

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.17

СВОЙСТВА ПРИМИТИВНЫХ МНОЖЕСТВ ОРИЕНТИРОВАННЫХ ГРАФОВ С ОБЩИМ МНОЖЕСТВОМ КОНТУРОВ

Я. Э. Авезова

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

Получены критерий примитивности и оценки экспонентов множеств орграфов с общим множеством простых контуров. Критерий примитивности позволил получить формулу для числа примитивных множеств n -вершинных орграфов с общим гамильтоновым контуром.

Ключевые слова: гамильтонов орграф, примитивное множество орграфов, экспонент множества орграфов.

DOI 10.17223/20710410/43/7

ON PROPERTIES OF PRIMITIVE SETS OF DIGRAPHS WITH COMMON CYCLES

Y. E. Avezova

National Research Nuclear University Moscow Engineering Physics Institute, Moscow, Russia

E-mail: avezovayana@gmail.com

Let $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$ be a set of digraphs with vertex set V , $p > 1$, and $U^{(p)}$ be the union of digraphs $\Gamma_1 \cup \dots \cup \Gamma_p$ with no multiple arcs. The smallest number such that the union of μ digraphs of the set $\hat{\Gamma}$ contains all arcs of $U^{(p)}$ is denoted by μ . Suppose $\hat{C} = \{C_1, \dots, C_m\}$ is a set of elementary cycles. This set is called common for $\hat{\Gamma}$ if every digraph of the set $\hat{\Gamma}$ contains all cycles of the set $\hat{C}$. Assume that $C_1^* \cup \dots \cup C_m^* = V$ where C_i^* denotes the vertex set of C_i , $i = 1, \dots, m$. For a given digraph Γ , the loop-character index in the semigroup $\langle \Gamma \rangle$ is the smallest integer h for which there is a loop on every vertex of Γ^h . In this paper, we study conditions for the set of digraphs with common cycles to be primitive. For $m \geq 1$, the set $\hat{\Gamma}$ with common cycles set $\hat{C}$ is primitive if and only if the digraph $U^{(p)}$ is primitive. If $\hat{\Gamma}$ is primitive, then $\exp \hat{\Gamma} \leq ((\mu - 1)h + 1) \exp U^{(p)}$, where h is the loop-character index in the semigroup $\langle \Gamma(\hat{C}) \rangle$, $\Gamma(\hat{C}) = C_1 \cup \dots \cup C_m$. For $m = 1$, we establish an improved bound on the exponent. Let all digraphs of the primitive set $\hat{\Gamma}$ have a common Hamiltonian cycle, then $\exp \hat{\Gamma} \leq (2n - 1)\mu + \sum_{\tau=1}^{\mu} (F(l_1^\tau, \dots, l_{m(\tau)}^\tau) + d_\tau - l_1^\tau)$, where $l_1^\tau, \dots, l_{m(\tau)}^\tau$ are all cycle lengths in Γ_τ , ordered so that $l_1^\tau < \dots < l_{m(\tau)}^\tau = n$, $d_\tau = \gcd(l_1^\tau, \dots, l_{m(\tau)}^\tau)$, $F(l_1^\tau, \dots, l_{m(\tau)}^\tau) = d_\tau \Phi(l_1^\tau/d_\tau, \dots, l_{m(\tau)}^\tau/d_\tau)$, $\Phi(l_1^\tau/d_\tau, \dots, l_{m(\tau)}^\tau/d_\tau)$ denotes the Frobenius number, $\tau = 1, \dots, \mu$. Finally, if $n = q^\alpha$, q is prime, $\alpha \in \mathbb{N}$, $m = n^2$, then the number of primitive sets of n -vertex digraphs with a common Hamiltonian cycle equals $2^\sigma - 2^\varepsilon$, where $\sigma = 2^{m-n}$, $\varepsilon = 2^{m/q-n}$.

Keywords: Hamiltonian digraph, primitive set of digraphs, exponent of digraphs set.

