ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/24/1

УДК 519.6

КОМБИНАТОРНЫЕ СВОЙСТВА СИСТЕМ РАЗНОРАЗМЕРНЫХ 0,1-МАТРИЦ

Я. Э. Авезова*, В. М. Фомичев*,**

*Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

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

E-mail: avezovayana@gmail.com, fomichev@nm.ru

Исследованы комбинаторные свойства мультипликативной частичной полугруппы, порождённой системой разноразмерных неотрицательных матриц. Понятие примитивности распространено с систем квадратных неотрицательных матриц на системы разноразмерных матриц. Даны оценки экспонента системы разноразмерных неотрицательных матриц.

Ключевые слова: *система разноразмерных матриц, частичная полугруппа, примитивная система матриц, экспонент.*

Введение

Исследование экспонентов квадратных неотрицательных матриц относится к одному из классических направлений исследований в дискретной математике и криптологии. Важность этого направления в криптологии связана с применением матрично-графового подхода к исследованию перемешивающих свойств композиций функций и, в конечном счете, с получением оценок стойкости криптосистем относительно методов последовательного опробования. Второе важное направление приложений — это исследование функций, распространяющих искажения.

В [1] понятие экспонента распространено с матрицы (графа) на систему квадратных неотрицательных матриц (систему графов). Ранее для систем квадратных матриц рассматривался также множественный экспонент [2]. Обзор известных результатов по экспонентам матриц (графов) и систем матриц дан в [3].

В данной работе понятие экспонента распространяется на новый класс алгебраических структур — множество систем неотрицательных разноразмерных (не квадратных) матриц. Таким образом, объект исследования здесь — мультипликативная частичная полугруппа матриц. Прикладное значение расширения объекта исследования определяется использованием в криптографических схемах композиций функций $X^n \to X^m$, где $n \neq m$ и, как правило, $X = \{0, 1\}$. Например, в DES-алгоритме раундовая подстановка построена с использованием отображения расширения, реализующего функцию $X^{32} \to X^{48}$, и системы s-боксов, реализующей функцию $X^{48} \to X^{32}$.

Полученные результаты могут быть использованы как для анализа, так и для построения криптографических систем.

1. Определяющие свойства систем разноразмерных матриц

Пусть $\hat{M} = \{M_1, \ldots, M_p\}$ — система разноразмерных 0,1-матриц, то есть матриц над множеством $\{0, 1\}$, где матрица M_i имеет размеры $m_i \times k_i$ и в общем случае $m_i \neq k_i$, $i = 1, \ldots, p$. Порядком системы разноразмерных матриц (СРМ), обозначаемым $|\hat{M}|$, назовём число p составляющих её матриц.

Рассмотрим СРМ $\hat{M}$ как алфавит, в котором можно строить слова. Длиной слова называется число символов алфавита, составляющих слово.

Пару матриц (M_i, M_j) назовем *разрешённой* (*допустимой*) *биграммой* (то есть разрешённым словом длины 2) в алфавите $\hat{M}$, если $k_i = m_j$, $i, j \in \{1, \ldots, p\}$. Для разрешённой пары (M_i, M_j) определено произведение матриц $M_i M_j$, в противном случае произведение матриц не определено. Слово $M_{i_1} \ldots M_{i_l}$ *разрешённое* (*допустимое*) тогда и только тогда, когда любая биграмма слова является разрешённой. Разрешённому слову $M_{i_1} \ldots M_{i_l}$ длины l в алфавите $\hat{M}$ соответствует матрица $\varphi(M_{i_1} \ldots M_{i_l})$ размера $m_{i_1} \times k_{i_l}$, являющаяся произведением матриц $M_{i_1} \ldots M_{i_l}$.

