$$\begin{cases} G_r(d) = G_r(d-r) + G_r(d-r-1), \text{ если } d > r, \\ G_r(r) = 2, \\ G_r(d) = 0, \text{ если } 0 \leqslant d < r. \end{cases}$$

При помощи конструкции из теоремы 2, применённой к паре граней в пространствах соответствующих размерностей, построено семейство множеств $\{Y_n^d\}$ $(n \geqslant 2d)$, имеющих большую (относительно мощности всего пространства) мощность. Индекс n отражает размерность булева куба, в котором лежит соответствующее множество, а d — его радиус покрытия. На основе сферы радиуса d в пространстве $\mathbb{F}_2^{2d}$ построено семейство множеств $\{Z_n^d\}$ (также для $n \geqslant 2d$). Вычислив точные размеры множеств семейств (либо оценив их снизу), получаем нижнюю оценку на мощность наибольших метрически регулярных множеств.

Теорема 4. Пусть A — наибольшее метрически регулярное множество с радиусом покрытия d в булевом кубе размерности n $(n \geqslant 2d)$, r — остаток от деления $n+1$ на $2d+1$. Тогда $|A| \geqslant \max\left\{2^{n-2d}\binom{2d}{d},\ 2^n\left(\frac{2}{2d+1} - \frac{2}{\sqrt{n-r+1}}\right)\right\}$.

Заметим, что при достаточно больших d, n первое число приблизительно равно $1/\sqrt{\pi d}$ от мощности булева куба, второе — $2/(2d+1)$ от мощности булева куба.

ЛИТЕРАТУРА

1. *Облаухов А. К.* О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. 2016. Т. 23. № 3. С. 93–106.
2. *Tokareva N.* Duality between bent functions and affine functions // Discr. Math. 2012. V. 312. No. 3. P. 666–670.
3. *Cusick T. W. and Stanica P.* Cryptographic Boolean Functions and Applications. Academic Press, 2017. 288 p.

УДК 519.1 DOI 10.17223/2226308X/11/5

УЛУЧШЕННАЯ ФОРМУЛА УНИВЕРСАЛЬНОЙ ОЦЕНКИ ЭКСПОНЕНТА ОРГРАФА[1]

В. М. Фомичев

Улучшена формула универсальной оценки экспонента n-вершинного примитивного орграфа, данная А. Далмэджем и Н. Мендельсоном (1964) с использованием множества контуров, длины которых взаимно простые. Предложенная формула использует в орграфе множество контуров $\hat{C}$ с множеством длин $L(\hat{C}) = \{l_1, \ldots, l_m\}$, где $d = (l_1, \ldots, l_m) \geqslant 1$, и множество длин кратчайших путей $\{r_{i,j}^{s/d}(\hat{C}) : s = 0, \ldots, d-1\}$ из вершины i в вершину j, проходящих через множество контуров $\hat{C}$ и образующих полную систему вычетов по модулю d. Показано, что $\exp\Gamma \leqslant 1 + \hat{F}\big(L(\hat{C})\big) + R(\hat{C})$, где $\hat{F}(L) = d \cdot F(l_1/d, \ldots, l_m/d)$; $F(a_1, \ldots, a_m)$ — число Фробениуса; $R(\hat{C}) = \max\limits_{(i,j)} \max\limits_{s} \{r_{i,j}^{s/d}(\hat{C})\}$. Указан класс орграфов с множеством вершин $\{0, \ldots, 2k-1\}$, $k > 2$, для которых предложенные оценки экспонентов лучше известных на величину $k-2$.

Ключевые слова: *число Фробениуса, примитивный орграф, экспонент орграфа.*

[1]Работа выполнена в соответствии с грантом РФФИ № 16-01-00226.

Введение

Обозначим: $\mathbb{Z}_n = \{0, \ldots, n-1\}$ — кольцо вычетов по модулю n, $n \in \mathbb{N}$; $M_n^{0,1}$ — множество $0,1$-матриц порядка n; $\exp \Gamma$ — экспонент орграфа Γ.