Введение

Введем основные обозначения:

- $\mathbb{N}$ — множество натуральных чисел;
- $\mathbb{N}_p = \{1, \dots, p\}$, $p \in \mathbb{N}$;
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$;
- $0, 1$ -матрица — матрица с элементами из множества $\{0, 1\}$;
- $M = (m_{i,j})$ — матрица смежности вершин орграфа;
- $M^t = (m_{i,j}^{(t)})$, $t \in \mathbb{N}$;
- $M > 0$ ($M \geq 0$) — все элементы матрицы M над полем действительных чисел неотрицательны (положительны);
- $\langle X \rangle$ — подполугруппа, порожденная подмножеством X мультипликативной полугруппы;
- $\|M\|$ — вес $0, 1$ -матрицы M , равный числу единичных элементов матрицы;
- M^T — транспонированная матрица M ;
- $\text{НОД}(a_1, \dots, a_n)$ — наибольший общий делитель натуральных чисел $a_1, \dots, a_n$;
- (i, j) — дуга в орграфе Γ , инцидентная вершинам i и j ;
- $[i, j]$ — путь в орграфе Γ из вершины i в вершину j ;
- $\text{len}[i, j]$ — длина пути $[i, j]$ в орграфе.

Важными характеристиками преобразования векторного пространства являются множества существенных переменных его координатных функций. Преобразование называется совершенным, если каждая координатная функция существенно зависит от всех переменных. Совершенство является одним из положительных свойств преобразований, применяемых в системах защиты информации. Часто совершенство преобразования обозначают как свойство полного перемешивания входных данных. В системах защиты информации полное перемешивание входных данных делает систему устойчивой к атакам типа последовательного опробования частей секретного параметра.

Существуют два равносильных подхода к оценке перемешивающих свойств преобразования: матричный и теоретико-графовый. Суть обоих подходов описана в [1, 2]. Полное перемешивание входных данных, как правило, осуществляется композицией несовершенных преобразований, допускающих несложную реализацию. Матрично-графовый подход позволяет оценить длину такой композиции. Основными задачами при этом являются распознавание примитивности неотрицательной матрицы и оценка её экспонента [3, 4]. Матрица M называется примитивной тогда и только тогда, когда существует $\gamma \in \mathbb{N}$, такое, что для любого $t \geq \gamma$ выполняется $M^t > 0$. Наименьшее $\gamma \in \mathbb{N}$, при котором $M^\gamma > 0$, называется экспонентом матрицы M , обозначается $\text{exp } M$. Исследование примитивности для неотрицательных матриц и $0, 1$ -матриц равносильно. Умножение $0, 1$ -матриц определено как умножение матриц над множеством целых неотрицательных чисел с последующей заменой в произведении всех положительных элементов единицами. Сложение выполняется аналогично. Мультипликативный моноид всех $0, 1$ -матриц порядка n обозначим $M_n^{0,1}$.

Свойство примитивности исследуется с использованием следующей теоремы теории графов [5]: если M — матрица смежности вершин графа Γ и $M^t = (m_{i,j}^{(t)})$, то число путей длины t из i в j в графе Γ равно $m_{i,j}^{(t)}$, $i, j \in \{1, \dots, n\}$. Известен критерий примитивности орграфа [6]: сильносвязный орграф примитивный, если и только если длины всех простых контуров орграфа взаимно простые.

Многообразие возникающих постановок задач в различных областях науки привели к обобщениям понятия примитивности неотрицательных матриц. В частности, введены определения примитивности множества матриц [1, 7–9]. В настоящей работе в соответствии с [1] множество матриц $\hat{M} \subseteq M_n^{0,1}$ называется примитивным, если порождённая множеством $\hat{M}$ мультипликативная полугруппа $\langle \hat{M} \rangle$ содержит положительную матрицу. Наименьшая длина слова из $\langle \hat{M} \rangle$, соответствующего положительной матрице, называется экспонентом множества $\hat{M}$ и обозначается $\text{exp } \hat{M}$. Дадим равносильное определение примитивности множества на теоретико-графовом языке. Обозначим $\Gamma(n)$ множество всех орграфов с множеством вершин $V = \{0, \dots, n-1\}$. Умножение орграфов из $\Gamma(n)$ определяется как умножение бинарных отношений. Множество $\hat{\Gamma} \subseteq \Gamma(n)$ называется примитивным, если порождённая множеством $\hat{\Gamma}$ мультипликативная полугруппа $\langle \hat{\Gamma} \rangle$ содержит полный орграф. Наименьшая длина слова из $\langle \hat{\Gamma} \rangle$, соответствующего полному орграфу, называется экспонентом множества $\hat{\Gamma}$ и обозначается $\text{exp } \hat{\Gamma}$. Если положительной матрицы в алфавите $\hat{M}$ (полного орграфа в алфавите $\hat{\Gamma}$) не существует, то $\text{exp } \hat{M} = \infty$ ($\text{exp } \hat{\Gamma} = \infty$).