Обозначим: $\hat{M}^*$ — множество всех слов в алфавите $\hat{M}$; $D(\hat{M}^*)$ — множество всех разрешённых слов в алфавите $\hat{M}$; $\langle \hat{M} \rangle$ — частичная полугруппа разноразмерных матриц (по умножению), порождённая системой $\hat{M} = \{M_1, \ldots, M_p\}$. Частичная полугруппа $\langle \hat{M} \rangle$ состоит из матриц, соответствующих всем разрешённым словам в алфавите $\hat{M}$, то есть $\langle \hat{M} \rangle = \varphi(D(\hat{M}^*))$. При умножении двух матриц в полугруппе $\langle \hat{M} \rangle$ сначала выполняется умножение этих матриц над множеством целых неотрицательных чисел, после чего все положительные элементы заменяются единицами.

На множестве $D(\hat{M}^*)$ определена частичная операция конкатенации слов. Конкатенация слов w_1 и w_2 (записывается как $w_1 w_2$) является разрешённой, если последний символ слова w_1 и первый символ слова w_2 образуют разрешённую пару в алфавите $\hat{M}$. Конкатенация пустого (то есть не содержащего символов) слова с любым словом является разрешённой. Заметим, что $D(\hat{M}^*)$ есть полугруппа относительно операции конкатенации и φ есть гомоморфизм $D(\hat{M}^*) \to \langle \hat{M} \rangle$.

Свойства СРМ удобно описывать с использованием композиционных графов.

Определение 1. *Композиционным графом системы матриц* $\hat{M}$ (обозначается $\Gamma(\hat{M})$) назовём p-вершинный ориентированный граф, в котором вершина i биективно соответствует матрице M_i и пара (i, j) есть дуга графа $\Gamma(\hat{M})$ тогда и только тогда, когда (M_i, M_j) есть разрешённая биграмма в алфавите $\hat{M}$, то есть $k_i = m_j$, $i, j \in \{1, \ldots, p\}$.

В частности, системе из p квадратных матриц порядка n соответствует полный p-вершинный ориентированный граф.

Далее считаем, что полугруппа $\langle \hat{M} \rangle$ не пуста и граф $\Gamma(\hat{M})$ не содержит изолированных вершин.

2. Связность СРМ

Классифицируем СРМ по свойству связности композиционных графов.

Определение 2. Если композиционный граф $\Gamma(\hat{M})$ имеет одну (более одной) компоненту связности, то соответствующую СРМ $\hat{M}$ назовём *связной* (*несвязной*).

Подсистему $\hat{M}'$ несвязной СРМ $\hat{M}$ назовем *компонентой связности системы* $\hat{M}$, если граф $\Gamma(\hat{M}')$ — максимальный связный подграф графа $\Gamma(\hat{M})$ (то есть связный подграф, не являющийся подграфом другого связного подграфа графа $\Gamma(\hat{M})$).

Определение 3. СРМ $\hat{M}$ назовём *сильносвязной*, если её композиционный граф $\Gamma(\hat{M})$ сильносвязный.

Пример 1. Проиллюстрируем связность на примере СРМ порядка 5.

Пусть $\hat{M}^{(1)} = \{M_1^{(1)}, \ldots, M_5^{(1)}\}$, где $M_1^{(1)}, \ldots, M_5^{(1)}$ имеют размеры 8×9, 9×10, 10×8, 11×12 и 12×11 соответственно. Частичная полугруппа $\langle\hat{M}^{(1)}\rangle$ не является связной. На рис. 1,*а* приведён композиционный граф $\Gamma(\hat{M}^{(1)})$.

Пусть $\hat{M}^{(2)} = \{M_1^{(2)}, \ldots, M_5^{(2)}\}$, где $M_1^{(2)}, \ldots, M_5^{(2)}$ имеют размеры 8×9, 9×10, 10×11, 11×12 и 12×9 соответственно. Частичная полугруппа $\langle\hat{M}^{(2)}\rangle$ является связной, но не сильносвязной. На рис. 1,*б* приведён композиционный граф $\Gamma(\hat{M}^{(2)})$.

Пусть $\hat{M}^{(3)} = \{M_1^{(3)}, \ldots, M_5^{(3)}\}$, где $M_1^{(3)}, \ldots, M_5^{(3)}$ имеют размеры 7×8, 8×9, 10×8, 9×10 и 10×7 соответственно. Частичная полугруппа $\langle\hat{M}^{(3)}\rangle$ является сильносвязной. На рис. 1,*в* приведён композиционный граф $\Gamma(\hat{M}^{(3)})$.

