ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.1

УСЛОВИЯ ПРИМИТИВНОСТИ И ОЦЕНКИ ЭКСПОНЕНТОВ МНОЖЕСТВ ОРИЕНТИРОВАННЫХ ГРАФОВ

Я. Э. Авезова*, В. М. Фомичев*,**,***

*Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия
**Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия
***Институт проблем информатики ФИЦ ИУ РАН, г. Москва, Россия

Исследованы вопросы минимизации заданного примитивного множества неотрицательных матриц порядка n (n-вершинных орграфов), где минимизация понимается как определение минимальных примитивных подмножеств. Получен универсальный критерий примитивности множества орграфов $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$, $p > 1$, выраженный через характеристики мультиграфа $\Gamma_1 \cup \ldots \cup \Gamma_p$, в котором каждая дуга орграфа Γ_i помечена символом i, $i = 1, \ldots, p$. Показано, что задача распознавания примитивности множества орграфов алгоритмически разрешима. Для частного класса множеств, когда орграфы $\Gamma_1, \ldots, \Gamma_p$ содержат общее множество контуров, получен ряд достаточных условий примитивности множества $\hat{\Gamma}$. Для множества орграфов $\hat{\Gamma} = \{\Gamma_0, \ldots, \Gamma_{n-1}\}$, где Γ_i — граф с множеством вершин $\{0, \ldots, n-1\}$, имеющий гамильтонов контур $(0, \ldots, n-1)$ и дугу $(i, (i+l) \bmod n)$, где $n \geqslant l > 1$, $i = 0, \ldots, n-1$, уточнён критерий примитивности (множество орграфов $\hat{\Gamma}$ примитивное тогда и только тогда, когда НОД$(n, l-1) = 1$) и в случае примитивности получены оценки экспонента: $n-1 \leqslant \exp \hat{\Gamma} \leqslant 2n-2$. Минимальное примитивное подмножество множества $\hat{\Gamma}$, на котором достигается верхняя оценка экспонента, содержит не более n/d орграфов, где $d =$ НОД(n, l).

Ключевые слова: *граф Виландта, примитивное множество матриц (графов), экспонент графа.*

DOI 10.17223/20710410/35/8

CONDITIONS OF PRIMITIVITY AND EXPONENT BOUNDS FOR SETS OF DIGRAPHS

Y. E. Avezova*, V. M. Fomichev*,**,***

*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia
**Financial University under the Government of the Russian Federation, Moscow, Russia
***The Institute of Informatics Problems of the Russian Academy of Sciences, Moscow, Russia

E-mail: avezovayana@gmail.com, fomichev.2016@yandex.ru

For a set of digraphs $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$, $p > 1$, we present a criterion to be primitive. We do it in terms of characteristics of the multidigraph $\Gamma^{(p)} = \Gamma_1 \cup \ldots \cup \Gamma_p$ where each edge in Γ_i is assigned the label i, $i = 1, \ldots, p$. Any walk of length s in $\Gamma^{(p)}$ is assigned a word $w = w_1 \ldots w_s$ of length s over the alphabet $\{1, \ldots, p\}$, and the corresponding

product of digraphs $\Gamma(w) = \Gamma_{w_1} \cdot \ldots \cdot \Gamma_{w_s}$ is introduced. The walk is assigned the label w^t if it is the concatenation of t walks labeled with w. The multidigraph $\Gamma^{(p)}$ is called w-strongly connected if it is strongly connected and, for all its vertices i and j, there exists a walk in $\Gamma^{(p)}$ from i to j labeled with w^t for some natural number t. By the definition, the set of digraphs $\hat{\Gamma}$ is primitive if and only if $\Gamma(w)$ is primitive for some word w. Thus, we have the following criterion: the digraph $\Gamma(w)$ is primitive if and only if $\Gamma^{(p)}$ is w-strongly connected and has cycles labeled with $w^{t_1}, \ldots, w^{t_m}$, where $\gcd(t_1, \ldots, t_m) = 1$. As a corollary, we prove that the problem of recognizing the primitivity of $\hat{\Gamma}$ is algorithmically decidable. In the particular case, when the digraphs in $\hat{\Gamma}$ have the common set of cycles $\hat{C} = \{C_1, \ldots, C_m\}$ of lengths $l_1, \ldots, l_m$ respectively, $m \geqslant 1$, $l_1 \leqslant \ldots \leqslant l_m$, the digraph $\Gamma(w)$, $w = w_1 \ldots w_s$, is primitive if any one of the following conditions holds: a) $m = 1$ and $l_1 = 1$; b) $\gcd(l_1, \ldots, l_m) = s$; c) the digraph $C_1 \cup \ldots \cup C_m$ is connected and has quasi-Eulerian $\hat{C}$-cycle of length s. At last, for the set of digraphs $\hat{\Gamma} = \{\Gamma_0, \ldots, \Gamma_{n-1}\}$ with vertex set $\{0, \ldots, n-1\}$, where for some l, $n \geqslant l > 1$, each Γ_i, $i \in \{0, \ldots, n-1\}$, has a Hamiltonian cycle $(0, \ldots, n-1)$ and the edge $(i, (i + l) \mod n)$, we prove the following criterion of primitivity and bounds for the exponent: the set $\hat{\Gamma} = \{\Gamma_0, \ldots, \Gamma_{n-1}\}$ is primitive if and only if $\gcd(n, l-1) = 1$, and in this case $n - 1 \leqslant \exp\hat{\Gamma} \leqslant 2n - 2$. The minimal subset of $\hat{\Gamma} = \{\Gamma_0, \ldots, \Gamma_{n-1}\}$ with exponent $2n - 2$ contains at most n/d digraphs, where $d = \gcd(n, l)$. The presented results are used for evaluating mixing properties of cryptographic functions compositions.

Keywords: *Wielandt's graph, primitive set of matrices (digraphs), exponent of digraph.*

Введение

Введём основные обозначения:

- $\mathbb{N}$ — множество натуральных чисел;
- $N_p = \{1, \ldots, p\}$, $p \in \mathbb{N}$;
- $V = \{1, \ldots, n\}$ — множество вершин орграфа;
- X^* — множество всех слов в конечном алфавите X;
- НОД$(a_1, \ldots, a_n)$ — наибольший общий делитель натуральных чисел $a_1, \ldots, a_n$;
- (i, j) — дуга в орграфе Γ, инцидентная вершинам i и j;
- $[i, j]$ — путь в орграфе Γ из вершины i в вершину j;
- $\langle Y \rangle$ — полугруппа, порождённая подмножеством Y мультипликативной полугруппы;
- $M_0(n)$ — множество всех $0, 1$-матриц порядка n;
- $\Gamma(n)$ — множество всех n-вершинных орграфов.

Понятие примитивности (множественной) для множества ориентированных графов и неотрицательных матриц впервые введено В. Н. Сачковым в [1]. Множество матриц $\hat{M}$ называется множественно примитивным, если при некотором $l \in \mathbb{N}$ положительны все слова длины l в алфавите $\hat{M}$. Наименьшее такое l называется множественным экспонентом множества $\hat{M}$. Множественный экспонент любого множественно примитивного множества не превышает $2^n - 2$. В [2] даны оценки множественного экспонента для некоторых классов множеств орграфов.

