ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.6

ПОЛОЖИТЕЛЬНЫЕ СВОЙСТВА НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

К. Г. Когос*, В. М. Фомичев**

*Национальный исследовательский ядерный университет (*МИФИ*), г. Москва, Россия*

**Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

E-mail: fomichev@nm.ru

Дан обзор результатов исследования примитивности графов (неотрицательных матриц) и некоторых направлений обобщения. Приведены оценки экспонентов различных классов графов и систем графов (матриц и систем матриц).

Ключевые слова: *примитивный граф, примитивная матрица, экспонент, субэкспонент.*

Одним из положительных криптографических свойств преобразований векторных пространств является хорошее перемешивание, то есть зависимость каждой координатной функции от всех переменных. Перемешивающие свойства преобразования g пространства P^n над полем P, заданного системой координатных функций $\{g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)\}$, определяются системой множеств $\{S(g_1),\dots,S(g_n)\}$, где $S(g_j)$ — множество номеров существенных переменных координатной функции $g_j(x_1,\dots,x_n)$, $j=1,\dots,n$. Наилучшее перемешивание достигается, если каждая из координатных функций преобразования g зависит от всех переменных, то есть $S(g_j)=\{1,\dots,n\}$, $j=1,\dots,n$. Такие преобразования принято называть совершенными. Обобщениями свойства совершенности функций являются такие свойства, как строгий лавинный критерий, критерии распространения, свойство «бент».

Почти все преобразования векторного пространства P^n над конечным полем P являются совершенными при $n\to\infty$. Однако подобный вывод неприменим к функциям, используемым в криптографических системах, так как они выбираются не случайно, а из отображений с рядом заданных свойств. Поэтому изучение перемешивающих свойств криптографических функций — актуальная задача криптографического анализа.

Некоторые функции с полным перемешиванием обладают свойством распространения искажений входных данных, что позволяет использовать их в криптосистемах аутентификации. С другой стороны, к функциям шифрования с неполным перемешиванием входов применимы методы определения ключа типа последовательного опробования, что делает привлекательным использование в криптосистеме шифрования совершенных преобразований.

Аппаратная или программная реализация совершенных преобразований затруднена в связи с необходимостью реализации функций от большого числа переменных. Поэтому для хорошего перемешивания используются итерации (возведение в степень) преобразования с относительно слабыми перемешивающими свойствами. Показатель степени преобразования, при которой достигается хорошее перемешивание, является

важной криптографической характеристикой. В частности, показатель степени раундовой подстановки блочного шифра, при которой достигается хорошее перемешивание, является определяющим при выборе разработчиком числа циклов шифрования.

Матрицу A над полем действительных чисел называют положительной (неотрицательной), если положительны (неотрицательны) все её элементы, при этом пишут $A > 0$ ($A \geqslant 0$). Носителем неотрицательной матрицы $A = (a_{i,j})$ называется $0,1$-матрица $v(A) = (v(a_{i,j}))$, где $v(a_{i,j}) = 1$, если $a_{i,j} > 0$, и $v(a_{i,j}) = 0$, если $a_{i,j} = 0$, при всех допустимых i, j. Заметим, что v есть гомоморфизм мультипликативного моноида неотрицательных матриц над полем действительных чисел на мультипликативный моноид $0,1$-матриц, где $v(AB) = v(A) \cdot v(B)$.

Точное определение множества $\{S(g_1), \ldots, S(g_n)\}$ является во многих случаях сложной вычислительной задачей. Поэтому при исследовании перемешивающих свойств степеней преобразований применяется оценочный теоретико-графовый или матричный подход. Обозначим $\Gamma(g)$ перемешивающий n-вершинный орграф преобразования g, в котором пара (i, j) является дугой тогда и только тогда, когда $i \in S(g_j)$, $i, j \in \{1, \ldots, n\}$. Матрицу $M(g)$ смежности вершин графа $\Gamma(g)$ называют перемешивающей матрицей преобразования g. Суть оценочного подхода состоит в исследовании степеней матрицы $M(g)$ и определении наименьшего натурального числа t, такого, что $(M(g))^t > 0$. Корректность такого подхода вытекает, например, из следствия 2 теоремы 10.3 [1]: если матрица $(M(g))^t$ не положительна, то преобразование g^t не совершенно. Оценочный теоретико-графовый или матричный подход реализуется существенно проще с точки зрения сложности вычислений, чем точное вычисление множеств существенных переменных.