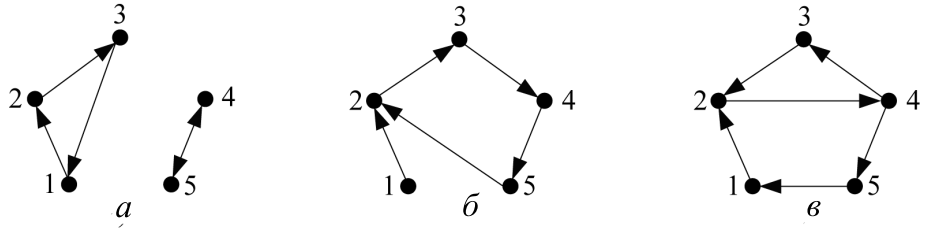

Рис. 1. Композиционные графы несвязной (*а*), связной (*б*) и сильносвязной (*в*) СРМ

3. Регулярность СРМ

Классифицируем СРМ по свойствам слов полугруппы $D(\hat{M}^*)$.

Если конкатенация wv слов w и v разрешена, то слово v называется продолжением слова w. Продолжение слова w называется нетривиальным, если v — непустое слово.

Например, если wvu — разрешённая конкатенация трёх слов, то v и vu — продолжения слова w, u — продолжение слов v и wv.

Определение 4. Пусть $w \in D(\hat{M}^*)$. Слово w называется:

— *нерегулярным*, если длина любого его продолжения ограничена, то есть не превышает некоторой фиксированной числовой границы τ;
— *регулярным*, если для любого натурального числа τ найдётся продолжение слова w, имеющее длину τ;
— *сильно регулярным*, если любое его продолжение допускает дальнейшее нетривиальное продолжение.

Из определения 4 следует:

— множества регулярных и нерегулярных слов не пересекаются;
— сильно регулярные слова являются регулярными.

Определение 5. СРМ $\hat{M}$ называется:

— *нерегулярной*, если полугруппа $D(\hat{M}^*)$ не содержит регулярных слов;
— *регулярной*, если полугруппа $D(\hat{M}^*)$ содержит хотя бы одно регулярное слово;
— *сильно регулярной*, если $D(\hat{M}^*)$ состоит только из сильно регулярных слов.

Теорема 1.

а) СРМ $\hat{M}$ регулярная тогда и только тогда, когда граф $\Gamma(\hat{M})$ циклический. В нерегулярной СРМ длина слов полугруппы $\langle\hat{M}\rangle$ не превышает p.

б) СРМ $\hat{M}$ сильно регулярная тогда и только тогда, когда граф $\Gamma(\hat{M})$ не содержит вершин с нулевой полустепенью исхода.

в) Сильносвязная СРМ является сильно регулярной.

Доказательство.

а) В силу определения регулярной СРМ $\hat{M}$, в полугруппе $D(\hat{M}^*)$ имеется регулярное слово w. Тогда w допускает продолжение сколь угодно большой длины. Так как алфавит $\hat{M}$ конечный, то слово w содержит повторение символов алфавита, то есть граф $\Gamma(\hat{M})$ имеет цикл.

Обратно, если граф $\Gamma(\hat{M})$ имеет цикл, то соответствующее слово, состоящее из k-кратного повторения цикла, принадлежит полугруппе $D(\hat{M}^*)$, $k = 1, 2, \ldots$, то есть полугруппа $D(\hat{M}^*)$ содержит регулярное слово.

Отсюда следует также, что нерегулярное слово не содержит повторяющихся символов, следовательно, длина его ограничена порядком p алфавита $\hat{M}$.

б) По определению сильно регулярной СРМ $\hat{M}$ имеем, что любое слово из $D(\hat{M}^*)$ сильно регулярное, то есть допускает дальнейшее продолжение. Это равносильно тому, что полустепень исхода любой вершины графа $\Gamma(\hat{M})$ отлична от нулевой.