Исследуемое в работе свойство примитивности множества матриц введено в [3] и определено как существование положительного слова в алфавите $\hat{M}$, где слово называется положительным, если произведение составляющих его матриц есть положи-

тельная матрица. Экспонентом примитивного множества $\hat{M}$ называется наименьшая длина положительного слова в алфавите $\hat{M}$.

Данная работа посвящена вопросам минимизации заданного примитивного множества $\hat{M}$ неотрицательных матриц порядка n (n-вершинных орграфов), где минимизация понимается как определение минимальных примитивных подмножеств множества $\hat{M}$. В [4] введено понятие сокращённого множества матриц и доказано, что экспонент множества матриц равен экспоненту его сокращённого подмножества. Таким образом, исследование примитивности множества матриц можно свести к исследованию примитивности сокращённых множеств. Заметим, что при сокращении исходного множества матриц (орграфов) величина экспонента может увеличиться. Понятие сокращённого множества обобщено, что позволяет ограничить исследование примитивности множества матриц ещё более узким классом множеств.

Построен критерий примитивности множества орграфов $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$, $p > 1$, в терминах свойств мультиграфа $\Gamma_1 \cup \ldots \cup \Gamma_p$. Показано, что задача распознавания примитивности множества орграфов алгоритмически разрешима. Для частного класса множеств, когда орграфы $\Gamma_1, \ldots, \Gamma_p$ содержат общее множество контуров, получен ряд достаточных условий примитивности множества $\hat{\Gamma}$.

В силу широкого применения в криптосистемах регистровых преобразований особый интерес представляет исследование примитивности множества графов, соответствующих регистрам сдвига. Для частного класса таких множеств уточнён критерий примитивности, получена оценка экспонента.

1. Минимизация примитивного множества матриц

Обозначим: $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ — множество орграфов с множеством вершин V, где все дуги орграфа Γ_r помечены числом r; $\hat{M} = \{M_1, \ldots, M_p\}$ — множество 0,1-матриц, где $M_r = (m_{ij}(r))$ — матрица смежности вершин орграфа Γ_r, $r = 1, \ldots, p$, $p > 1$.

Пусть $w = w_1 \ldots w_s$ — слово в алфавите N_p. Тогда слову $(M_{w_1}, \ldots, M_{w_s}) \in \langle \hat{M} \rangle$ (слову $(\Gamma_{w_1}, \ldots, \Gamma_{w_s}) \in \langle \hat{\Gamma} \rangle$) соответствует произведение матриц $M(w) = M_{w_1} \ldots M_{w_s}$ (произведение орграфов $\Gamma(w) = \Gamma_{w_1} \ldots \Gamma_{w_s}$); положим $M(w) = (m_{ij}(w))$. Слово $(M_{w_1}, \ldots, M_{w_s})$ назовём положительным (примитивным), если матрица $M(w)$ положительная (примитивная). Слово $(\Gamma_{w_1}, \ldots, \Gamma_{w_s})$ назовём положительным (примитивным), если орграф $\Gamma(w)$ полный (примитивный). Множество $\hat{M}$ (множество $\hat{\Gamma}$) называется примитивным, если полугруппа $\langle \hat{M} \rangle$ содержит положительное слово (полугруппа $\langle \hat{\Gamma} \rangle$ содержит полный орграф), наименьшая длина положительного слова называется экспонентом множества $\hat{M}$ (множества $\hat{\Gamma}$) (обозначается $\exp \hat{M}$ и $\exp \hat{\Gamma}$ соответственно).

Отметим важные свойства множеств $M_0(n)$ и $\Gamma(n)$ [3, 5]:

1) На множестве $M_0(n)$ задан частичный порядок: $M \leqslant M' \Leftrightarrow m_{ij} \leqslant m'_{ij}$ для всех $i, j = 1, \ldots, n$. Если при этом существуют такие i и j, что $m_{ij} < m'_{ij}$, то пишем $M < M'$. Пусть M, M' — матрицы смежности орграфов Γ, Γ' соответственно и $M \leqslant M'$, тогда все дуги орграфа Γ являются дугами орграфа Γ', т. е. Γ — часть орграфа Γ' (обозначается $\Gamma \leqslant \Gamma'$).
2) На множестве всех подмножеств множества $\Gamma(n)$ задан квазипорядок: $\hat{\Gamma} \geqslant \hat{\Gamma}'$ для данных множеств $\hat{\Gamma}, \hat{\Gamma}' \Leftrightarrow$ для любого орграфа $\Gamma' \in \hat{\Gamma}'$ имеется орграф $\Gamma \in \hat{\Gamma}$, где $\Gamma \geqslant \Gamma'$. Если $\hat{\Gamma} \geqslant \hat{\Gamma}'$, то $\exp \hat{\Gamma} \leqslant \exp \hat{\Gamma}'$.
3) Если множество $\hat{\Gamma}$ примитивное, то орграф $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_p$ также примитивный и $\exp \Gamma \leqslant \exp \hat{\Gamma} \leqslant \min\{\exp \Gamma_1, \ldots, \exp \Gamma_p\}$.

Пусть $\hat{M}$ — примитивное множество матриц из $M_0(n)$, $\hat{\Gamma}$ — примитивное множество n-вершинных орграфов, $M \in \hat{M}$, $\Gamma \in \hat{\Gamma}$. Обозначим: $\hat{M}\backslash M$ — подмножество $\hat{M}$, полученное удалением из $\hat{M}$ матрицы M; $\hat{\Gamma}\backslash\Gamma$ — подмножество $\hat{\Gamma}$, полученное удалением из $\hat{\Gamma}$ орграфа Γ. Слово $(M_{w_1}, \ldots, M_{w_s})$ в алфавите $\hat{M}\backslash M$ назовём покрывающим для M, если $M \leqslant M(w)$. Слово $(\Gamma_{w_1}, \ldots, \Gamma_{w_s})$ в алфавите $\hat{\Gamma}\backslash\Gamma$ назовём покрывающим для Γ, если $\Gamma \leqslant \Gamma(w)$. Матрицу M (орграф Γ), для которой существует покрывающее слово, назовём избыточной матрицей в множестве $\hat{M}$ (избыточным орграфом в множестве $\hat{\Gamma}$). Множество $\hat{M}$ (множество $\hat{\Gamma}$) называется минимальным, если оно не содержит избыточной матрицы (орграфа). В частности, если множество $\hat{M}$ содержит примитивную матрицу M, то минимальным является одноэлементное множество $\{M\}$.

Задача минимизации примитивного множества $\hat{M}$ (множества $\hat{\Gamma}$) состоит в определении его минимальных примитивных подмножеств.

Утверждение 1. Матрица M — избыточная в примитивном множестве $\hat{M}$, если и только если подмножество $\hat{M}\backslash M$ примитивное.

Доказательство. Необходимость. Пусть M — избыточная в примитивном множестве $\hat{M}$ и $(M_{w_1}, \ldots, M_{w_s})$ — покрывающее слово для матрицы M, $M(w) = M_{w_1} \ldots M_{w_s}$. Так как множество $\hat{M}$ примитивное, то существует положительное слово в алфавите $\hat{M}$. Заменим в этом слове каждое вхождение символа M на слово $(M_{w_1}, \ldots, M_{w_s})$, получим слово в алфавите $\hat{M}\backslash M$. Поскольку $M \leqslant M(w)$, полученное слово положительное. Следовательно, подмножество $\hat{M}\backslash M$ примитивное.