Универсальный критерий примитивности множества орграфов формулируется весьма сложно как на матричном, так и на теоретико-графовом языках, и распознавание его выполнимости предполагает проверку ряда условий для множества орграфов. В связи с этим актуальна задача поиска множеств орграфов, важных с прикладной точки зрения, для которых критерий примитивности существенно упрощается.

В множестве орграфов $\hat{\Gamma}$ простой контур назовем общим, если он имеется в любом орграфе этого множества. Множество орграфов $\hat{\Gamma}$ имеет общее множество контуров $\hat{C}$, если каждый орграф множества $\hat{\Gamma}$ содержит все контуры множества $\hat{C}$. Настоящая работа посвящена исследованию примитивности множеств орграфов с общим множеством контуров и логически продолжает работы [10–12], обобщая некоторые полученные в них результаты.

1. Комбинаторные свойства множества примитивных матриц (орграфов)

Если множество $\hat{M}$ содержит примитивную матрицу, то оно примитивное. В наиболее интересном для исследования примитивности случае множество $\hat{M}$ состоит из непримитивных матриц.

Известно необходимое условие примитивности множества матриц [2, теорема 11.8]: если множество $\hat{M} = \{M_1, \dots, M_p\}$, $p > 1$, примитивное, то матрица $M = M_1 + \dots + M_p$ примитивная и $\text{exp } \hat{M} \geq \text{exp } M$. Существуют непримитивные матрицы веса $n^2 - n + 1$, такие матрицы при $k = 1, \dots, n$ образуют множество H_k , определяемое правилом: $M = (m_{i,j}) \in H_k \Leftrightarrow m_{k,j} = 0$ при всех $j \in \{1, \dots, n\} \setminus \{k\}$, остальные элементы равны 1. Непримитивной является также матрица веса $n^2 - n + 1$, транспонированная к любой матрице из H_k , $k = 1, \dots, n$. Любая матрица, вес которой превышает $n^2 - n + 1$, является примитивной [13].

На множестве $M_n^{0,1}$ введём частичный порядок: $M \leq M' \Leftrightarrow m_{i,j} \leq m'_{i,j}$ для всех $i, j = 1, \dots, n$. Если M, M' — матрицы смежности орграфов Γ, Γ' соответственно и $M \leq M'$, то все дуги орграфа Γ являются дугами орграфа Γ' , т. е. Γ — часть орграфа Γ' (обозначается $\Gamma \leq \Gamma'$).

Непримитивное множество матриц $\hat{M}$ назовем максимальным непримитивным, если при объединении с любой матрицей $B \in M_n^{0,1} \setminus \hat{M}$ множество $\hat{M} \cup \{B\}$ является примитивным. Актуальной является задача описания всех максимально непримитивных множеств и оценка их мощностей. Опишем одно из таких множеств.

Теорема 1. Пусть M — непримитивная 0,1-матрица веса $n^2 - n + 1$, $\hat{M} = \{M_1, \dots, M_p\}$ — множество матриц со свойством $M_\tau \leq M$, $\tau = 1, \dots, p$, где $p = 2^{m-n+1}$, $m = n^2$. Тогда $\hat{M}$ — максимальное непримитивное множество.