При исследовании перемешивающих свойств часто используется эпиморфизм φ мультипликативного моноида неотрицательных матриц порядка n на моноид n-вершинных орграфов, где умножение графов определено как умножение бинарных отношений. При эпиморфизме φ матрице M соответствует орграф Γ с множеством вершин $\{1, \ldots, n\}$ и множеством дуг U, где $(i, j) \in U \Leftrightarrow m_{i,j} > 0$. При эпиморфизме φ выполнено: $M > 0$, если и только если граф $\Gamma = \varphi(M)$ полный. Эпиморфизм φ всякой неотрицательной матрице A ставит в соответствие орграф $\Gamma = \varphi(A)$, матрица смежности вершин которого есть $v(A)$. В частности, $\varphi(M(g)) = \Gamma(g)$ для графа Γ. Следовательно, орграф $\Gamma = \varphi(A)$ полный в том и только в том случае, если $A > 0$. И вообще, система понятий, связанных с изучением перемешивающих свойств преобразований, применима как для неотрицательных матриц, так и для графов.

Ограничение эпиморфизма φ на подмоноид симметричных матриц (для них $m_{i,j} = m_{j,i}$ при всех допустимых i, j) есть эпиморфизм на подмоноид n-вершинных неориентированных графов.

Настоящий обзор посвящён положительным свойствам неотрицательных матриц, под которыми понимаются свойства, связанные со способностью порождения тем или иным способом положительной матрицы. Обзор содержит известные результаты по оценке таких характеристик систем неотрицательных матриц (графов и орграфов), как экспоненты, множественные экспоненты, субэкспоненты. Экспонент системы неотрицательных матриц Ω есть наименьшая длина записи положительной матрицы в системе образующих Ω мультипликативной полугруппы. Множественный экспонент определяет наименьшую длину произведений образующих матриц, при которой каждое произведение данной длины есть положительная матрица. Субэкспонент неотрицательной матрицы есть наименьшее число первых членов мультипликативной циклической полугруппы, порождённой данной матрицей, сумма которых положительна.

1. Примитивность неотрицательных матриц

Неотрицательную матрицу A называют примитивной, если $A^t > 0$ при некотором натуральном t, а наименьшее натуральное γ, при котором $A^\gamma > 0$, называют экспонентом или показателем примитивности матрицы A и обозначают как $\exp A$. Если такого t не существует, то $\exp A = \infty$.

Абсолютная оценка экспонента примитивной матрицы A порядка n дана Виландтом [2]:

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

В [3, с. 409] получены выражения экспонента примитивной матрицы через характеристики матрицы (в частности, через число положительных элементов на главной диагонали). Пусть A — примитивная матрица порядка n, а матрица A^h имеет не менее $d > 0$ положительных элементов на главной диагонали для любого $h \geqslant k$ при целом неотрицательном k. Тогда

$$\exp A \leqslant 2n - d + k - 1.$$

Отсюда следует, что если матрица A имеет не менее $d > 0$ положительных элементов на главной диагонали, то

$$\exp A \leqslant 2n - d - 1,$$

и если положительны все элементы на главной диагонали, то

$$\exp A \leqslant n - 1.$$

Пусть матрица A примитивна и матрица $A + \ldots + A^h$, $h \geqslant 1$, имеет не менее $d > 0$ положительных элементов на главной диагонали. Тогда [3, с. 409]