Достаточность. Если $\hat{M}\backslash M$ примитивное, то существует некоторое положительное слово в алфавите $\hat{M}\backslash M$, а следовательно, и в алфавите $\hat{M}$. ■

Матрица M называется максимальной матрицей множества $\hat{M}$, если для матрицы $M' \in \hat{M}$ из соотношения $M \leqslant M'$ следует $M = M'$. Множество матриц $\hat{M}$ называется сокращённым, если оно состоит только из максимальных матриц [4]. Аналогично определяются понятия максимального орграфа и сокращённого множества орграфов. Любое множество матриц (орграфов) может быть приведено к сокращённому удалением всех немаксимальных матриц (орграфов).

Если множество матриц $\hat{M}$ (орграфов $\hat{\Gamma}$) не сокращённое, то в $\hat{M}$ ($\hat{\Gamma}$) есть такие матрицы M, M' (орграфы Γ, Γ'), что $M < M'$ ($\Gamma < \Gamma'$). Тогда M' (Γ') есть покрывающее слово длины 1 для M (Γ). Следовательно, минимальное множество матриц (орграфов) является сокращённым.

Множество $\langle M_0(n), \leqslant\rangle$ с введённым выше отношением частичного порядка образует решётку порядка 2^m, где $m = n^2$, изоморфную решётке двоичных n^2-мерных векторов. Количество положительных элементов матрицы M назовём её весом. Слоем с номером k решетки $\langle M_0(n), \leqslant\rangle$ назовём её подмножество, состоящее из матриц веса k, $k = 0, 1, \ldots, m$.

Утверждение 2. Пусть $\hat{M} = \{M_1, \ldots, M_p\}$ — сокращенное множество матриц. Тогда:

1) $\hat{M}$ образует антицепь в решётке $\langle M_0(n), \leqslant\rangle$ и $p \leqslant C_m^{\lceil m/2 \rceil}$;
2) при $p = 2$ существует $2^{2m-1} + 2^{m-1} - 3^m$ сокращённых множеств матриц.

Доказательство.

1) По определению любые две различные максимальные матрицы несравнимы. Значит, сокращённое множество состоит из попарно несравнимых матриц.

Количество матриц в антицепи не превышает ширину решетки $\langle M_0(n), \leqslant\rangle$, обозначаемую h, где $h = C_m^{\lceil m/2 \rceil}$ [3, с. 25].

2) Пусть M — матрица веса k. Тогда существует 2^{m-k} матриц, которые не меньше (поэлементно) матрицы M, и (2^k-1) матриц, которые поэлементно меньше матрицы M. Следовательно, для каждой матрицы веса k существует $r_k = 2^m - 2^{m-k} - 2^k + 1$ матриц, которые с ней несравнимы. Число матриц в k-м слое решётки равно C_m^k. Тогда общее количество упорядоченных пар несравнимых матриц равно

$$\begin{aligned}\sum_{k=1}^{m-1} C_m^k r_k = 2^m \sum_{k=1}^{m-1} C_m^k - \sum_{k=1}^{m-1} C_m^k 2^{m-k} - \sum_{k=1}^{m-1} C_m^k 2^k + \sum_{k=1}^{m-1} C_m^k = \\ = 2^m(2^m-2) - 2(3^m - 2^m - 1) + (2^m - 2) = 2^{2m} - 2\cdot 3^m + 2^m.\end{aligned} \tag{1}$$

Поскольку матрицы не упорядочены, число сокращённых множеств при $p=2$ вдвое меньше (1), т. е. равно $2^{2m-1} + 2^{m-1} - 3^m$. ■

Определим условия, при которых сокращённое множество из двух матриц $\hat{M} = \{A, B\}$ не является минимальным. Это означает, что матрицы A и B несравнимы, но существует такое натуральное t, что $A^t \geqslant B$ (либо $B^t \geqslant A$), и примитивность множества равносильна примитивности матрицы A (матрицы B).

Для оценки t воспользуемся понятием локальной примитивности матриц и орграфов [6]. Пусть $I = \{i_1, \ldots, i_k\}$, $J = \{j_1, \ldots, j_r\}$, $\varnothing \neq I, J \subseteq N_n$, A — матрица порядка n, $A(I \times J)$ — её подматрица размера $k \times r$, полученная из A удалением строк с номерами $i \notin I$ и столбцов $j \notin J$. Матрица A называется $I \times J$-примитивной, если существует число $\gamma \in \mathbb{N}$, такое, что матрица $A^t(I \times J)$ положительна при любом $t \geqslant \gamma$. Наименьшее такое число γ называется $I \times J$-экспонентом матрицы A, обозначается через $I \times J$-exp A. Орграф Γ называется $I \times J$-примитивным, если при некотором $\gamma \in \mathbb{N}$ для любых $(i,j) \in I \times J$ в Γ имеются пути длины $t \geqslant \gamma$ из i в j, наименьшее такое t равно $I \times J$-exp Γ. Если A — матрица смежности орграфа Γ, то A примитивная тогда и только тогда, когда примитивный Γ, и $I \times J$-exp $A = I \times J$-exp Γ. При $I = \{i\}$, $J = \{j\}$ обозначим $i \times j$-exp $A = I \times J$-exp A.

Далее $\Gamma(A)$ и $\Gamma(B)$ — n-вершинные орграфы с матрицами смежности $A = (a_{ij})$ и $B = (b_{ij})$ соответственно, $A^t = (a_{i,j}^{(t)})$, $t \geqslant 1$. Множество дуг орграфа $\Gamma(B)$ обозначим $E(B)$.

Утверждение 3. Пусть матрицы A и B несравнимы. Отношение $A^t \geqslant B$ выполнено при $t \in \mathbb{N}$, если и только если в $\Gamma(A)$ имеется путь длины t из i в j при любой паре $(i,j) \in E(B)$. В частности, если матрица A является $i \times j$-примитивной при любой паре $(i,j) \in E(B)$, то

$$t \leqslant \max_{(i,j) \in E(B)} i \times j\text{-exp } A.$$

Доказательство. Для выполнения условия $A^t \geqslant B$ необходимо и достаточно, чтобы $a_{i,j}^{(t)} = 1$ при любой паре $(i,j) \in E(B)$. В соответствии с теоремой, устанавливающей связь между орграфами и их матрицами смежности [7, с. 143], в матрице A^t элемент $a_{i,j}^{(t)}$ равен 1 тогда и только тогда, когда в $\Gamma(A)$ есть путь длины t из вершины i в вершину j. Следовательно, $A^t \geqslant B$ тогда и только тогда, когда в $\Gamma(A)$ есть путь длины t из вершины i в вершину j при любой паре $(i,j) \in E(B)$.

Если матрица A является $i \times j$-примитивной при любой паре $(i,j) \in E(B)$, то при любом $\tau \geqslant \max\limits_{(i,j) \in E(B)} i \times j$-exp$A$ выполнено $A^\tau \geqslant B$. Следовательно, $t \leqslant \max\limits_{(i,j) \in E(B)} i \times j$-exp A. ■

Замечание 1. Для выполнения условия $A^t \geqslant B$ при любом $t \leqslant \max\limits_{(i,j) \in E(B)} i \times j$-exp A необходимо, чтобы при любой паре $(i,j) \in E(B)$ в орграфе $\Gamma(A)$ существовал путь

из вершины i в вершину j, проходящий через вершину некоторого сильносвязного подграфа орграфа $\Gamma(A)$ [6, с. 73]. Достаточные условия $i\times j$-примитивности орграфа и оценки $i\times j$-экспонента приведены в [8].