Доказательство. Пусть $M = (m_{i,j})$, где, не ограничивая общности, положим, что $m_{1,j} = 0$ при $j = 2, \dots, n$, остальные элементы матрицы положительны. Заметим, что $M = M_1 + \dots + M_p$. В силу [2, теорема 11.8] из непримитивности матрицы M следует, что множество $\hat{M}$ также непримитивное. Покажем, что множество $\hat{M}$ максимальное непримитивное. Добавим к множеству $\hat{M}$ матрицу $B = (b_{i,j})$, $B \in M_n^{0,1} \setminus \hat{M}$, тогда $b_{1,k} > 0$ при некотором $k \in \{2, \dots, n\}$. Следовательно, $\|M'\| > m - n + 1$, где $M' = M_1 + \dots + M_p + B$, и матрица M' примитивная.

Покажем, что множество $\hat{M}' = \{M_1, \dots, M_p, B\}$ примитивное, построив положительное слово в алфавите $\hat{M}'$. Обозначим: $C = M \cdot B$, $C' = C \cdot M$, $C = (c_{i,j})$, $C' = (c'_{i,j})$. В силу правила произведения матриц, $c_{i,j} = m_{i,1}b_{1,j} + \dots + m_{i,n}b_{n,j}$, откуда следует, что $c_{i,k} > 0$ при $i = 1, \dots, n$. Тогда $c'_{i,j} = c_{i,1}m_{1,j} + \dots + c_{i,n}m_{n,j} > 0$ при всех $i, j = 1, \dots, n$. Таким образом, произведение $C' = M \cdot B \cdot M$ является положительной матрицей в алфавите $\hat{M}'$. Следовательно, множество $\hat{M}'$ примитивное. Отсюда $\hat{M}$ — максимальное непримитивное множество. ■

Далее обозначим: $m = n^2$, $\sigma(n) = |M_n^{0,1}| = 2^m$ — число всех 0,1-матриц порядка n ; $\pi(n)$ — число примитивных 0,1-матриц порядка n ; $\beta(n)$ — число примитивных множеств, состоящих только из непримитивных 0,1-матриц порядка n ; $\eta(n)$ — число всех примитивных множеств 0,1-матриц порядка n . Установим формулу для $\eta(n)$, которая далее используется при доказательстве одного из основных результатов.

Теорема 2. $\eta(n) = 2^{\sigma(n)} - 2^{\sigma(n) - \pi(n)} + \beta(n)$.

Доказательство. Множество матриц, содержащее хотя бы одну примитивную матрицу, примитивное. Число непустых множеств, состоящих только из примитивных матриц, равно $\eta_1(n) = 2^{\pi(n)} - 1$. Число непримитивных матриц равно $\sigma(n) - \pi(n)$, тогда число множеств непримитивных матриц равно $\eta_0(n) = 2^{\sigma(n) - \pi(n)}$. Объединяя каждое непустое множество примитивных матриц с каждым множеством непримитивных матриц, получим $\eta_1(n)\eta_0(n)$ примитивных множеств, в которых есть примитивные и, возможно, непримитивные матрицы. Тогда общее число примитивных множеств $\eta(n) = \eta_1(n)\eta_0(n) + \beta(n)$. После элементарных преобразований получаем необходимое равенство. ■

Критерий примитивности множества матриц $\hat{M}$ получен в [14]. Впервые универсальная оценка экспонента примитивного множества матриц порядка n дана в [15]:

$$\exp \hat{M} \leq \frac{n^3 + n^2}{2} - 2n + 1. \quad (1)$$

По замечанию автора оценки, она допускает уточнение, поскольку не зависит от мощности множества $\hat{M}$. Оценка (1) улучшена в [16]:

$$\exp \hat{M} \leq \frac{7n^3 + 6n^2 + 8n}{24} - 1. \quad (2)$$

Представляет также интерес критерий примитивности множества графов, полученный в [11]. Приведём этот критерий. Пусть в множестве орграфов $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$, $p > 1$, все дуги орграфа Γ_τ помечены числом τ , $\tau = 1, \dots, p$. Тогда множеству $\hat{\Gamma}$ однозначно соответствует мультиграф $\Gamma^{(p)} = \Gamma_1 \cup \dots \cup \Gamma_p$, в котором любой путь длины s