$$\exp A \leqslant n - d + h(n - 1).$$

Экспонент примитивной симметричной матрицы [3, с. 409] удовлетворяет оценке

$$\exp A \leqslant 2(n - 1).$$

Замечание 1 [4, с. 140]. В связи с абсолютной оценкой (1) отметим, что Далмейджем (Dulmage A. L.) и Мендельсоном (Mendelsohn N. S.) выделены «лакуны», то есть некоторые числа, не превышающие $n^2 - 2n + 2$ и не являющиеся показателями примитивности какой-либо матрицы порядка n. Таковы, например, числа из интервалов $(n^2 - 3n + 4, (n - 1)^2)$ и $(n^2 - 4n + 6, n^2 - 3n + 2)$. При чётном n «лакуной» является интервал $(n^2 - 4n + 6, (n - 1)^2)$, объединяющий оба предыдущих. В [5] данные результаты усилены. Показано, что для любых целых n, t не существует примитивной матрицы порядка n, экспонент которой удовлетворяет неравенствам

$$n^2 - tn + \frac{1}{4}(t + 1)^2 < \exp A < n^2 - (t - 1)n + t - 2.$$

Замечание 2 [2, с. 243]. При $n \to \infty$ случайная равновероятная 0, 1-матрица порядка n с вероятностью, стремящейся к единице, является примитивной и имеет экспонент равный двум.

Матрица A порядка n называется частично разложимой, если у нее есть нулевая подматрица размера $r \times s, r + s = n$. Матрица A вполне неразложима, если она не является частично разложимой.

Известно [3, с. 300], что вполне неразложимая матрица A примитивна и

$$\exp A \leqslant n - 1.$$

Критерий примитивности матрицы A дан ниже в связи с рассмотрением орграфа $\Gamma = \varphi(A)$.

2. Примитивность графов

Примитивность графа определяется естественным образом: граф Γ примитивен, если примитивна матрица смежности его вершин, то есть неотрицательная матрица A и орграф $\Gamma = \varphi(A)$ одновременно примитивны или не примитивны, в случае примитивности их экспоненты равны. При исследованиях примитивности матриц и графов применяется как матричный, так и теретико-графовый язык.

Связь между графами и неотрицательными матрицами устанавливает следующая теорема [6]: пусть M — матрица смежности вершин графа Γ и $M^t = (m_{ij}^{(t)})$, тогда число путей длины t из i в j в графе Γ равно $m_{ij}^{(t)}$, $i, j \in \{1, \ldots, n\}$.

Таким образом, примитивность графа и величина экспонента определяются свойствами путей в графе. В частности, любой примитивный орграф Γ является сильносвязным и $\exp\Gamma$ не меньше диаметра графа Γ.

Напомним, что абсолютная оценка диаметра сильносвязного n-вершинного орграфа Γ имеет вид

$$\operatorname{diam}\Gamma \leqslant n.$$

2.1. Свойства экспонентов ориентированных графов

В [7] указаны примитивные орграфы, на которых достигается абсолютная оценка (1). При $n > 2$ рассмотрим n-вершинный орграф Γ, состоящий из гамильтонова контура $C = (1, 2, \ldots, n)$, к которому добавлена дуга (i, j), где вершины i, j расположены на контуре C на расстоянии 2, $i, j \in \{1, \ldots, n\}$. Множество n-вершинных орграфов, изоморфных орграфу Γ, назовём n-вершинными графами Виландта и обозначим это множество $\Gamma_W(n)$. При любом $n > 2$ множество $\Gamma_W(n)$ состоит из $n!$ изоморфных графов; абсолютная оценка Виландта достигается на графах Виландта, и только на них.

Для остальных примитивных n-вершинных орграфов Γ при нечётном $n > 3$ верна достижимая оценка (в соответствии с известными «лакунами»)

$$\exp\Gamma \leqslant n^2 - 3n + 4.$$

Верхняя граница экспонента примитивного орграфа может быть понижена [3, с. 227], если в орграфе известна длина простого контура. Пусть Γ — примитивный орграф с n вершинами, l — длина кратчайшего простого контура в Γ, тогда

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

В частности, если в примитивном орграфе имеется петля, то $\exp\Gamma \leqslant 2n - 2$.