в) Сильносвязный граф $\Gamma(\hat{M})$ не содержит вершин с нулевой полустепенью исхода. Отсюда по теореме 1, б СРМ $\hat{M}$ — сильно регулярная. ■

Пример 2. Рассмотрим композиционные графы сильно регулярных, регулярных и нерегулярных СРМ на примере СРМ порядка 5.

Пусть $\hat{M}^{(4)} = \{M_1^{(4)}, \ldots, M_5^{(4)}\}$, где $M_1^{(4)}, \ldots, M_5^{(4)}$ имеют размеры 2×5, 5×5, 5×5, 6×6 и 3×6 соответственно. Данная СРМ является сильно регулярной, её композиционный граф представлен на рис. 2,*а*.

Пусть $\hat{M}^{(5)} = \{M_1^{(5)}, \ldots, M_5^{(5)}\}$, где $M_1^{(5)}, \ldots, M_5^{(5)}$ имеют размеры 2×5, 5×5, 5×5, 6×7 и 3×6 соответственно. Данная СРМ является регулярной (например, M_1M_2 — регулярное слово), но не сильно регулярной (полустепень исхода вершины 4 равна 0), её композиционный граф представлен на рис. 2,*б*.

Пусть $\hat{M}^{(6)} = \{M_1^{(6)}, \ldots, M_5^{(6)}\}$, где $M_1^{(6)}, \ldots, M_5^{(6)}$ имеют размеры 2×5, 5×6, 6×7, 7×8 и 8×3 соответственно. Данная СРМ является нерегулярной, её композиционный граф представлен на рис. 2,*в*.

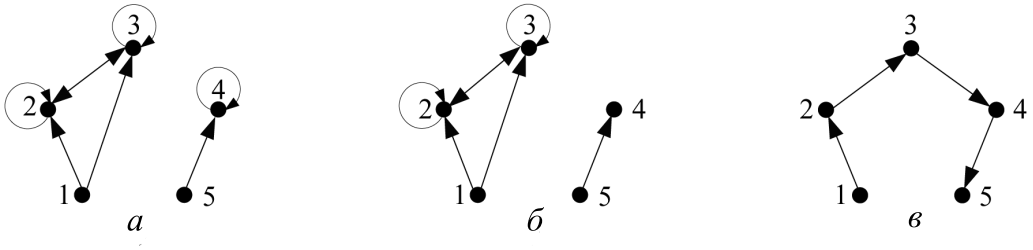

Рис. 2. Композиционные графы сильно регулярной (*а*), регулярной (*б*) и нерегулярной (*в*) СРМ

4. Примитивность СРМ

Данное в [1] определение примитивности системы квадратных неотрицательных матриц порядка n (n-вершинных графов) распространено в [2] на СРМ. Приведём это определение в равносильной формулировке, удобной для дальнейшего изложения.

Система разноразмерных матриц $\hat{M}$ называется примитивной, если в полугруппе $D(\hat{M}^*)$ найдётся слово w, такое, что $\varphi(w) > 0$, то есть все элементы матрицы $\varphi(w)$ положительны. *Экспонентом системы матриц* $\hat{M}$ (обозначается $\exp \hat{M}$) называется наименьшая из длин слов w, таких, что $\varphi(w) > 0$. Если такого слова w не существует,

то полагаем $\varphi(w) = \infty$. Отметим, что такое определение экспонента является корректным и для множества несвязных СРМ.

Пусть X — частично упорядоченное или квазиупорядоченное множество, L — линейно упорядоченное множество. Функция $f : X \to L$ называется изотонной (антиизотонной) [4] (по другой терминологии — монотонной (антимонотонной)), если для любых $x, x' \in X$ из отношения $x \leqslant x'$ следует, что $f(x) \leqslant f(x')$ $(f(x) \geqslant f(x'))$.