помечен непустым множеством слов длины s . 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. В частности, путь длины t имеет метку w^t , если каждая дуга пути помечена числом $w \in N_p$. Если множество $\hat{\Gamma}$ примитивное, то мультиграф $\Gamma^{(p)}$ сильносвязный [1, 2]. Сильносвязный мультиграф $\Gamma^{(p)}$ называется w -сильносвязным, если для любых вершин i и j 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 , $i = 0, \dots, n-1$. Критерий: орграф $\Gamma(w) = \Gamma_{w_1} \dots \Gamma_{w_s}$, где $w = w_1 \dots w_s$, примитивный, если и только если $\Gamma^{(p)}$ является w -сильносвязным и содержит контуры с метками $w^{t_1}, \dots, w^{t_m}$, где $\text{НОД}(t_1, \dots, t_m) = 1$.

Задача распознавания примитивности множества n -вершинных орграфов алгоритмически разрешима [11].

Критерий примитивности множества $\hat{\Gamma}$ существенно упрощается для некоторых частных классов, важных для приложений в области анализа систем защиты информации, в то же время уточняется оценка (2).

2. Примитивность множества орграфов с общим гамильтоновым контуром

Говорят, что «путь проходит через контур», если у пути и контура есть общая вершина. Путь проходит через множество контуров, если он проходит через каждый контур множества.

Обозначим: (θ, π) — тип орграфа Γ в мультипликативной циклической полугруппе $\langle \Gamma \rangle$, где θ и π — циклическая глубина и период орграфа Γ соответственно; $kC(i)$ — контур в Γ , соответствующий k -кратному проходу контура C из вершины i , где $k \in \mathbb{N}_0$; $0C(i)$ — пустой контур. Для подмножества натуральных чисел $\{a_1, \dots, a_m\}$, таких, что $\text{НОД}(a_1, \dots, a_m) = d = 1$, $m > 1$, числом Фробениуса $\Phi(a_1, \dots, a_m)$ называется наибольшее целое число, не принадлежащее аддитивной полугруппе $\langle a_1, \dots, a_m \rangle$. Обозначим $F(a_1, \dots, a_m) = d\Phi(a_1/d, \dots, a_m/d)$, $d \geq 1$ (если $d = 1$, то $F(a_1, \dots, a_m) = \Phi(a_1, \dots, a_m)$). Далее полагаем, что $1 \leq a_1 < \dots < a_m$.

Установим соотношения между длинами простых контуров в гамильтоновом орграфе Γ и его типом (циклической глубиной и периодом) как элемента циклической полугруппы $\langle \Gamma \rangle$. Данные соотношения позволяют оценить экспонент примитивного множества орграфов с общим гамильтоновым контуром.

Обозначим: $L = \{l_1, \dots, l_m\}$ — множество всех длин простых контуров в сильносвязном орграфе Γ , где $m > 1$, $l_1 < \dots < l_m$; $\hat{C} = \{C_1, \dots, C_m\}$ — множество простых контуров длин $l_1, \dots, l_m$ соответственно; $l(i, \hat{C}, j)$ — длина кратчайшего пути из вершины i в вершину j , проходящего через множество контуров $\hat{C}$.

Лемма 1. Если $\text{НОД}(L) = d$ в n -вершинном сильносвязном орграфе Γ , то для любой пары вершин (i, j) длины всех путей из i в j сравнимы по модулю d .

Доказательство. Пусть для некоторых вершин i, j в Γ есть пути из i в j длин l и $l+c$. Обозначим l_{ji} длину любого простого пути из j в i в орграфе Γ . Простой путь из j в i существует, поскольку орграф Γ сильносвязный. Следовательно, в Γ есть контуры длин $l + l_{ji}$ и $l + c + l_{ji}$. Так как длина любого контура есть сумма длин нескольких простых контуров, то в условиях леммы $d \mid (l + l_{ji})$ и $d \mid (l + c + l_{ji})$. Следовательно, $d \mid c$. ■

Теорема 3. Гамильтонов n -вершинный орграф Γ , в котором $\text{НОД}(L) = d$, имеет полугрупповой тип (θ, π) , где $\pi = d$ и $\theta \leq F(l_1, \dots, l_m) + d + \max_{0 \leq i, j \leq n-1} l(i, \hat{C}, j)$.