Граница (2) экспонента примитивного орграфа может быть понижена [7], если в орграфе известны длины l и λ двух простых контуров, где $(l, \lambda) = 1$. Пусть в n-вершинном орграфе Γ имеются простые контуры C и C' длины соответственно l и λ, где $n > 2$, $1 < \lambda < l \leqslant n$ и $(l, \lambda) = 1$. Обозначим $C \cap C'$ пересечение множеств вершин контуров C и C'. Тогда

1) если $C \cap C' = \varnothing$, то $\exp\Gamma \leqslant l\lambda - 2l - 3\lambda + 3n$;
2) если $C \cap C' = H$, где $|H| = h > 0$, то $\exp\Gamma \leqslant l\lambda - l - 3\lambda + h + 2n$.

Отсюда следует, что для любого примитивного n-вершинного орграфа Γ при $n > 2$ верно:

1) если контуры C и C' не имеют общих вершин, то

$$\exp\Gamma \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor \left\lceil \frac{n+1}{2} \right\rceil \leqslant \frac{n^2}{4} + \frac{n}{2} + \frac{1}{4};$$

2) если контуры C и C' имеют h общих вершин, где $1 \leqslant h \leqslant \lambda$, то

$$\exp\Gamma \leqslant \left\lfloor \frac{n+h+2}{2} \right\rfloor \left\lceil \frac{n+h+2}{2} \right\rceil - 2h - n \leqslant n^2 - 2n + 2.$$

В [8] получена оценка диаметра и экспонента nr-вершинного перемешивающего графа $\Gamma(\varphi)$ обратимого преобразования φ регистра сдвига длины n над множеством V_r двоичных r-мерных векторов, где n, r — натуральные (такие графы возникают при рассмотрении обобщения блочных шифров Фейстеля). Подстановка φ такого регистра сдвига имеет вид

$$\varphi(y_1, \ldots, y_n) = (y_2, \ldots, y_n, \psi(y_2, \ldots, y_n) \oplus y_1),$$

где $y_1, \ldots, y_n \in V_r$; $\psi(y_2, \ldots, y_n)$ называется функцией усложнения.

Пусть подстановка φ задается системой булевых координатных функций $\{\varphi_1(x_1, x_2, \ldots, x_{nr}), \varphi_2(x_1, x_2, \ldots, x_{nr}), \ldots, \varphi_{nr}(x_1, x_2, \ldots, x_{nr})\}$. Тогда функции усложнения $\psi(y_2, \ldots, y_n)$ соответствует r-вершинный граф Γ_ψ: пара (v, w) образует дугу тогда и только тогда, когда функция $\varphi_{(n-1)r+w}$ зависит существенно от некоторой переменной из множества $\{x_v, x_{r+v}, \ldots, x_{(n-1)r+v}\}$. Показано, что перемешивающий граф $\Gamma(\varphi)$ сильно связен тогда и только тогда, когда сильно связен граф Γ_ψ.

Получено, что если граф Γ_ψ сильносвязный и $\operatorname{diam}\Gamma_\psi \leqslant d$, то

1) $\operatorname{diam}\Gamma(\varphi) \leqslant (n-1) \cdot \min\{d, r-1\} + n$;
2) если граф $\Gamma(\varphi)$ примитивный и $\psi(y_2, \ldots, y_n) = \psi(y_n, \ldots, y_2)$ (в этом случае алгоритм блочного шифрования инволютивен), то $\operatorname{diam}\Gamma(\varphi) \leqslant n/2 \cdot \min\{d, r-1\} + n$;
3) если граф $\Gamma(\varphi)$ примитивный, то $\exp\Gamma(\varphi) \leqslant n^2 r + nr - 2n$.

