}(G)$ обозначим *диаметр* графа $G = (V, E)$, т. е. $\mathrm{diam}(G) = \max\limits_{u, v \in V} (\mathrm{dist}(u, v))$, где $\mathrm{dist}(u, v)$ – расстояние между вершинами u, v в графе G.

В дальнейших рассуждениях будем использовать следующее неравенство Чигера.

Предложение 2 [10, гл. 1]. *Пусть $G = (V, E)$ – конечный связный k-регулярный граф, σ – спектральный пробел графа G. Тогда выполняется двойное неравенство*

$$\frac{\sigma}{2} \le h_E(G) \le \sqrt{2\sigma k}.$$

Для любого связного вершинно-транзитивного графа имеет место следующий результат Бабаи.

Предложение 3 [11]. *Пусть $G = (V, E)$ – конечный связный вершинно-транзитивный граф. Тогда для любого $S \subset V$, $0 < |S| \le \frac{|V|}{2}$, справедливо неравенство*

$$|\partial_V S| \ge \frac{|S|}{4\mathrm{diam}(G)}.$$

Поскольку $|\partial_E S| \ge |\partial_V S|$ для любого $S \subset V$, $0 < |S| \le \frac{|V|}{2}$, то из предложения 3 получаем следующий результат.

Следствие 1. *Пусть $G = (V, E)$ – конечный связный вершинно-транзитивный граф. Тогда справедливо неравенство*

$$h_E(G) \ge \frac{1}{4\mathrm{diam}(G)}.$$

Получим оценку сверху для диаметров графов Кэли $A(m, p, n)$.

Предложение 4. *Для любых* $m, p, n \in \mathbb{N}$, $n > 2$, $p \mid m$, *справедливо неравенство*

$$\operatorname{diam}\big(A(m, p, n)\big) \le 2n^2 m.$$

Доказательство. *Так как граф* $A(m, p, n)$ вершинно-транзитивный, то достаточно доказать существование пути длиной не более $2n^2m$ из произвольной вершины $v \in G(m, p, n)$ в вершину $\mathrm{id} \in G(m, p, n)$.

Зафиксируем произвольный элемент $w = (w_1, \ldots, w_n) \in G(m, p, n)$, где $w_i = \xi^{a_i} c_i$, $a_i \in \mathbb{Z}_m$, $c_i = \sigma(i)$ для некоторого $\sigma \in S_n$. Пусть $w^0 = \big(w_1^0, \ldots, w_n^0\big)$ – единичный элемент группы $G(m, p, n)$, где $w_i^0 = i$. Так как диаметр графа $A(1, 1, n)$ равен $\dfrac{n(n-1)}{2}$ [8], то $\operatorname{dist}(w, w\tau) \le \dfrac{n(n-1)}{2}$ для любого $\tau \in S_n$. Таким образом, достаточно показать, что существует элемент $\tau \in S_n$ такой, что $\operatorname{dist}\big(w\tau, w^0\big) \le 2n^2(m-1)$.

Рассмотрим случай $p = m > 1$ и опишем соответствующий алгоритм получения элемента $w\tau$ из единичного элемента w^0 с применением образующих $s_1, \ldots, s_{n-1}, t_1$. Существует целое неотрицательное число $k \le n$ такое, что

$$\sum_{i=1}^{n} a_i = kp. \tag{1}$$

Пусть $A_- = \{1, \ldots, k\}$, $A_+ = \{k+1, \ldots, n\}$. Используем следующий алгоритм для получения элемента $w\tau$ из элемента w^0.

Шаг А1. Взять некоторые символы w_i^0, $i \in A_+$, и w_j^0, $j \in A_-$, и перемещать их на первую и вторую позиции соответственно, применяя транспозиции $s_1, \ldots, s_{n-1}$.

Шаг А2. Умножить перемещенные символы w_i^0, w_j^0 на ξ, ξ^{-1} соответственно (эти действия эквивалентны применению образующего t_1).

Шаг А3. Повторять шаги А1 и А2 $\sum\limits_{i \in A_+} a_i$ раз так, что каждый символ w_i^0, $i \in A_+$, будет умножен на ξ a_i раз, а каждый символ w_j^0, $j \in A_-$, будет умножен на ξ^{-1} $p - a_j$ раз (это возможно в силу равенства (1)).