Обозначим $M_0(n \times m)$ множество всех неотрицательных матриц размера $n \times m$. Пусть $A, A' \in M_0(n \times m)$, где $A = (a_{ij})$, $A' = (a'_{ij})$. Положим $A \geqslant A'$ тогда и только тогда, когда $a_{ij} \geqslant a'_{ij}$ для всех $i = 1, \ldots, n$, $j = 1, \ldots, m$. Если при этом существуют такие i и j, что $a_{ij} > a'_{ij}$, то запишем $A > A'$. Бинарное отношение $\geqslant$ обладает свойствами рефлексивности, антисимметричности и транзитивности и, следовательно, является отношением частичного порядка.

Обозначим $[M_0]$ множество всех СРМ. Пусть $\hat{M}, \hat{U} \in [M_0]$, где $\hat{M} = \{M_1, \ldots, M_p\}$, $\hat{U} = \{U_1, \ldots, U_s\}$ — связные СРМ. Положим $\hat{U} \leqslant \hat{M}$, если при любом $i = 1, \ldots, s$ найдётся $j \in \{1, \ldots, p\}$, такое, что $U_i \leqslant M_j$. Данное бинарное отношение рефлексивно и транзитивно, но не антисимметрично, следовательно, является отношением квазипорядка.

Рассмотрим экспонент как функцию $[M_0] \to \mathbb{N}$.

Утверждение 1. Экспонент является антиизотонной функцией $[M_0] \to \mathbb{N}$.

Доказательство. Пусть $\hat{U} \leqslant \hat{M}$ и $A_1, \ldots, A_t \in \hat{U}$. Тогда произведение $A_1 \cdot \ldots \times \times A_t \in \langle \hat{U} \rangle$. Так как $\hat{U} \leqslant \hat{M}$, то в СРМ $\hat{M}$ найдутся матрицы $B_1, \ldots, B_t$, такие, что $A_i \leqslant B_i$, $i = 1, \ldots, t$. Тогда $A_1 \cdot \ldots \cdot A_t \leqslant B_1 \cdot \ldots \cdot B_t$. Следовательно, если $A_1 \cdot \ldots \cdot A_t > 0$, то и $B_1 \cdot \ldots \cdot B_t > 0$. Отсюда $\exp \hat{M} \leqslant \exp \hat{U}$. ■

Следствие 1. Экспонент является антиизотонной функцией $M_0(n \times n) \to \mathbb{N}$.

Доказательство. Пусть $\hat{U}$ и $\hat{M}$ — системы порядка 1, то есть $\hat{U} = \{A\}$, $\hat{M} = \{B\}$, где $A, B \in M_0(n \times n)$. Тогда отношение $\hat{U} \leqslant \hat{M}$ равносильно отношению $A \leqslant B$ и $\exp \hat{M} = \exp B$, $\exp \hat{U} = \exp A$. Тогда $\exp B \leqslant \exp A$ по утверждению 1. ■

Следствие 2. Если $\hat{U} \subseteq \hat{M}$, то $\exp \hat{M} \leqslant \exp \hat{U}$.

Доказательство. Если $\hat{U} \subseteq \hat{M}$, то $\hat{U} \leqslant \hat{M}$. Тогда $\exp \hat{M} \leqslant \exp \hat{U}$ по утверждению 1. ■

Замечание 1. Из утверждения 1 и его следствий получаем:

— если СРМ $\hat{M}$ не примитивна, то любая её подсистема $\hat{U}$ тоже не примитивна;

— если подсистема $\hat{U}$ системы $\hat{M}$ примитивная, то СРМ $\hat{M}$ тоже примитивная; в частности, СРМ, содержащая квадратную примитивную матрицу, примитивна.

Утверждение 2. Если $\tilde{M}_1, \ldots, \tilde{M}_r$ суть все примитивные компоненты связности несвязной СРМ $\hat{M}$, то $\exp \hat{M} = \min\{\exp \tilde{M}_1, \ldots, \exp \tilde{M}_r\}$.