2. Критерий примитивности множества графов

Если множество $\hat{\Gamma}$ примитивное, то мультиграф $\Gamma^{(p)}$ сильносвязный [3, 5]. В $\Gamma^{(p)}$ любой путь длины s помечен некоторым словом w длины s из N_p^*. В частности, путь в мультиграфе $\Gamma^{(p)}$ имеет метку w^t, если он есть конкатенация t путей с метками w; путь с меткой w^0 положим пустым.

Утверждение 4. В мультиграфе $\Gamma^{(p)}$ есть путь $[i,j]$ с меткой w^t, где $w = w_1 \dots w_s$, если и только если в орграфе $\Gamma(w)$ есть путь $[i,j]$ длины t.

Доказательство. В мультиграфе $\Gamma^{(p)}$ число путей длины l из вершины i в вершину j с меткой w равно $m_{ij}(w)$ [3, с. 57]. Отсюда в мультиграфе $\Gamma^{(p)}$ имеется путь $[i,j]$ с меткой w, если и только если в орграфе $\Gamma(w)$ есть дуга (i,j). Следовательно, в мультиграфе $\Gamma^{(p)}$ есть путь $[i,j]$ с меткой w^t, если и только если в орграфе $\Gamma(w^t)$ есть дуга (i,j), т. е. в орграфе $\Gamma(w)$ есть путь $[i,j]$ длины t. ■

Сильносвязный мультиграф $\Gamma^{(p)}$ назовём w-сильносвязным, если для любых $i,j\in V$ существует путь с меткой $w^{t_{ij}}$ из i в j при некотором $t_{ij}\in\mathbb{N}$. Из данного определения следует, что в w-сильносвязном мультиграфе $\Gamma^{(p)}$ есть контур с меткой w^{t_i} при некотором $t_i\in\mathbb{N}$ с началом обхода в вершине i, $i=1,\dots,n$. В частности, при $t_i=1$ мультиграф $\Gamma^{(p)}$ содержит контур с меткой w и, в соответствии с утверждением 4, $\Gamma(w)$ имеет петлю в вершине i.

В мультиграфе $\Gamma^{(p)}$ обозначим $V_w(i)$ — множество вершин, до которых существует путь с меткой w с началом в вершине $i\in V$.

Пример 1. На рис. 1 изображены множество графов $\hat{\Gamma}=\{\Gamma_1,\Gamma_2\}$ и $(1,2)$-сильносвязный мультиграф $\Gamma^{(2)}$, где $V_w(1)=\{3\}$, $V_w(2)=\{4,5\}$, $V_w(3)=\{1,2\}$, $V_w(4)=\{3\}$, $V_w(5)=\{4,5\}$.

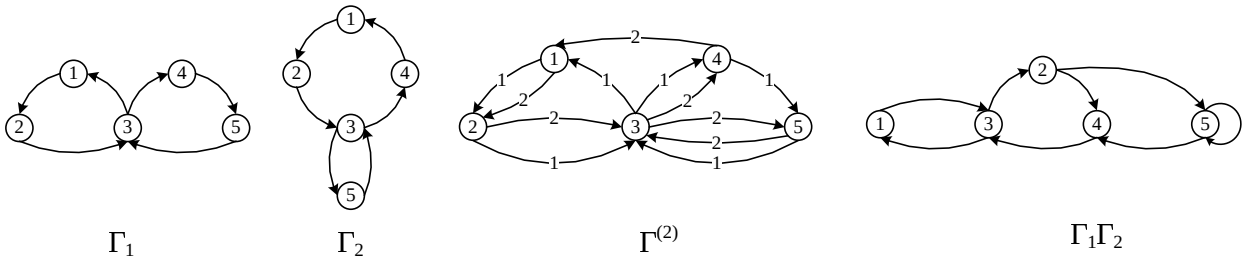

Рис. 1. Иллюстрация к примеру 1

Утверждение 5. В w-сильносвязном мультиграфе $\Gamma^{(p)}$:

а) $V_w(i)\neq\varnothing$ для любой вершины $i\in V$;

б) если $i\in V_w(i)$, то $|V_w(i)|>1$;

в) $\bigcup\limits_{i\in V} V_w(i)=V$.

Доказательство. В w-сильносвязном мультиграфе $\Gamma^{(p)}$ для любых вершин $i,j\in V$ существует путь с меткой $w^{t_{ij}}$ из вершины i в вершину j при некотором $t_{ij}\in\mathbb{N}$. Этот путь есть конкатенация t_{ij} путей с меткой w, первый из которых имеет начальную вершину i, а последний — конечную вершину j. Поскольку вершина i (вершина j) является начальной (конечной) вершиной пути с меткой $w^{t_{ij}}$, то она является

начальной (конечной) и для первого (последнего) пути в рассматриваемой конкатенации путей с меткой w. Следовательно, в w-сильносвязном орграфе $\Gamma^{(p)}$ любая вершина является начальной для некоторого пути с меткой w, а также любая вершина является конечной для некоторого пути с меткой w.

Если $V_w(i) = \varnothing$ для некоторой вершины $i \in V$, то в $\Gamma^{(p)}$ не существует пути с меткой w с началом в вершине i; если $V_w(i) = \{i\}$, то для любой вершины $j \neq i$ в $\Gamma^{(p)}$ не существует пути с меткой w с началом в вершине i; если $\bigcup\limits_{i \in V} V_w(i) = Q$ и $Q \subset V$, то вершины множества $V \backslash Q$ не являются конечными ни для одного из путей с меткой w; в каждом из трёх случаев имеем противоречие с w-сильной связностью мультиграфа $\Gamma^{(p)}$. ■

Обозначим $C(i)$ — контур (не обязательно простой) с началом обхода из вершины i. Выполнено необходимое условие w-сильной связности мультиграфа $\Gamma^{(p)}$.

Утверждение 6. Если мультиграф $\Gamma^{(p)}$ w-сильносвязный, то для любой его вершины i существует контур $C(i)$ с меткой w^{t_i}, проходящий через все вершины $\Gamma^{(p)}$.