Очевидно, что описанный алгоритм построит элемент $w\tau$ для некоторого $\tau \in S_n$. Так как $|A_+| \le n$ и $0 \le a_i < p$ для любого $i \in A_+$, то имеют место неравенства

$$\operatorname{dist}\big(w\tau, w^0\big) \le (2n-1)n(p-1) < 2n^2(p-1).$$

Таким образом, $\operatorname{diam}\big(A(m, p, n)\big) \le 2n^2 p = 2n^2 m$.

Теперь рассмотрим случай $m > p$. Для получения единичного элемента w^0 из элемента w используем следующие шаги.

Шаг В1. Получить элемент $\tilde{w} = (\tilde{w}_1, \ldots, \tilde{w}_n)$ из элемента $w = (w_1, \ldots, w_n)$, где $\tilde{w}_i = \xi^{k_i p} i$, $k_i = \left[\dfrac{a_i}{p}\right]$.

Шаг В2. Получить элемент $\varsigma \in S_n$ из элемента $\tilde{w}$.

Шаг В3. Получить единичный элемент w^0 из элемента ς.

Если $p = 1$, то шаг В1 тривиальный: $\tilde{w} = w$. Предположим, что $p > 1$. Применяя шаги алгоритма А1 – А3, можно получить элемент $w\tau$ из элемента $\tilde{w}$ для некоторого $\tau \in S_n$ (достаточно заменить w^0 на $\tilde{w}$ и a_i на $a_i \pmod p$). После этого мы получим элемент w из $w\tau$, используя транспозиции $s_1, \ldots, s_{n-1}$. Длина построенного пути из $\tilde{w}$ в w не превосходит $(2n-1)n(p-1) + \dfrac{n(n-1)}{2}$.

Для получения элемента $\varsigma \in S_n$ из элемента $\tilde{w}$ достаточно переместить каждый символ $\tilde{w}_i = \xi^{k_i p} i$, для которого $k_i \ne 0$, на первую позицию с помощью транспозиций $s_1, \ldots, s_{n-1}$ и затем применить $\dfrac{m}{p} - k_i$ раз образующий t. Длина построенного пути из $\tilde{w}$ в ς не превосходит $n\left(n - 2 + \dfrac{m}{p}\right)$.

Для получения единичного элемента w^0 из элемента ς достаточно применить не более $\dfrac{n(n-1)}{2}$ транспозиций $s_1, \ldots, s_{n-1}$.

Таким образом, $\operatorname{dist}\big(w, w^0\big) \le 2n^2 m$. Предложение доказано.

Основным результатом настоящей статьи является следующая теорема.

Теорема. *Пусть* $\frac{m}{p}$ *нечетно,* $p < m$. *Тогда существует постоянная* $C = C(m, p)$ *такая, что для любых натурального* $n > 2$, *подмножества* S *вершин графа* $A(m, p, n)$, $v \in G(m, p, n)$ *и* $t \geq Cn^7 \ln n$ *выполняется двойное неравенство*

$$\frac{|S|}{2|G(m, p, n)|} \leq \mathbb{P}\left(X_t \in S \,|\, X_0 = v\right) \leq \frac{3|S|}{2|G(m, p, n)|}.$$

Доказательство. Так как $\frac{m}{p}$ нечетно и больше единицы, то в графе $A(m, p, n)$ существуют циклы нечетной длины, и, следовательно, граф $A(m, p, n)$ не является двудольным. Отсюда вытекает, что нетривиальные собственные значения λ матрицы смежности графа $A(m, p, n)$ удовлетворяют неравенству $|\lambda| < d_{m, p, n}$. Таким образом, можем воспользоваться предложением 1. В качестве постоянной c из предложения 1 можно взять величину $d_{m, p, n} - \sigma_{m, p, n}$, где $\sigma_{m, p, n}$ – спектральный пробел графа $A(m, p, n)$. Получим оценку снизу для $\sigma_{m, p, n}$. Используя предложения 2, 4 и следствие 1, имеем

$$\sigma_{m, p, n} \geq \frac{h_E^2\left(A(m, p, n)\right)}{2d_{m, p, n}} \geq \frac{1}{32(n+2)\left(\operatorname{diam}\left(A(m, p, n)\right)\right)^2} \geq \frac{1}{128n^4(n+2)m^2}. \quad (2)$$

Используя неравенство (2), получаем оценки, справедливые для всех m, p, n:

$$\ln\left(\frac{d_{m, p, n}}{d_{m, p, n} - \sigma_{m, p, n}}\right) = -\ln\left(1 - \frac{\sigma_{m, p, n}}{d_{m, p, n}}\right) = \frac{\sigma_{m, p, n}}{d_{m, p, n}} + \frac{1}{2}\left(\frac{\sigma_{m, p, n}}{d_{m, p, n}}\right)^2 \geq \frac{\sigma_{m, p, n}}{d_{m, p, n}} \geq \frac{C(m, p)}{n^6},$$

где постоянная $C(m, p) > 0$ не зависит от n.