Рассмотрим неотрицательную матрицу M (все её элементы суть неотрицательные действительные числа), свойство неотрицательности записывают так: $M \geqslant 0$. Матрицу M, все элементы которой положительные, называют положительной ($M > 0$).

Для квадратной неотрицательной матрицы M в [1] был поставлен вопрос: имеются ли положительные матрицы в ряду $\{M^i : i = 1, 2, \ldots\}$? То есть содержит ли циклическая полугруппа $\langle M \rangle$ положительные матрицы? Если содержит, то матрицу M называют примитивной, в противном случае — непримитивной. Наименьшее натуральное γ, при котором $M^\gamma > 0$, называется экспонентом матрицы M, обозначается $\exp M$. Если матрица M непримитивная, то положим $\exp M = \infty$. В случае примитивной матрицы $M^{\gamma+i} > 0$ при любом $i \in \mathbb{N}$.

Мультипликативная полугруппа всех неотрицательных матриц гомоморфно отображается на полугруппу всех $0,1$-матриц (все элементы суть целые числа 0 или 1) с помощью замены каждого положительного элемента единицей. Этот эпиморфизм согласован со свойством примитивности: прообразом любой примитивной (непримитивной) $0,1$-матрицы является класс, состоящий только из примитивных (непримитивных) матриц. Данное свойство позволяет ограничиться исследованием мультипликативных моноидов $M_n^{0,1}$, $n \in \mathbb{N}$, где умножение выполняется как обычное умножение целочисленных матриц с последующей заменой положительных элементов единицами.

Множество матриц смежности вершин n-вершинных ориентированных графов с петлями совпадает с $M_n^{0,1}$, и на орграфы распространены понятия примитивности и экспонента, где умножение орграфов определено как умножение бинарных отношений. Заметим, что примитивный граф является сильносвязным.

Далее обозначаем через M матрицу смежности вершин орграфа Γ с множеством вершин $\mathbb{Z}_n$. Связь между графами и неотрицательными матрицами устанавливает общеизвестная теорема теории графов (назовём её основной теоремой): число путей длины t из i в j в графе Γ равно $m_{ij}^{(t)}$, $i, j \in \{1, \ldots, n\}$, где $M^t = \big(m_{ij}^{(t)}\big)$. Таким образом, примитивность орграфа и величина экспонента определяется свойствами путей в графе, в частности $M > 0$, если и только если орграф Γ полный. Утверждения о примитивности и об экспонентах равносильно формулируются и на матричном, и на графовом языке.

Известные оценки экспонентов матриц и орграфов можно разделить на универсальные и специальные (для частных классов). Работа посвящена улучшению универсальной оценки экспонента примитивного орграфа.

1. Известные универсальные оценки экспонентов

Основополагающие результаты получены в середине XX в. авторами [2–4], предложившими термин «экспонент».

Обозначим: $\hat{C} = \{C_1, \ldots, C_m\}$ — множество контуров длин $l_1, \ldots, l_m$ соответственно, $L(\hat{C}) = \{l_1, \ldots, l_m\}$. Индексом множества контуров $\hat{C}$ (обозначается $\operatorname{ind} \hat{C}$) назовём число $d = \text{НОД}\big(L(\hat{C})\big)$. Критерий примитивности орграфа Γ [3] определяется множеством его контуров: сильносвязный орграф Γ примитивный, если и только если содержит множество контуров индекса 1.

Универсальная оценка экспонента примитивного орграфа дана Виландтом [2] в 1950 г.:

$$\exp \Gamma \leqslant n^2 - 2n + 2. \tag{1}$$

Доказательство оценки (1) представлено в [3, 5]. При $n > 1$ описаны n-вершинные орграфы [4, 6] (названные в [6] в честь Виландта), на которых достигается оценка (1). Эти орграфы изоморфны, имеют $n+1$ дугу и содержат ровно два простых контура длин n и $n-1$.