В [3, с. 398] дана оценка экспонентов турнира, то есть ориентированного n-вершинного орграфа T_n без петель, в котором каждая пара i, j различных вершин соединена ровно одной дугой. Турнир T_n называется приводимым, если существует такое разбиение множества вершин на два подмножества, что в T_n присутствуют все дуги, направленные из первого блока разбиения во второй блок. В противном случае турнир называется неприводимым. Показано, что при $n \geqslant 4$ турнир T_n примитивен тогда и только тогда, когда он неприводим. Экспонент турнира T_n оценивается при $n \geqslant 5$ через его диаметр d:

$$d \leqslant \exp T_n \leqslant d + 3.$$

В общем случае

$$3 \leqslant \exp T_n \leqslant n - 1.$$

При $n \geqslant 6$ и $3 < \gamma < n+2$ существует неприводимый турнир T_n, экспонент которого равен γ.

Для вершины i ориентированного n-вершинного графа, $i = 1, \ldots, n$, обозначим через p_i число дуг, входящих в вершину i, и через q_i — число дуг, исходящих из вершины i (полустепень захода и полустепень исхода вершины i). Граф называется псевдосимметрическим, если $p_i = q_i$ при $i = 1, \ldots, n$ (дихотомическим при $p_i = q_i = 2$, $i = 1, \ldots, n$). В [9] получены верхние оценки экспонентов примитивных псевдосимметрических и дихотомических графов, при этом рассматриваемые графы классифицированы по длине обхвата (кратчайшего контура). Класс сильносвязных псевдосимметрических графов с n вершинами, каждая из которых имеет не менее k (в точности k) входящих и исходящих дуг, с обхватом не менее p (в точности p) обозначается $H(n, k, p)$ ($G(n, k, p)$). Класс

примитивных графов из $G(n,k,p)$ с обхватом в точности p обозначается $P(n,k,p)$. Справедлива цепочка включений

$$P(n,k,p) \subset G(n,k,p) \subset H(n,k,p).$$

В [9, § 3, ч. 3] описаны структурные свойства графов из множества $G(n,2,(n-1)/2)$. При нечётном $n > 12$ доказано, что $G(n,2,(n-1)/2) = P(n,2,(n-1)/2)$ и для любого $\Gamma \in P(n,2,(n-1)/2)$

$$\exp\Gamma \leqslant \frac{(n-1)^2}{4} + 5.$$

Верхние оценки экспонентов дихотомических графов получены в [9, § 4, ч. 3]. Для любого орграфа $\Gamma \in P(n,2,p)$, где $3 \leqslant p \leqslant \lceil n/2 \rceil$, доказано, что

$$\exp\Gamma \leqslant \frac{(p+1)n}{2p-1} + p(n-2) + 5.$$

В [9, § 5, ч. 3] получены верхние оценки экспонентов графов из классов $P(n,k,p)$ при $p = 1, 2$. В частности, для любого $\Gamma \in P(n,k,2)$, где $k > 2$, справедливо неравенство

$$\exp\Gamma \leqslant \begin{cases} \dfrac{1}{2}\left(29\dfrac{n-1}{k+1} - 5\right), & k > 6\dfrac{n-1}{n+1} - 1, \\ \\ n + \dfrac{1}{2}\left(\dfrac{11n-6}{k+1} - 3\right), & k \leqslant 6\dfrac{n-1}{n+1} - 1. \end{cases}$$

Для любого $\Gamma \in P(n,k,1)$, где $k > 2$, выполнено

$$\exp\Gamma \leqslant 3\left(\frac{n-1}{k+1} + \frac{n-2}{k}\right) - 2.$$

Универсальный критерий примитивности орграфа Γ [3, с. 226] определяется длинами его простых контуров. Если $C_1, \ldots, C_k$ есть все простые контуры орграфа Γ длин $l_1, \ldots, l_k$ соответственно, то сильносвязный орграф Γ примитивный, если и только если $(l_1, \ldots, l_k) = 1$.