Таким образом, получаем оценку для параметра t_0 из предложения 1:

$$t_0 = \ln\left(\frac{2|G(m, p, n)|}{|S|^{1/2}}\right)\left(\ln\left(\frac{d_{m, p, n}}{d_{m, p, n} - \sigma_{m, p, n}}\right)\right)^{-1} \leq \frac{\ln\left(|G(m, p, n)|\right) + \ln 2}{\frac{C(m, p)}{n^6}} \leq C_1(m, p)n^7 \ln n := \tilde{t}_0,$$

где постоянная $C_1(m, p)$ не зависит от n.

Следовательно, согласно предложению 1 для любого $t \geq \tilde{t}_0$ выполнено двойное неравенство

$$\frac{|S|}{2|G(m, p, n)|} \leq \mathbb{P}\left(X_t \in S \,|\, X_0 = v\right) \leq \frac{3|S|}{2|G(m, p, n)|},$$

что и требовалось доказать.

Замечание 1. Условие теоремы, обеспечивающее недвудольность графа $A(m, p, n)$, является существенным, так как в противном случае при четных значениях времени t вероятность оказаться в доле, не содержащей начальную вершину v, равна нулю. Отмеченный факт демонстрирует существенное отличие групп $G(m, p, n)$ от группы S_n, граф $A(1, 1, n)$ которой является двудольным.

Замечание 2. Выбирая в качестве множеств S одноэлементные подмножества $G(m, p, n)$, получаем, что $\mathbb{P}\left(X_t \in S \,|\, X_0 = v\right) = \Theta\left(\frac{1}{|G(m, p, n)|}\right)$, это свидетельствует о близости распределения X_t к равномерному распределению для достаточно больших t.

Библиографические ссылки / References

1. Jao D, Miller SD, Venkatesan R. Expander graphs based on GRH with an application to elliptic curve cryptography. *Journal of Number Theory*. 2009;129(6):1491–1504. DOI: 10.1016/j.jnt.2008.11.006.

2. Charles DX, Lauter KE, Goren EZ. Cryptographic hash functions from expander graphs. *Journal of Cryptology.* 2009;22(1): 93–113. DOI: 10.1007/s00145-007-9002-x.

3. Spielman DA. Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory.* 1996; 42(6):1723–1731. DOI: 10.1109/18.556668.

4. Sauerwald T. *Randomized protocols for information dissemination.* Padeborn: University of Padeborn; 2008. 146 p.

5. Shephard GC, Todd JA. Finite unitary reflection groups. *Canadian Journal of Mathematics.* 1954;6:274–304. DOI: 10.4153/CJM-1954-028-3.

6. Boalch P. Painleve equations and complex reflections. *Annales de l'Institut Fourier.* 2003;53(4):1009–1022. DOI: 10.5802/aif.1972.

7. Aldous DJ. Random walks on finite groups and rapidly mixing Markov chains. In: Azéma J, Yor M, editors. *Séminaire de probabilités de Strasbourg. Volume 17.* Berlin: Springer; 1983. p. 243–297 (Lecture notes in mathematics; 986).

8. Vaskouski M, Zadorozhnyuk A. Resistance distances in Cayley graphs on symmetric groups. *Discrete Applied Mathematics.* 2017;227:121–135. DOI: 10.1016/j.dam.2017.04.044.

9. Jian-yi Shi. Formula for the reflection length of elements in the group $G(m, p, n)$. *Journal of Algebra.* 2007;316(1):284–296. DOI: 10.1016/j.jalgebra.2007.06.031.

10. Krebs M, Shaheen A. *Expander families and Cayley graphs: a beginner's guide.* New York: Oxford University Press; 2011. 258 p.

11. Babai L. Local expansion of vertex-transitive graphs and random generation in finite groups. In: *Proceedings of the 23rd annual ACM symposium on theory of computing; 1991 May 5–8; New Orleans, Louisiana, USA.* New York: ACM Press; 1991. p. 164–174. DOI: 10.1145/103418.103440.

Получена 29.08.2021 / исправлена 20.09.2021 / принята 30.10.2021.
Received 29.08.2021 / revised 20.09.2021 / accepted 30.10.2021.