В [4] уточнена оценка (1) при известной длине l контура в орграфе:

$$\exp\Gamma \leqslant n + l(n-2).$$

Для более точных оценок введём определения. Говорят, что «путь проходит через контур», если у пути и контура есть общая вершина. Путь проходит через множество контуров, если он проходит через каждый контур множества. В орграфе Γ обозначим: $\mathcal{C}$ — множество всех простых контуров; $\mathcal{C}_d$ — класс всех множеств простых контуров индекса d; $r_{i,j}(\hat{C})$ — длина кратчайшего пути из i в j, проходящего через множество контуров $\hat{C}$; $r(\hat{C}) = \max\limits_{(i,j)} r_{i,j}(\hat{C})$. Оценочная формула Далмэджа и Мендельсона [4] определяется неравенством

$$\exp\Gamma \leqslant 1 + F\big(L(\hat{C})\big) + r(\hat{C}), \tag{2}$$

где $\hat{C}$ — любое множество контуров индекса 1; F — число Фробениуса. Уточним (2):

$$\exp\Gamma \leqslant 1 + \min_{\hat{C}\in\mathcal{C}_1} \Big\{ F\big(L(\hat{C})\big) + r(\hat{C}) \Big\}. \tag{3}$$

Для получения из (2) числовых оценок экспонента достаточно определить число Фробениуса $F\big(L(\hat{C})\big)$ [7, 8] и величину $r(\hat{C})$. С помощью оценки величины $r(\hat{C})$ [9, ч. 1, с. 185] получено

$$\exp\Gamma \leqslant n(m+1) + F\big(L(\hat{C})\big) - l_1 - \ldots - l_m. \tag{4}$$

Учёт структуры множества $\hat{C}$ улучшает оценку (4) [10, с. 80]. Обозначим $\Gamma(\hat{C}) = C_1 \cup \ldots \cup C_m$ — часть орграфа Γ, где $l_1 \leqslant \ldots \leqslant l_m$. Если орграф $\Gamma(\hat{C})$ сильносвязный, то он содержит контур K, проходящий через множество контуров $\hat{C}$ и проходящий через каждую дугу столько раз, сколько контуров множества $\hat{C}$ содержат эту дугу. Контур K в общем случае определён неоднозначно и называется квазиэйлеровым $\hat{C}$-контуром, его длина $\operatorname{len} K = l_1 + \ldots + l_m$. Если $\Gamma(\hat{C})$ имеет компоненты связности $\hat{C}_1, \ldots, \hat{C}_r$, $1 \leqslant r \leqslant m$, содержащие независимые квазиэйлеровы контуры $K_1, \ldots, K_r$ длин $\mu_1, \ldots, \mu_r$ соответственно, то, полагая без ущерба для общности $\mu_1 \geqslant \ldots \geqslant \mu_r$, получаем оценку

$$\exp\Gamma \leqslant n(r+1) + F\left(L(\hat{C})\right) - \sum_{j=1}^{r} \left(l_j + (j-1)\mu_j\right). \tag{5}$$

В частности, если орграф $\Gamma(\hat{C})$ связный, то $\exp\Gamma \leqslant 2n - l_1 + F\left(L(\hat{C})\right)$.

Оценка (5) следует из (2) и из оценки величины $r(\hat{C})$ для примитивных орграфов.

2. Улучшение универсальной оценки экспонента орграфа

Для усиления формулы (3) используем понятие локального экспонента орграфа [11]. Орграф Γ называют (i,j)-примитивным, $i, j \in \mathbb{Z}_n$, если при некотором $\gamma \in \mathbb{N}$ для любого $t \geqslant \gamma$ в орграфе Γ имеется путь длины t из вершины i в вершину j. Наименьшее такое γ называется (i,j)-экспонентом орграфа Γ и обозначается

(i,j)-exp Γ. Примитивный орграф Γ является (i,j)-примитивным для любых $i,j \in \mathbb{Z}_n$ и $\exp\Gamma = \max\limits_{0\leqslant i,j\leqslant n-1} (i,j)\text{-}\exp\Gamma$.