Доказательство. Так как $\text{НОД}(l_1/d, \dots, l_m/d) = 1$, то в соответствии со свойствами чисел Фробениуса для любого $b \in \mathbb{N}$ при некоторых $k_1, \dots, k_m \in \mathbb{N}_0$, зависящих от b , выполнено

$$k_1 l_1 + \dots + k_m l_m = F(l_1, \dots, l_m) + db.$$

Так как в Γ имеется путь из i в j длины $l(i, \hat{C}, j)$, проходящий через множество контуров $\hat{C}$, то для любого $b \in \mathbb{N}$ в Γ имеется путь из i в j длины $t_b(i, j)$, где

$$t_b(i, j) = l(i, \hat{C}, j) + F(l_1, \dots, l_m) + db,$$

содержащий обход контуров $C_1, \dots, C_m$ соответственно $k_1, \dots, k_m$ раз. В силу леммы 1, $t_b(i, j) \equiv l(i, \hat{C}, j) \pmod{d}$. Следовательно, дуга (i, j) одновременно имеется или не имеется в орграфах Γ^t и Γ^{t+d} , $t \geq t_1(i, j)$. Данные рассуждения верны для любой пары вершин (i, j) , значит, $\Gamma^t = \Gamma^{t+d}$, $t \geq \max_{0 \leq i, j \leq n-1} t_1(i, j)$. Следовательно, $\pi \mid d$.

По определению, $\Gamma^t = \Gamma^{t+\pi}$, $t \geq \max_{0 \leq i, j \leq n-1} t_1(i, j)$. Тогда в Γ имеются пути из i в j длины t и $t + \pi$ для некоторых вершин i и j , что при $\pi < d$ противоречит лемме 1. Отсюда $\pi = d$. ■

Следствие 1. Имеет место

$$\theta \leq 2n - l_1 + \begin{cases} F(l_1, \dots, l_m) + d - 1, & d > 1, \\ \Phi(l_1, \dots, l_m), & d = 1. \end{cases}$$

Доказательство. Обозначим: $w(i, j)$ — кратчайший путь из вершины i в вершину j , $w(i, i)$ — путь длины 0; $\lambda_k = n - l_k$, $k = 1, \dots, m$.

Заметим, что путь $w(i, j)$ определен неоднозначно и $0 \leq \text{len } w(i, j) \leq n - 1$ при любых i, j . Для вершин i, j построим путь $[i, j]$, проходящий через множество контуров $\hat{C}$, и оценим длину этого пути.

Если $\text{len } w(i, j) \geq \lambda_k$, то $w(i, j)$ проходит через контур C_k , имеющий l_k вершин, $k = 1, \dots, m$. Отсюда если $\text{len } w(i, j) \geq \lambda_1$, то путь $w(i, j)$ проходит через множество контуров $\hat{C}$, так как $\lambda_1 > \lambda_2 > \dots > \lambda_m$. В случае $\text{len } w(i, j) \geq \lambda_1$ полагаем $[i, j] = w(i, j)$. В случае $\text{len } w(i, j) < \lambda_1$ полагаем $[i, j] = w(i, j) \circ C_m(j)$, где путь $[i, j]$ проходит через множество контуров $\hat{C}$ в силу гамильтоновости контура C_m и $\text{len } [i, j] = \text{len } w(i, j) + n < \lambda_1 + n = 2n - l_1$. Следовательно, $l(i, \hat{C}, j) \leq \text{len } [i, j] \leq 2n - l_1 - 1$ для любых вершин i, j . Отсюда и из теоремы 3 получаем нужную оценку θ . ■

Замечание 1. Данная оценка θ при $d = 1$ совпадает с оценкой экспонента примитивного гамильтонова орграфа Γ [17, следствие 2].