Доказательство. В w-сильносвязном мультиграфе $\Gamma^{(p)}$ существуют пути $[1,2]$ с меткой $w^{t_{12}}$ и $[2,1]$ с меткой $w^{t_{21}}$, пути $[1,3]$ с меткой $w^{t_{13}}$ и $[3,1]$ с меткой $w^{t_{31}}$, …, пути $[1,n]$ с меткой $w^{t_{1n}}$ и $[n,1]$ с меткой $w^{t_{n1}}$. Конкатенация этих путей в названном порядке образует контур $C(1)$ с меткой w^{t_1}, где $t_1 = \sum\limits_{j=2}^{n} t_{1j} + t_{j1}$, проходящий через все вершины $\Gamma^{(p)}$. Аналогичным образом для вершин $i = 2, \ldots, n$ доказывается наличие в $\Gamma^{(p)}$ контура $C(i)$ с меткой w^{t_i}, где $t_i = \sum\limits_{j \in V \backslash \{i\}} t_{ij} + t_{ji}$, проходящего через все вершины $\Gamma^{(p)}$. ■

Замечание 2. Утверждение, обратное к утверждению 6, в общем случае неверно. Проиллюстрируем это на простейшем примере. Рассмотрим двухвершинный мультиграф $\Gamma^{(2)}$ с четырьмя дугами: $(1,2)$ с меткой 1, $(1,2)$ с меткой 2, $(2,1)$ с меткой 1 и $(2,1)$ с меткой 2. Пусть $w = (1,2)$. Тогда в мультиграфе есть контуры $C(1)$, $C(2)$ с меткой w, однако нет путей $[1,2]$ и $[2,1]$ с метками $w^{t_{12}}$ и $w^{t_{21}}$ соответственно ни при каких t_{12}, t_{21}. Следовательно, $\Gamma^{(2)}$ не является w-сильносвязным при $w = (1,2)$.

Справедлив следующий критерий примитивности орграфа $\Gamma(w)$.

Теорема 1. Орграф $\Gamma(w) = \Gamma_{w_1} \ldots \Gamma_{w_s}$, где $w = w_1 \ldots w_s$, примитивный, если и только если $\Gamma^{(p)}$ является w-сильносвязным и содержит контуры с метками $w^{t_1}, \ldots, w^{t_m}$, где $\text{НОД}(t_1, \ldots, t_m) = 1$.

Доказательство. Необходимость. Пусть орграф $\Gamma(w)$ примитивный и $\exp \Gamma(w) = t$, тогда любые две вершины в $\Gamma(w)$ соединены путём длины t и в $\Gamma(w)$ есть множество контуров длин $t_1, \ldots, t_m$, где $\text{НОД}(t_1, \ldots, t_m) = 1$, в частности петля. Из наличия в $\Gamma(w)$ пути длины t между любой парой вершин следует, что в орграфе $\Gamma^{(p)}$ для любых $i, j \in V$ есть путь с меткой w^t из вершины i в вершину j. Следовательно, $\Gamma^{(p)}$ w-сильносвязный.

По утверждению 4, при любом $l \in \mathbb{N}$ в мультиграфе $\Gamma^{(p)}$ есть контур с меткой w^l, если и только если в орграфе $\Gamma(w)$ есть контур длины l. Следовательно, в $\Gamma^{(p)}$ есть контуры с метками $w^{t_1}, \ldots, w^{t_m}$, где $\text{НОД}(t_1, \ldots, t_m) = 1$. В частности, если в $\Gamma(w)$ есть петля, то в $\Gamma^{(p)}$ есть контур с меткой w. В этом случае без ущерба для общности полагаем $t_1 = 1$ и тогда $\text{НОД}(1, t_2, \ldots, t_m) = 1$.

Достаточность. Пусть мультиграф $\Gamma^{(p)}$ w-сильносвязный, тогда в нём есть путь с меткой $w^{t_{ij}}$ из вершины i в вершину j для любых i, j. Отсюда следует, что $m_{ij}(w^{t_{ij}})$=1,

т. е. в орграфе $\Gamma(w^{t_{ij}})$ есть дуга (i,j). Следовательно, в $\Gamma(w)$ есть путь $[i,j]$ длины t_{ij} для любых вершин i,j. Значит, орграф $\Gamma(w)$ сильносвязный.

Пусть в $\Gamma^{(p)}$ имеются $m \geqslant 1$ контуров с метками $w^{t_1},\dots,w^{t_m}$. Тогда, по утверждению 4, в $\Gamma(w)$ есть контуры длины $t_1,\dots,t_m$. При НОД$(t_1,\dots,t_m)=1$ орграф $\Gamma(w)$ примитивный. ■

Следствие 1. Задача распознавания примитивности множества n-вершинных орграфов алгоритмически разрешима.

Доказательство. Покажем, что w-сильную связность мультиграфа $\Gamma^{(p)}$ достаточно проверить для конечного множества слов w.

Слова w и w' в алфавите N_p назовём эквивалентными (обозначается $w \cong w'$), если $\Gamma(w)=\Gamma(w')$. Пусть $|\Gamma(n)|=l$, тогда число классов эквивалентности не превышает l.

Докажем (от противного), что в каждом классе эквивалентности содержится слово длины не более l. Пусть в некотором классе эквивалентности K наименьшая длина содержащихся слов равна t, где $l<t$. Запишем такое слово $w=w_1\dots w_t$ и обозначим $w(\tau)=w_1\dots w_\tau$, $\tau=1,\dots,t$. Тогда при $l<t$ в последовательности $\Gamma(w(\tau))$, $\tau=1,\dots,t$, имеются одинаковые орграфы, то есть $\Gamma(w(\tau))=\Gamma(w(\theta))$, где $1\leqslant\tau<\theta\leqslant t$. Значит, $w(\tau)\cong w(\theta)$. Если $\theta=t$, то $w(\tau)\cong w(t)$, и если $\theta<t$, то $w(\tau)\cdot(w_{\theta+1}\dots w_t)\cong w(\theta)\cdot(w_{\theta+1}\dots w_t)$, где символ $\cdot$ обозначает конкатенацию слов. Так как $w(\theta)\cdot(w_{\theta+1}\dots w_t)=w(t)$, в любом случае получаем, что в K имеется слово длины меньше t, что противоречит условию. Следовательно, w-сильную связность мультиграфа $\Gamma^{(p)}$ достаточно проверить для всех слов w длины не более l, при этом для любого слова w задача равносильна распознаванию примитивности орграфа $\Gamma(w)$. ■

Пусть $\hat{C}=\{C_1,\dots,C_m\}$ — множество контуров длин $l_1,\dots,l_m$ соответственно в орграфе Γ. Если орграф $C_1\cup\dots\cup C_m$ связный, то он содержит контур Z, обходящий однократно каждый контур множества $\hat{C}$ и проходящий через каждую дугу столько раз, сколько контуров множества $\hat{C}$ содержат эту дугу [9, с. 79]. Контур Z называется квазиэйлеровым $\hat{C}$-контуром, его длина равна $l_1+\dots+l_m$.

Теорема 2. Пусть мультиграф $\Gamma^{(p)}$ w-сильносвязный, где $w=w_1\dots w_s$, и орграфы $\Gamma_1,\dots,\Gamma_p$ имеют общее множество контуров $\hat{C}=\{C_1,\dots,C_m\}$ длин $l_1,\dots,l_m$ соответственно, где $m\geqslant 1$, $l_1\leqslant\dots\leqslant l_m$. Тогда орграф $\Gamma_{w_1}\dots\Gamma_{w_s}$ примитивный при любом из условий:

а) $m=1$ и $l_1=1$;

б) НОД$(l_1,\dots,l_m)=s$;

в) орграф $C_1\cup\dots\cup C_m$ связный и содержит квазиэйлеров $\hat{C}$-контур длины s.

Доказательство. В соответствии с теоремой 1, достаточно доказать, что в $\Gamma^{(p)}$ имеются контуры с метками $w^{t_1},\dots,w^{t_m}$, где НОД$(t_1,\dots,t_m)=1$, в частности, при $m=1$ — контур с меткой w.