Обозначим: $\hat{F}(L) = d \cdot F(l_1/d,\ldots,l_m/d)$, где $L = \{l_1,\ldots,l_m\}$, $d = \text{НОД}(L)$ ($\hat{F}(L) = F(L)$ при $d = 1$); $r_{i,j}^{s/d}(\hat{C})$ — длина кратчайшего пути w из i в j, проходящего через множество контуров $\hat{C}$, сравнимая с $s \bmod d$, $s = 0,\ldots,d-1$ (такие пути в Γ есть); $R_{i,j}(\hat{C}) = \max\left\{r_{i,j}^{0/d}(\hat{C}),\ldots,r_{i,j}^{d-1/d}(\hat{C})\right\}$; $R(\hat{C}) = \max\limits_{0\leqslant i,j\leqslant n-1} R_{i,j}(\hat{C})$. Заметим, что $r_{i,j}(\hat{C}) = \min\left\{r_{i,j}^{0/d}(\hat{C}),\ldots,r_{i,j}^{d-1/d}(\hat{C})\right\}$, если $\hat{C}$ — множество контуров индекса 1.

Теорема 1. Для любого непустого множества контуров $\hat{C}$ индекса более 1

$$(i,j)\text{-}\exp\Gamma \leqslant 1 + \hat{F}\left(L(\hat{C})\right) + R_{i,j}(\hat{C}),$$
$$\exp\Gamma \leqslant 1 + \hat{F}\left(L(\hat{C})\right) + R(\hat{C}). \tag{6}$$

Следствие 1. Для любого примитивного орграфа Γ

$$\exp\Gamma \leqslant 1 + \min_{\hat{C}\subseteq\mathcal{C},\,\hat{C}\neq\varnothing}\left\{\hat{F}\left(L(\hat{C})\right) + R(\hat{C})\right\}. \tag{7}$$

Замечание 1. Уточнение (по сравнению с (3)) оценки экспонента с помощью формулы (7) возможно только при оценке (6) для множества $\hat{C}$ индекса больше 1.

Найден класс орграфов, для которого формула (6) дает оценки существенно лучше, чем (3).

Теорема 2. Пусть множество вершин орграфа Γ есть $\mathbb{Z}_{2k}$, $k > 1$, множество дуг содержит дуги контуров $C_0 = (k-1, 2k-1)$, $C_1 = (0,\ldots,k-2,2k-1)$, $C_2 = (k-1,\ldots,2k-2)$, и ещё дуги $(k-2,k-1)$ и $(2k-2,2k-1)$ (рис. 1). Тогда для орграфа Γ:
— оценка (3) принимает значение $3k-2$ при чётных k и $3k-3$ при нечётных k;
— оценка (6) принимает значение $2k$ при чётных k и $2k-1$ при нечётных k.

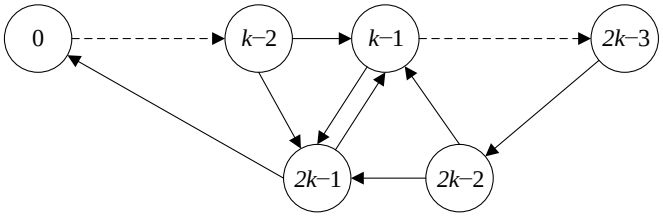

Рис. 1. Орграф Γ (теорема 2)

Множество простых контуров орграфа Γ есть $\mathcal{C} = \{C_0, C_1, C_2, C_3, C_4, C_5\}$, где $C_3 = (0,\ldots,k-1,2k-1)$, $C_4 = (k-1,\ldots,2k-2,2k-1)$ и C_5 есть гамильтонов контур $(0,1,\ldots,2k-1)$. Множество длин всех простых контуров есть $L(\mathcal{C}) = \{2,k,k+1,2k\}$, $\operatorname{ind}\mathcal{C} = 1$.