Доказательство. Так как СРМ $\hat{M}$ несвязная, то алфавит $\hat{M}$ разбивается на непустые блоки $\tilde{M}_1, \ldots, \tilde{M}_r$, соответствующие компонентам связности графа $\Gamma(\hat{M})$. Это разбиение индуцирует разбиение полугруппы $D(\hat{M}^*)$ на подполугруппы $D(\tilde{M}_1^*), \ldots, D(\tilde{M}_r^*)$. Следовательно, если наименьшая длина слова w_i из $D(\tilde{M}_i^*)$, такого, что $\varphi(w_i) > 0$, равна $\exp \tilde{M}_i$, $i = 1, \ldots, r$, то кратчайшее слово w из $D(\hat{M}^*)$, такое, что $\varphi(w) > 0$, совпадает с одним из слов $w_1, \ldots, w_r$, и длина слова w равна $\min\{\exp \tilde{M}_1, \ldots, \exp \tilde{M}_r\}$. ■

Разрешённое слово $w = M_{i_1} \ldots M_{i_l}$ длины l в алфавите $\hat{M}$ назовём *правильным*, если $m_{i_1} = k_{i_l}$. Если слово w правильное, то $\varphi(w)$ — квадратная матрица порядка m_{i_1}

и определён $\exp\varphi(w)$. Обозначим через $R(\hat{M}^*)$ множество всех правильных слов в алфавите $\hat{M}$.

Утверждение 3.

а) Разрешённое слово $w = M_{i_1} \dots M_{i_l}$ является правильным тогда и только тогда, когда $(i_1, \dots, i_l)$ есть цикл в графе $\Gamma(\hat{M})$.

б) Пусть $R(\hat{M}^*) = \{w_1, w_2, \dots\}$, тогда $\exp\hat{M} \leqslant \min\{\exp w_1, \exp w_2, \dots\}$.

Доказательство.

а) Путь $(i_1, \dots, i_l)$ в графе $\Gamma(\hat{M})$ является циклом тогда и только тогда, когда в $\Gamma(\hat{M})$ имеется дуга (i_l, i_1), то есть $m_{i_1} = k_{i_l}$. Это равносильно тому, что слово w правильное.

б) Любая степень матрицы $\varphi(w_i)$ принадлежит полугруппе $\langle\hat{M}\rangle$, $i = 1, 2, \dots$ Если матрица $\varphi(w_i)$ примитивная, то существует $\exp\varphi(w_i)$, равный наименьшему натуральному $t(i)$, такому, что $(\varphi(w_i))^{t(i)} > 0$. Следовательно, $\exp\hat{M} \leqslant t(i) = \exp w_i$, $i = 1, 2, \dots$ Отсюда получаем утверждение. ■

5. Эквивалентность СРМ

СРМ $\hat{M}$ и $\hat{U}$ называются *эквивалентными* (обозначим $\hat{M} \approx \hat{U}$), если $\exp\hat{M} = \exp\hat{U}$.

Утверждение 4. $\hat{M} \approx \hat{U}$, если $\hat{U} \leqslant \hat{M}$ и $\hat{M} \leqslant \hat{U}$.

Доказательство. Если $\hat{U} \leqslant \hat{M}$, то $\exp\hat{M} \leqslant \exp\hat{U}$ по утверждению 1. Если $\hat{M} \leqslant \hat{U}$, то по утверждению 1 $\exp\hat{U} \leqslant \exp\hat{M}$. Следовательно, $\exp\hat{U} = \exp\hat{M}$. ■

Пусть матрица $A \in \hat{M}$. Матрица A называется *максимальной матрицей системы* $\hat{M}$, если из отношения $A \leqslant A'$ следует $A = A'$.

СРМ $\hat{M}$ называется *сокращённой*, если она состоит только из максимальных матриц. Заметим, что любая СРМ может быть приведена к сокращённой СРМ удалением всех немаксимальных матриц.

Утверждение 5. Любая СРМ $\hat{M}$ эквивалентна своей сокращенной подсистеме.

Доказательство. Рассмотрим СРМ $\hat{U} = \hat{M} \setminus \hat{V}$, где $\hat{V}$ — подмножество всех немаксимальных матриц системы $\hat{M}$. По построению $\hat{U} \subseteq \hat{M}$, значит, $\exp\hat{M} \leqslant \exp\hat{U}$ по следствию 2 утверждения 1.