а) Если $m=1$ и $l_1=1$, то в вершине $u\in V$ имеется петля как в орграфах $\Gamma_1,\dots,\Gamma_p$, так и в $\Gamma^{(p)}$ (с любой из меток $1,\dots,p$). Следовательно, в $\Gamma^{(p)}$ конкатенация s петель в вершине u с метками $w_1,\dots,w_s$ образует контур с меткой w.

б) При НОД$(l_1,\dots,l_m)=s$ длины контуров $C_1,\dots,C_m$ можно представить в виде $l_1=st_1$, $l_2=st_2$, …, $l_m=st_m$, где $t_1,\dots,t_m\in\mathbb{N}$ и НОД$(t_1,\dots,t_m)=1$. Контуры $C_1,\dots,C_m$ есть в каждом из графов $\Gamma_1,\dots,\Gamma_p$, следовательно, в $\Gamma^{(p)}$ есть контуры длин $l_1,\dots,l_m$ с любыми метками, в том числе с метками $w^{t_1},\dots,w^{t_m}$, $w=w_1\dots w_s$.

в) Квазиэйлеров контур $\hat{C}$-контур длины s есть в каждом из графов $\Gamma_1, \ldots, \Gamma_p$, следовательно, в $\Gamma^{(p)}$ есть контур с любой меткой длины s, в том числе с меткой w. Без ущерба для общности положим $t_1 = 1$. Следовательно, НОД$(1, t_2, \ldots, t_m) = 1$. ■

3. Оценки экспонентов некоторых множеств орграфов

Исследуем примитивность частного класса множеств орграфов и определим минимальное подмножество, на котором достигается оценка экспонента. Используем универсальный критерий примитивности орграфа [1]: орграф Γ примитивный, если и только если Γ сильносвязный и длины его простых контуров взаимно простые.

В дальнейшем потребуется следующее утверждение.

Утверждение 7. Пусть n-вершинный орграф Γ содержит гамильтонов контур $(0, \ldots, n-1)$ и множество дуг $E = \{(i, (i+l) \bmod n) : i = 0, \ldots, n-1\}$, $n \geqslant l > 1$. Тогда орграф Γ примитивный, если НОД$(n, l-1) = 1$, и $\exp \Gamma = n - 1$.

Доказательство. В данных условиях в сильносвязном орграфе Γ через каждую вершину проходит контур длины $(n-l+1)$. Так как НОД$(n, l-1) =$ НОД$(n, n-l+1) = 1$, орграф Γ примитивный согласно универсальному критерию.

В орграфе Γ при любых $i, k = 0, \ldots, n-1$ путь длины t из вершины i в вершину $j = (i + k) \bmod n$ состоит из x_k дуг множества E и $(t - x_k)$ дуг контура $(0, \ldots, n-1)$, где $t \geqslant x_k$. Следовательно, выполнена система сравнений

$$i + x_k l + t - x_k \equiv i + k \pmod{n}, \;\; k = 0, \ldots, n-1.$$

После элементарных преобразований данная система принимает вид

$$(l-1)x_k \equiv k - t \pmod{n}, \;\; k = 0, \ldots, n-1. \tag{2}$$

Все сравнения системы (2) при любых фиксированных k, t имеют единственное решение относительно x_k, так как НОД$(n, l-1) = 1$. Значит, при $k = 0, \ldots, n-1$ величина x_k принимает все значения от 0 до $n-1$. Длина t пути одинакова при любых $i, k = 0, \ldots, n-1$ и $t \geqslant x_k$. Следовательно, в орграфе Γ есть путь длины t из любой вершины в любую при всех $t \geqslant n-1$, отсюда $\exp \Gamma \leqslant n-1$.

Докажем (от противного), что для пар вершин $(i, (i+k) \bmod n)$, $i = 0, \ldots, n-1$, отсутствует путь длины $(n-2)$ при $k = ((n-1)(l-1)-2) \bmod n$. Действительно, если в Γ есть путь длины $t = n-2$ при указанном k, то сравнение (2) принимает вид

$$(l-1)x_k \equiv (n-1)(l-1) \pmod{n}.$$

Данное сравнение имеет единственное решение $x_k \equiv (n-1) \bmod n$, что противоречит условию $x_k \leqslant t = n-2$. Следовательно, $\exp \Gamma \geqslant n-1$. Объединяя оценки, получаем $\exp \Gamma = n-1$. ■

Следствие 2 (при $l = n$). Если орграф Γ имеет петли во всех вершинах гамильтонова контура, то $\exp \Gamma = n-1$.

Докажем критерий примитивности множества орграфов, обобщающего множество орграфов Виландта, и оценим его экспонент.

Теорема 3. Пусть $\hat{\Gamma} = \{\Gamma_0, \ldots, \Gamma_{n-1}\}$ — множество орграфов с вершинами $0, \ldots, n-1$, где орграф Γ_i имеет гамильтонов контур $(0, \ldots, n-1)$ и дугу $(i, (i+l) \bmod n)$, $n \geqslant l > 1$, $i = 0, \ldots, n-1$. Тогда множество орграфов $\hat{\Gamma}$ примитивное, если и только если НОД$(n, l-1) = 1$, при этом

$$n - 1 \leqslant \exp \hat{\Gamma} \leqslant 2n - 2.$$

Доказательство. Необходимость. Пусть множество орграфов $\hat{\Gamma}$ примитивное. Тогда некоторое слово $\Gamma = \Gamma_{w_1} \dots \Gamma_{w_t}$ длины $t > 0$ в алфавите $\hat{\Gamma}$ является полным графом, то есть любая пара вершин в орграфе Γ есть дуга. В силу правила умножения графов это означает, что в мультиграфе $\Gamma^{(p)}$ для любых $i, k \in \{0, \dots, n-1\}$ имеется путь $[i, (i+k) \bmod n] = (i_{w_0}, i_{w_1}, \dots, i_{w_t})$ длины t, где $i_{w_0} = i$, $i_{w_t} = (i+k) \bmod n$ и $i_{w_s} = (i_{w_{s-1}} + \xi_s^{(i,k)}) \bmod n$, $\xi_s^{(i,k)} \in \{1, l\}$, $s = 1, \dots, t$. Обозначим через $x^{(i,k)}$ частоту символа l в слове $(\xi_1^{(i,k)}, \dots, \xi_t^{(i,k)})$, тогда $(t - x^{(i,k)})$ есть частота символа 1 в том же слове. Из существования пути $(i_{w_0}, i_{w_1}, \dots, i_{w_t})$ длины t при любых $i, k \in \{0, \dots, n-1\}$ следует, что выполнена система сравнений

$$i + lx^{(i,k)} + t - x^{(i,k)} \equiv i + k \pmod{n}, \;\; k = 0, \dots, n-1.$$

После элементарных преобразований данная система принимает вид

$$(l-1)x^{(i,k)} \equiv k - t \pmod{n}, \;\; k = 0, \dots, n-1. \tag{3}$$

По построению каждое сравнение системы (3) при фиксированном t имеет решение относительно $x^{(i,k)}$, что возможно только при условии НОД$(n, l-1) = 1$.