Пусть $\hat{C} \subseteq \mathcal{C}$. При нечётном k $\operatorname{ind}\hat{C} = 1$, если и только если $2,k \in L(\hat{C})$ или $k,k+1 \in L(\hat{C})$. Класс $\mathcal{C}_1$ состоит из 42 множеств (при чётном k также).

В данном орграфе величина $F\big(L(\hat{C})\big) + r(\hat{C})$ принимает наименьшее значение при $\hat{C} = \mathcal{C}$. Обозначим через $\rho(i,j)$ длину кратчайшего пути из i в j, тогда $\max\limits_{0\leqslant i,j\leqslant 2k-1}\rho(i,j) = \rho(0,2k-2) = \rho(k,k-2) = 2k-2$. Кратчайшие пути $w = (0,\ldots,2k-2)$ и $w' = (k,\ldots,k-2)$ суть части гамильтонова контура и проходят через вершины $k-1$ и

$2k-1$ соответственно. Значит, через любое множество контуров индекса 1 проходит либо w, либо w'. Отсюда $r(\hat{C}) = 2k-2$ для любого $\hat{C} \in \mathcal{C}_1$.

Заметим: $F(L) \leqslant F(L')$ при НОД$(L') =$ НОД$(L) = 1$, если $L' \subseteq L$. Отсюда $F\big(L(\hat{C})\big) \geqslant F\big(L(\mathcal{C})\big) = F(2, k, k+1, 2k)$ для любого множества $\hat{C}$ индекса 1. Отсюда получаем нужные значения оценки (3), так как $F\big(L(\mathcal{C})\big) = F(2,k) = k-2$ при нечётных k и $F\big(L(\mathcal{C})\big) = F(2,k+1) = k-1$ при чётных k.

Получим оценку (6) для контура C_0 длины 2. При нечётных k: $R(C_0) = R_{2k-1,2k-2}(C_0) = 2k$. При чётных k: $R(C_0) = R_{2k-1,2k-2}(C_0) = \max\{\operatorname{len} w, \operatorname{len} w'\} = 2k+1$. В обоих случаях имеем нужные значения оценки (6), так как $\hat{F}(C_0) = \hat{F}(2) = -2$.

В таблице приведены экспоненты орграфов (теорема 2) и их оценки (3), (6) при $k = 2, \ldots, 7$.

Число вершин орграфа $2k$	Оценка (3) $\exp\Gamma$	Оценка (6) $\exp\Gamma$ для контура C_0	$\exp\Gamma$
4	4	4	4
6	6	5	5
8	10	8	8
10	12	9	9
12	16	12	11
14	18	13	13

ЛИТЕРАТУРА

1. *Frobenius G.* Uber Matrizen aus nicht negativen Elementen // K. Preuss. Akad. Wiss. Berlin. 1912. S. 456–477.
2. *Wielandt H.* Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. N. 52. S. 642–648.
3. *Perkins P.* A theorem on regular graphs // Pacific J. Math. 1961. V. II. P. 1529–1533.
4. *Dulmage A. L. and Mendelsohn N. S.* Gaps in the exponent set of primitive matrices // Illinoise J. Math. 1958. No. 86. P. 642–656.
5. *Holladay J. C. and Varga R. S.* On powers of non-negative matrices // Proc. Amer. Math. Soc. 1958. V. IX. P. 631.
6. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
7. *Фомичев В. М.* О вычислительной сложности оригинальной и расширенной диофантовой проблемы Фробениуса // Дискретный анализ и исследование операций. 2017. Т. 24. № 3. С. 104–124.
8. *Alfonsin J. R.* The Diophantine Frobenius Problem. Oxford University Press, 2005.
9. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Юрайт, 2016. 209 с.
10. *Фомичев В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.
11. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1. С. 97–119.