Пример 1. В табл. 1 приведены оценки и точные значения циклической глубины гамильтоновых орграфов при $n = 6$. Орграфы Γ_1 и Γ_2 непримитивные, орграф Γ_3 примитивный (граф Виландта). Как видно из табл. 1, для орграфов Γ_2 и Γ_3 достигается верхнее значение оценки величины $\max_{0 \leq i, j \leq n-1} l(i, \hat{C}, j)$, для орграфа Γ_3 — верхняя оценка θ , приведённые в следствии 1.

Т а б л и ц а 1

Оценки и точные значения циклической глубины для орграфов Γ_1 и Γ_2

Γ	$\hat{C}$	d	$F(l_1, \dots, l_m)$	$\max_{0 \leq i, j \leq n-1} l(i, \hat{C}, j)$	$\max_{0 \leq i, j \leq n-1} t_1(i, j)$	θ
Γ_1	$C_1 = (0, 4, 5),$ $C_2 = (1, 2, 3),$ $C_3 = (0, 1, 2, 3, 4, 5)$	3	$3\Phi(1, 2) = -3$	$l(1, \hat{C}, 0) = 5$	$3 - 3 + 5 = 5$	3
Γ_2	$C_1 = (0, 4, 5),$ $C_2 = (0, 1, 2, 3, 4, 5)$	3	$3\Phi(1, 2) = -3$	$l(1, \hat{C}, 3) = 8$	$3 - 3 + 8 = 8$	6
Γ_3	$C_1 = (0, 1, 2, 3, 4),$ $C_2 = (0, 1, 2, 3, 4, 5)$	1	$\Phi(5, 6) = 19$	$l(5, \hat{C}, 5) = 6$	$1 + 19 + 6 = 26$	26

Рассмотрим множество орграфов $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$, $p > 1$. Обозначим $U^{(p)}$ орграф, полученный из мультиграфа $\Gamma^{(p)} = \Gamma_1 \cup \dots \cup \Gamma_p$ удалением всех меток и отождествлением кратных дуг. Наименьшее количество орграфов множества $\hat{\Gamma}$, объединение которых содержит все дуги орграфа $U^{(p)}$, обозначим μ . По определению $1 \leq \mu \leq p$.

Множество орграфов называется сокращённым (понятие введено в [18]), если ни один из орграфов множества не является частью другого орграфа этого множества. Примитивность любого множества равносильна примитивности его сокращённого подмножества (следует из [18, утверждение 5]), и в случае примитивности их экспоненты равны. При $p > \mu = 1$ множество $\hat{\Gamma}$ не сокращённое, поскольку все орграфы являются частью одного из орграфов множества $\hat{\Gamma}$. Этот случай выходит за рамки данной работы, так как исследование примитивности множества $\hat{\Gamma}$ сводится к проверке свойства примитивности орграфа с наибольшим числом дуг. Без ограничения общности далее полагаем, что $U^{(p)} = U^{(\mu)}$, где $1 < \mu \leq p$.

Установим критерий примитивности множества орграфов с общим гамильтоновым контуром.

Теорема 4. Пусть $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$ — множество орграфов с общим гамильтоновым контуром $Z = (0, \dots, n-1)$, $p > 1$. Множество $\hat{\Gamma}$ примитивное, если и только если орграф $U^{(p)}$ примитивный. Для экспонента примитивного множества орграфов $\hat{\Gamma}$ верна оценка

$$\exp \hat{\Gamma} \leq (2n-1)\mu + \sum_{\tau=1}^{\mu} (F(l_1^{\tau}, \dots, l_{m(\tau)}^{\tau}) + d_{\tau} - l_1^{\tau}), \quad (3)$$

где $l_1^{\tau}, \dots, l_{m(\tau)}^{\tau}$ — длины всех простых контуров орграфа Γ_{τ} , $l_1^{\tau} < \dots < l_{m(\tau)}^{\tau} = n$; $d_{\tau} = \text{НОД}(l_1^{\tau}, \dots, l_{m(\tau)}^{\tau})$, $\tau = 1, \dots, \mu$.