Достаточность. При НОД$(n, l-1) = 1$ орграфы $\Gamma_0, \dots, \Gamma_{n-1}$ примитивные, так как каждый из них сильносвязный и содержит контуры длины n и $(n-l+1)$, где НОД$(n, n-l+1) = 1$. Следовательно, множество $\hat{\Gamma}$ примитивное. Для получения оценок экспонента множества $\hat{\Gamma}$ докажем промежуточную лемму.

Для $a \in \mathbb{N}$ и $Y \subset \mathbb{N}$ положим $(a \pm Y) \bmod n = \{(a \pm y) \bmod n : y \in Y\}$. Обозначим S_r, $r = 1, 2, \dots$, последовательность множеств чисел, где $S_1 = \{1, l\}$, $S_r = (1 + S_{r-1}) \bmod n \cup \cup \{(rl) \bmod n\}$, $r > 1$.

Лемма 1. При НОД$(n, l-1) = 1$ множество S_r содержит полную систему вычетов по модулю n, если и только если $r \geqslant n-1$.

Доказательство. Число a принадлежит S_r, если и только если $a = xl + (r - x)$, где $x \in \{0, \dots, r\}$. Следовательно, S_r содержит полную систему вычетов по модулю n, если и только если в множестве $\{0, \dots, r\}$ имеется решение (относительно x) каждого сравнения системы

$$xl + r - x \equiv a \pmod{n}, \quad a = 0, \dots, n-1.$$

После элементарных преобразований получаем, что указанная система сравнений равносильна следующей:

$$\{x(l-1) \equiv a - r \pmod{n}, \quad a = 0, \dots, n-1,$$

где функция $x(l-1) \bmod n$ при НОД$(n, l-1) = 1$ реализует подстановку множества $\{0, \dots, n-1\}$. Значит, каждое сравнение исходной системы имеет решение в множестве $\{0, \dots, r\}$, если и только если $r \geqslant n-1$. Лемма доказана. ■

Построим слово длины $(2n-2)$ в алфавите $\hat{\Gamma}$, которому при умножении соответствует полный орграф.

Обозначим $G_{r,1} = \Gamma_{(n-lr) \bmod n} \cdot \ldots \cdot \Gamma_{(n-l) \bmod n}$, $r = 1, \dots, n-1$. Покажем (индукция по r), что в орграфе $G_{r,1}$ есть дуги $(j, 0)$ для любого $j \in (n - S_r) \bmod n$.

При $r = 1$ выполнено: $S_1 = \{1, l\}$, $G_{1,1} = \Gamma_{n-l}$. Орграф Γ_{n-l} имеет дуги $(n-1, 0)$ и $(n-l, 0)$ по определению, то есть при $r = 1$ утверждение верно.

Пусть утверждение доказано для $r = 1, \ldots, \tau - 1$, где $1 < \tau \leqslant n - 1$, докажем его для $r = \tau$.

По предположению индукции, для любого $j \in (n - S_{\tau-1}) \bmod n$ в орграфе $G_{\tau-1,1}$ есть дуга $(j, 0)$. По условию $G_{\tau,1} = \Gamma_{(n-l\tau) \bmod n} \cdot G_{\tau-1,1}$, где орграф $\Gamma_{(n-l\tau) \bmod n}$ имеет гамильтонов контур $(0, \ldots, n-1)$ и дугу $((n - l\tau) \bmod n, (n - l(\tau - 1)) \bmod n)$. Тогда, в соответствии с правилом умножения орграфов, орграф $G_{\tau,1}$ имеет дуги $(j, 0)$ для любого $j \in (n - S_{\tau-1} - 1) \bmod n$, а также дугу $((n - l\tau) \bmod n, 0)$. По определению $S_\tau = (1 + S_{\tau-1}) \bmod n \cup \{(\tau l) \bmod n\}$, следовательно, орграф $G_{\tau,1}$ имеет дуги $(j, 0)$ для любого $j \in (n - S_\tau) \bmod n$.

По лемме 1 множество S_{n-1} содержит полную систему вычетов по модулю n. Следовательно, в орграфе $G_{n-1,1}$ есть дуги $(j, 0)$ при $j = 0, \ldots, n - 1$.

Обозначим $G_{0,r} = \Gamma_{0 \bmod n} \cdot \ldots \cdot \Gamma_{lr \bmod n}$, $r = 0, \ldots, n - 2$. Покажем (индукция по r), что в орграфе $G_{0,r}$ есть дуги $(0, j)$ для любого $j \in S_{r+1}$.

При $r = 0$ выполнено: $S_1 = \{1, l\}$, $G_{0,0} = \Gamma_0$. Орграф Γ_0 имеет дуги $(0, 1)$ и $(0, l)$ по определению, то есть при $r = 0$ утверждение верно.

Пусть утверждение доказано для $r = 0, \ldots, \tau - 1$, где $0 < \tau \leqslant n - 2$, докажем его для $r = \tau$.

По предположению индукции, для любого $j \in S_\tau$ в орграфе $G_{0,\tau-1}$ есть дуга $(0, j)$. По условию $G_{0,\tau} = G_{0,\tau-1} \cdot \Gamma_{l\tau \bmod n}$, где орграф $\Gamma_{l\tau \bmod n}$ имеет гамильтонов контур $(0, \ldots, n-1)$ и дугу $(l\tau \bmod n, (\tau + 1)l \bmod n)$. Тогда, в соответствии с правилом умножения орграфов, орграф $G_{0,\tau}$ имеет дуги $(0, j)$ для любого $j \in (S_\tau + 1) \bmod n$, а также дугу $(0, (\tau+1)l \bmod n)$. По определению $S_{\tau+1} = (1 + S_\tau) \bmod n \cup \{(\tau+1)l \bmod n\}$, значит, орграф $G_{0,\tau}$ имеет дуги $(0, j)$ для любого $j \in S_{\tau+1}$.

По лемме 1 множество S_{n-1} содержит полную систему вычетов по модулю n. Следовательно, в орграфе $G_{0,n-2}$ есть дуги $(0, j)$ при $j = 0, \ldots, n - 1$.

В соответствии с правилом умножения орграфов, в произведении $\Gamma = G_{n-1,1} \cdot G_{0,n-2}$ есть дуги из любой вершины в любую, т. е. орграф Γ полный и $\exp \Gamma \leqslant 2n - 2$.

Для получения нижней оценки экспонента множества рассмотрим орграф $\Gamma^{(n)} = \Gamma_0 \cup \ldots \cup \Gamma_{n-1}$. Если множество $\hat{\Gamma}$ примитивное, то орграф $\Gamma^{(n)}$ также примитивный [5, с. 188] и $\exp \hat{\Gamma} \geqslant \exp \Gamma^{(n)}$. По утверждению 7 $\exp \Gamma^{(n)} = n - 1$. Теорема 3 доказана. ■

Замечание 3. При $l = 2$ имеем множество графов Виландта. Тогда $\exp \Gamma_0 = \ldots = \exp \Gamma_{n-1} = n^2 - 2n + 2$, вместе с тем $\exp \hat{\Gamma} \leqslant 2n - 2$.

Замечание 4. При $l = n$ орграф Γ_i содержит гамильтонов контур и петлю в вершине i, тогда $\exp \hat{\Gamma} = \exp \Gamma_i = 2n - 2$, $i = 0, \ldots, n - 1$.