Периодом вершины i орграфа называется наибольший общий делитель таких чисел k, что $a_{i,i}^{(k)} > 0$, $i = 1, \ldots, n$. Иными словами, период d вершины i равен наибольшему общему делителю длин всех контуров, проходящих через вершину i в орграфе Γ. Неотрицательная матрица $A = (a_{i,j})$ порядка $n > 1$ называется неразложимой (или неприводимой), если для всех $i, j = 1, \ldots, n$ существует $t \in N$, такое, что $a_{i,j}^{(t)} > 0$, где $A^t = (a_{i,j}^{(t)})$. Это означает, что орграф $\Gamma = \varphi(A)$ сильносвязный: в орграфе Γ для любой пары вершин (i,j), $i, j = 1, \ldots, n$, существует путь из i в j. Неразложимая матрица A называется периодической (или циклической), если период любой вершины орграфа Γ равен $d > 1$. Если $d = 1$ для некоторой вершины орграфа Γ, то матрица называется апериодической (или ациклической).

Универсальный критерий примитивности на матричном языке имеет вид [3, с. 392]: неотрицательная матрица A примитивна тогда и только тогда, когда A неразложима и апериодична.

Сумма неразложимой матрицы A и единичной матрицы I является примитивной матрицей (ей соответствует граф с n петлями), и $\exp(A+I) \leqslant n-1$.

Достаточные условия примитивности орграфа $\Gamma(\varphi)$ подстановки φ регистра сдвига длины n над множеством V_r двоичных r-мерных векторов получены в [8]. Сильносвязный граф $\Gamma(\varphi)$ примитивен, если выполнено любое из следующих условий:

1) координатная функция φ_m зависит существенно от переменной x_m при некотором $m \in \{(n-1)r+1, (n-1)r+2, \ldots, nr\}$, в этом случае $\exp\Gamma(\varphi) \leqslant 2nr-2$;
2) $\psi(y_2, \ldots, y_n) = \psi(y_n, \ldots, y_2)$ и при некоторых $m \in \{(n-1)r+1, (n-1)r+2, \ldots, nr\}$ и $\mu \in \{1, \ldots, r\}$ координатная функция φ_m зависит существенно от переменной $x_{jr+\mu}$ при $n-2j=1$, в этом случае $\exp\Gamma(\varphi) \leqslant (ln/2)^2 + n(r-l) - 2$, где l — длина кратчайшего цикла графа Γ_ψ, проходящего через дугу (μ, m).

В [10] исследован алгоритм «поиска в глубину», используемый для определения длин всех простых циклов сильносвязного n-вершинного орграфа. Вычислительная сложность алгоритма оценивается величиной порядка $\mathrm{O}(n^2 \log n)$, где элементарной операцией считается обращение к памяти и распознавание смежности двух вершин.

В [10] исследован также алгоритм распознавания примитивности n-вершинного орграфа и вычисления его экспонента, основанный на быстром возведении в степень матрицы смежности вершин. Алгоритм требует $\mathrm{O}(n^3 \log n)$ операций сложения и умножения в поле $\mathrm{GF}(2)$.

2.2. Свойства экспонентов неориентированных графов

В [7] сформулированы равносильные критерии примитивности неориентированных графов (далее просто графов) при условии, что ребро можно считать циклом длины 2:

1) связный n-вершинный граф G примитивен тогда и только тогда, когда в G имеется простой цикл нечётной длины;
2) связный n-вершинный граф G примитивен тогда и только тогда, когда G не является двудольным.

Универсальная оценка экспонента примитивного графа [3, с. 409] значительно ниже аналогичной оценки для примитивных орграфов. Если n-вершинный граф G примитивен, то

$$\exp G \leqslant 2(n-1). \tag{3}$$

Рассмотрим n-вершинный граф G. Обозначим при $i \neq j$, где $i, j \in \{1, \ldots, n\}$: $w(i,j)$ — путь из i в j; $[i,j]$ — кратчайший путь из i в j; $[i,i]$ — кратчайший цикл, проходящий через вершину i; $\mathrm{len}[i,j]$ — длина пути $[i,j]$, измеряемая числом рёбер графа G, составляющих путь.