С другой стороны, $\hat{M} \leqslant \hat{U}$ в силу того, что СРМ $\hat{U}$ состоит из всех максимальных матриц системы $\hat{M}$. Следовательно, по утверждению 1 $\exp\hat{U} \leqslant \exp\hat{M}$, то есть выполнено обратное неравенство. Отсюда $\hat{M} \approx \hat{U}$. ■

6. Универсальная нижняя оценка экспонента сильносвязных СРМ

СРМ $\hat{M} = \{M_1, \dots, M_p\}$ поставим в соответствие (обозначим это соответствие ψ) систему квадратных матриц $\hat{M}' = \{M_1', \dots, M_p'\}$ порядка n, где $n = \max\{m_1, \dots, m_p\}$. Матрица M_i' получена из матрицы M_i размера $m_i \times k_i$ дополнением снизу $n - m_i$ нулевыми строками размера k_i и справа $n - k_i$ нулевыми столбцами размера n, $i = 1, \dots, p$.

Теорема 2. Если СРМ $\hat{M}$ сильносвязная, то:

а) $\max\{k_1, \dots, k_p\} = n$;

б) ψ — гомоморфизм со свойством $\psi(\langle\hat{M}\rangle) = \langle\hat{M}'\rangle$;

в) если матрица $A = M_1' + \dots + M_p'$ примитивная, то $\exp\hat{M} \geqslant \exp A$.

Доказательство.

а) По определению числа n в СРМ $\hat{M}$ имеется матрица размера $n \times k$, где $k \in \{k_1, \ldots, k_p\}$. Пусть для определённости это матрица M_1. В сильносвязном графе $\Gamma(\hat{M})$ имеется дуга $(j, 1)$, где $j \in \{2, \ldots, p\}$. Тогда матрица M_j имеет размеры $m_j \times n$, следовательно, $\max\{k_1, \ldots, k_p\} \geqslant n$.

Если $\max\{k_1, \ldots, k_p\} = n' > n$, то в СРМ $\hat{M}$ имеется матрица размера $m \times n'$, где $m \in \{m_1, \ldots, m_p\}$. Пусть для определённости это матрица M_p. В сильносвязном графе $\Gamma(\hat{M})$ имеется дуга (p, j), где $j \in \{1, \ldots, p-1\}$. Тогда матрица M_j имеет размеры $n' \times k_j$, отсюда $\max\{m_1, \ldots, m_p\} = n' > n$, то есть имеем противоречие с определением числа n. Следовательно, $\max\{k_1, \ldots, k_p\} = n$.

б) Из правил построения матриц $M'_1, \ldots, M'_p$ и умножения матриц следует, что для разрешённой биграммы $(M_i M_j)$ выполнено $\psi(M_i M_j) = \psi(M_i)\psi(M_j)$, то есть ψ — гомоморфизм полугрупп $\langle \hat{M} \rangle \to \langle \hat{M}' \rangle$.

в) При любом натуральном t матрица A^t есть сумма матриц, соответствующих всем словам длины t в алфавите $\hat{M}'$, а именно

$$A^t = \sum_{w \in (\hat{M})^t} \psi(\varphi(w)).$$

Удалив из суммы все матрицы, соответствующие неразрешённым словам в алфавите $\hat{M}$, выполним суммирование по словам длины t из полугруппы $\langle \hat{M} \rangle$. Тогда

$$A^t \geqslant \sum_{w \in (\hat{M})^t \cap \langle \hat{M} \rangle} \psi(\varphi(w)).$$

Если хотя бы одному разрешённому слову длины t соответствует положительная матрица, то $A^t > 0$. Вместе с тем матрица A^t может быть положительной, когда ни одна из слагаемых матриц не положительна. Следовательно, $\exp \hat{M} \geqslant \exp A$. ■

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
3. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 116–121.
4. *Биркгоф Г.* Теория решёток. М.: Наука, 1984. 567 с.