Замечание 5. Полугруппа $\langle \hat{\Gamma} \rangle$ содержит не менее n положительных слов длины $(2n - 2)$, а именно содержит слова $G^{(k)}_{n-1,1} \cdot G^{(k)}_{0,n-2}$ при $k = 0, \ldots, n - 1$, где $G^{(k)}_{n-1,1} = \Gamma_{(k-l(n-1)) \bmod n} \cdot \ldots \cdot \Gamma_{(k-l) \bmod n}$, $G^{(k)}_{0,n-2} = \Gamma_{k \bmod n} \cdot \ldots \cdot \Gamma_{(k+l(n-2)) \bmod n}$. Доказательство проводится аналогично.

Следствие 3. Минимальное примитивное подмножество множества орграфов $\hat{\Gamma} = \{\Gamma_0, \ldots, \Gamma_{n-1}\}$, на котором достигается верхняя оценка теоремы 3, является сокращённым и содержит не более n/d орграфов, где $d = \text{НОД}(n, l)$.

Доказательство. Множество $\{(n - lr) \bmod n : r = 1, \ldots, n - 1\} \cup \{lr \bmod n : r = 0, \ldots, n - 2\} = \{lr \bmod n : r = 0, \ldots, n - 1\}$ содержит n/d различных вычетов по модулю n, где $d = \text{НОД}(n, l)$. Следовательно, в произведении $\Gamma = G_{n-1,1} \cdot G_{0,n-2}$ записаны n/d различных орграфов.

Множество орграфов $\hat{\Gamma}$ сокращённое, так как ни один орграф из $\Gamma_0, \ldots, \Gamma_{n-1}$ не является частью другого орграфа. ■

Пример 2. Пусть $n = 4$, $\hat{\Gamma} = \{\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3\}$. При $l = 2$ НОД$(n, n - l + 1) =$ $=$ НОД$(4, 3) = 1$ (множество графов Виландта). Орграф Γ_0 содержит дугу $(0, 2)$, Γ_1 содержит дугу $(1, 3)$ и т. д. Тогда $G_{3,1} = \Gamma_2\Gamma_0\Gamma_2$, $G_{0,2} = \Gamma_0\Gamma_2\Gamma_0$. Орграф $G_{3,1}$ имеет дуги $(0, 0)$, $(1, 0)$, $(2, 0)$, $(3, 0)$; орграф $G_{0,2}$ имеет дуги $(0, 0)$, $(0, 1)$, $(0, 2)$, $(0, 3)$. Тогда $G_{3,1} \cdot G_{0,2}$ полный и $\exp\hat{\Gamma} \leqslant 6$.

Пример 3. Пусть $n = 5$, $\hat{\Gamma} = \{\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4\}$. При $l = 3$ НОД$(n, n - l + 1) =$ $=$ НОД$(5, 3) = 1$. Орграф Γ_0 содержит дугу $(0, 3)$, Γ_1 содержит дугу $(1, 4)$ и т. д. Тогда $G_{4,1} = \Gamma_3\Gamma_1\Gamma_4\Gamma_2$, $G_{0,3} = \Gamma_0\Gamma_3\Gamma_1\Gamma_4$. Орграф $G_{4,1}$ имеет дуги $(0, 0)$, $(1, 0)$, $(2, 0)$, $(3, 0)$, $(4, 0)$; орграф $G_{0,3}$ имеет дуги $(0, 0)$, $(0, 1)$, $(0, 2)$, $(0, 3)$, $(0, 4)$. Тогда $G_{4,1} \cdot G_{0,3}$ полный и $\exp\hat{\Gamma} \leqslant 8$.

Выводы

1) Показано, что исследование примитивности данного множества неотрицательных матриц (орграфов) может быть сведено к исследованию примитивности подмножества. Задача минимизации нетривиальна для множеств, состоящих из непримитивных матриц (орграфов).
2) Получен универсальный критерий примитивности множества $\hat{M}$ неотрицательных матриц (множества $\hat{\Gamma}$ орграфов). В силу конечности полугруппы $\langle\hat{M}\rangle$ (полугруппы $\langle\hat{\Gamma}\rangle$) при фиксированном n задача распознавания примитивности множества матриц $\hat{M}$ (орграфов $\hat{\Gamma}$) алгоритмически разрешима. Актуальной задачей является построение соответствующего алгоритма и оценка его вычислительной сложности.
3) Показано, что критерий примитивности множества перемешивающих орграфов может быть упрощен для частных классов, в том числе для классов, важных с прикладной точки зрения.
4) На примере некоторых множеств примитивных орграфов показано, что экспонент множества может быть существенно меньше экспонента любого орграфа из данного множества.

ЛИТЕРАТУРА

1. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
2. *Князев А. В.* Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: дис. ... д-ра физ.-мат. наук. М., 2002. 203 с.
3. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
4. *Авезова Я. Э., Фомичев В. М.* Комбинаторные свойства систем разноразмерных 0, 1-матриц // Прикладная дискретная математика. 2014. № 2(24). С. 5–11.
5. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: Изд-во Юрайт, 2016. 209 с.
6. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
7. *Берж К.* Теория графов и её применение. М.: ИЛ, 1962. 320 с.
8. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1. С. 97–119.

9. *Фомичев В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.

REFERENCES

1. *Sachkov V. N. and Tarakanov V. E.* Kombinatorika neotritsatel'nykh matrits [Combinatorics of Non-Negative Matrices]. Moscow, TVP Publ., 2000, 448 p. (in Russian)
2. *Knyazev A. V.* Otsenki ekstremal'nykh znacheniy osnovnykh metricheskikh kharakteristik psevdosimmetricheskikh grafov [Estimates for the Extreme Values of the Basic Metric Characteristics of Pseudosymmetric Graphs]. Doctor of Physics and Mathematics Thesis, Moscow, 2002, 203 p. (in Russian)
3. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MEPhI Publ., 2010, 424 p. (in Russian)
4. *Avezova Ya. E. and Fomichev V. M.* Kombinatornye svoystva sistem raznorazmernykh 0, 1-matrits [Combinatorial properties of rectangular 0,1-matrix systems]. Prikladnaya Diskretnaya Matematika, 2014, no. 2(24), pp. 5–11. (in Russian)
5. *Fomichev V. M. and Mel'nikov D. A.* Kriptograficheskie metody zashchity informatsii. Ch. 1. Matematicheskie aspekty [Cryptographic Methods of Information Security. Part 1. Mathematical Aspects]. Moscow, Yurayt Publ., 2016, 209 p. (in Russian)
6. *Kyazhin S. N. and Fomichev V. M.* Lokal'naya primitivnost' grafov i neotritsatel'nykh matrits [Local primitiveness of graphs and nonnegative matrices]. Prikladnaya Diskretnaya Matematika, 2014, no. 3(25), pp. 68–80. (in Russian)
7. *Berzh K.* Teoriya grafov i ee primenenie [Graph Theory and its Application.]. Moscow, Foreign Literature Publ., 1962, 320 p. (in Russian)
8. *Fomichev V. M. and Kyazhin S. N.* Lokal'naya primitivnost' matrits i grafov [Local primitiveness of matrices and graphs]. Diskretn. Anal. Issled. Oper., 2017, vol. 24, no. 1, pp. 97–119. (in Russian)
9. *Fomichev V. M.* Novaya universal'naya otsenka eksponentov grafov [The new universal estimation for exponents of graphs]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 78–84. (in Russian)