Обозначим через $e(C)$ эксцентриситет цикла C в неориентированном графе G, т. е.

$$e(C) = \max_{i \notin C} \{\min_{j \in C} \mathrm{len}[i,j]\}.$$

Верхнюю границу (3) экспонента графа G при $n > 1$ можно уточнить [7]: если l — длина длиннейшего простого цикла C нечётной длины в примитивном n-вершинном графе G, $1 \leqslant l \leqslant n$, то

$$\exp\Gamma \leqslant 2e(C) + l - 1 \leqslant 2n - l - 1.$$

Если простые циклы нечётных длин покрывают множество вершин графа G, то $\exp\Gamma \leqslant n-1$.

Построено множество графов [7], на которых достигается верхняя граница неравенства (3). Обозначим через $\Gamma_P(n)$ множество примитивных n-вершинных графов, состоящих из гамильтонова пути и петли, инцидентной одной из концевых вершин. При любом $n > 1$ множество $\Gamma_P(n)$ состоит из $n!$ изоморфных графов; абсолютная оценка $\exp\Gamma = 2n-2$ достигается на графах G из множества $\Gamma_P(n)$, и только на них.

3. Оценки субэкспонентов и множественных экспонентов систем матриц

Неотрицательную матрицу A называют субпримитивной, если $A^{[1,t]} > 0$, где $t \in N$, $A^{[1,t]} = A + A^2 + \ldots + A^t$. Субэкспонентом матрицы A называется наименьшее $\sigma \in N$, такое, что $A^{[1,\sigma]} > 0$, и обозначается $\operatorname{sbxp} A$. Если матрица A не субпримитивна, то положим $\operatorname{sbxp} A = \infty$.

Понятия экспонента и субэкспонента могут быть обобщены на систему квадратных неотрицательных матриц $\Omega = \{M_1, \ldots, M_p\}$ одинакового размера. Пусть $N_p = \{1, \ldots, p\}$, N_p^* — множество всех слов в алфавите N_p. Слову $w = s_1 \ldots s_l$ из N_p^* при заданной системе матриц Ω соответствует матрица $M_{s_1} \ldots M_{s_l}$, являющаяся элементом мультипликативной полугруппы $\langle\Omega\rangle$ неотрицательных матриц, порождённой системой Ω. Обозначим $M_{s_1} \ldots M_{s_l} = M(w) = (m_{i,j}(w))$.

Экспонентом системы матриц Ω (обозначается $\exp \Omega$) называется наименьшая длина l слова $w \in N_p^*$, при котором $M(w) > 0$. Если такого слова не существует, то полагаем $\exp \Omega = \infty$.

Субэкспонентом системы матриц Ω (обозначается $\operatorname{sbxp} \Omega$) называется наименьшая длина l слова $w \in N_p^*$, при котором $M^{[1,l]}(w) > 0$, где $M^{[1,l]}(w) = M_{s_1} + M_{s_1} M_{s_2} + \ldots + M(w)$. Если такого слова не существует, то полагаем $\operatorname{sbxp} \Omega = \infty$.

Известно [11], что для любой системы Ω квадратных неотрицательных матриц одинакового размера справедливо

$$\operatorname{sbxp} \Omega \leqslant \exp \Omega.$$

Пусть G_s — орграф с множеством вершин $\{1, \ldots, n\}$, где все дуги помечены числом s, а $M_s = (m_{ij}(s))$ — матрица смежности вершин орграфа G_s, $s = 1, \ldots, p$. Тогда объединение графов $G^{(p)} = G_1 \cup \ldots \cup G_p$ есть либо орграф, либо мультиграф (в зависимости от множества объединяемых дуг), которому соответствует система матриц смежности $\Omega = \{M_1, \ldots, M_p\}$. При этом любой путь длины l в мультиграфе (графе) $G^{(p)}$ помечен словом в алфавите N_p^* длины l. Отсюда система неотрицательных матриц Ω и соответствующий ей мультиграф $G^{(p)}$ одновременно примитивны (субпримитивны) или не примитивны (не субпримитивны), в случае примитивности (субпримитивности) их экспоненты (субэкспоненты) равны.

Для любого мультиграфа $G^{(p)}$ справедливо [11]

$$\operatorname{diam} G^{(p)} \leqslant \operatorname{sbxp} \Omega,$$

причём если $G = G_1 = \ldots = G_p$, то $\operatorname{diam} G = \operatorname{sbxp} \Omega$.

В [11] показано, что мультиграф $G^{(p)}$ сильно связен тогда и только тогда, когда он субпримитивен. Если n-вершинный мультиграф $G^{(p)}$ сильно связен, то при $n \geqslant 4$

$$\operatorname{sbxp} \Omega \leqslant \frac{(n^2 - 2)(n - 1)}{2}.$$

Система квадратных неотрицательных матриц одинакового размера называется множественно примитивной, если существует натуральное l, такое, что для любого слова длины l в алфавите N_p^* имеет место неравенство $M(w) > 0$. Минимальное число k, обладающее таким свойством, называется множественным экспонентом системы матриц Ω.

В [12] доказано, что множество вполне неразложимых матриц порядка n является множественно примитивным и для множественного экспонента k имеет место оценка

$$k \leqslant n - 1.$$

Известна достижимая оценка множественного экспонента любой множественно примитивной системы Ω квадратных неотрицательных матриц порядка n: $k \leqslant 2^n - 2$.

Неотрицательная матрица A порядка n называется r-неразложимой, $0 \leqslant r \leqslant n$, если она не содержит нулевой подматрицы размера $p \times q$, $p + q = n - r + 1$, $0 < p$, $q \leqslant n - r$. Наибольшее из чисел r, при которых матрица A является r-неразложимой, называется индексом неразложимости A.

Пусть $\Omega = \{M_1, \ldots, M_p\}$ — система квадратных неотрицательных матриц порядка n, где индекс неразложимости каждой матрицы M_i, $i = 1, \ldots, p$, не меньше некоторого фиксированного числа r, $r \geqslant 1$. Тогда система Ω множественно примитивна [13], причём для множественного экспонента k системы Ω справедливо

$$k \leqslant \begin{cases} \dfrac{n-1}{r}, & (n-1) \bmod r = 0, \\ \left[\dfrac{n-1}{r}\right] + 1, & (n-1) \bmod r \neq 0. \end{cases}$$

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2009.
2. *Wielandt H.* Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. No. 52. S. 642–648.
3. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
4. *Носов В. А., Сачков В. Н., Тараканов В. Е.* Комбинаторный анализ. Неотрицательные матрицы, алгоритмические проблемы // Итоги науки и техники. Сер. теория вер., матем. статист., теорет. киберн. 1983. Т. 21. С. 120–178.
5. *Lewin M. and Vitek Y.* A system of gaps in the exponent set of primitive matrices // Illinois J. Math. 1981. Issue 1. No. 25. P. 87–98.
6. *Берж К.* Теория графов и её применение. М.: ИЛ, 1962.
7. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
8. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
9. *Князев А. В.* Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: дис. ... докт. физ.-мат. наук. М., 2002. 203 с.
10. *Кяжин С. Н., Фомичев В. М.* О примитивных наборах натуральных чисел // Прикладная дискретная математика. 2012. № 2(16). С. 5–14.
11. *Фомичев В. М.* Свойства путей в графах и мультиграфах // Прикладная дискретная математика. 2010. № 1(7). С. 118–124.
12. *Сачков В. Н.* Вероятностные преобразователи и правильные мультиграфы // Труды по дискретной математике. 1997. Т. 1. С. 227–250.
13. *Сачков В. Н., Ошкин И. Б.* Экспоненты классов неотрицательных матриц // Дискретная математика. 1993. Т. 5. Вып. 2. С. 150–159.