Доказательство. Необходимость. Пусть множество $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$ примитивное и $M_1, \dots, M_p$ — матрицы смежности орграфов $\Gamma_1, \dots, \Gamma_p$ соответственно. Из примитивности множества $\hat{\Gamma}$ следует примитивность множества $\hat{M} = \{M_1, \dots, M_p\}$. Тогда матрица $M = M_1 + \dots + M_p$ примитивная в силу [2, теорема 11.8]. Заметим, что матрица M является матрицей смежности вершин орграфа $U^{(p)}$. Следовательно, орграф $U^{(p)}$ примитивный.

Достаточность. Считаем, что все орграфы множества $\hat{\Gamma}$ непримитивные, иначе очевидно, что орграф $U^{(p)}$ примитивный и теорема верна.

Пусть примитивный орграф $U^{(p)}$ содержит множество простых контуров $\hat{C} = \{C_1, \dots, C_m\}$ длин $l_1, \dots, l_m$ соответственно, где $\text{НОД}(l_1, \dots, l_m) = 1$ и $m > 1$, иначе один из орграфов множества $\hat{\Gamma}$ гамильтонов и имеет петлю, т. е. примитивный.

Поскольку $U^{(p)} = U^{(\mu)}$, то $U^{(\mu)}$ содержит все дуги контуров множества $\hat{C}$. Обозначим: $(\theta_{\tau}, \pi_{\tau})$ — тип орграфа Γ_{τ} , $\tau = 1, \dots, \mu$; $\pi = \text{НОД}(\pi_1, \dots, \pi_{\mu})$. Из теоремы 3

следует, что $\pi_\tau = d_\tau = \text{НОД}(l_1^\tau, \dots, l_{m(\tau)}^\tau)$, $\tau = 1, \dots, \mu$, значит, π делит длину любого контура любого орграфа из множества $\{\Gamma_1, \dots, \Gamma_\mu\}$. Докажем, что $\pi = 1$.

Пусть $C = (u_0, \dots, u_{l-1})$ — любой контур. Конкатенация дуги $(u_k, u_{(k+1) \bmod l})$ и части контура Z образуют в некотором из орграфов $\Gamma_1, \dots, \Gamma_\mu$ контур длины $\lambda_k = n - (u_{(k+1) \bmod l} - u_k) \bmod n + 1$, значит, $\pi \mid \lambda_k$, $k = 0, \dots, l-1$, и $\pi \mid \sum_{k=0}^{l-1} (n - \lambda_k)$, где

$$\sum_{k=0}^{l-1} (n - \lambda_k) = \sum_{k=0}^{l-1} ((u_{(k+1) \bmod l} - u_k) \bmod n - 1) = n - l.$$

Тогда $\pi \mid (n - l)$ и π делит длину l любого контура из $\hat{C}$, что при $\pi > 1$ противоречит условию $\text{НОД}(l_1, \dots, l_m) = 1$. Следовательно, $\pi = 1$.

Построим в мультиграфе $\Gamma^{(p)}$ для любых вершин i, j путь из i в j с меткой $1^{t_1} \dots \mu^{t_\mu}$, где $t_1, \dots, t_\mu \in \mathbb{N}$. Контур Z гамильтонов, следовательно, в Γ_1 есть пути из вершины i в вершину $(i + t_1) \bmod n$ длины t_1 и в вершину $(i + t_1 + \pi_1) \bmod n$ длины $t_1 + \pi_1$ при любом $t_1 \in \mathbb{N}$. Тогда $(i, (i + t_1) \bmod n)$ есть дуга орграфа $\Gamma_1^{t_1}$ и $(i, (i + t_1 + \pi_1) \bmod n)$ есть дуга орграфа $\Gamma_1^{t_1 + \pi_1}$. В соответствии с теоремой 3, $\Gamma_1^{t_1} = \Gamma_1^{t_1 + \pi_1}$ при $t_1 \geq \theta_1$, значит, при указанных t_1 в орграфе $\Gamma_1^{t_1}$ есть дуга $(i, (i + t_1 + \pi_1) \bmod n)$, тогда в Γ_1 есть путь из вершины i в вершину $(i + t_1 + \pi_1) \bmod n$ длины t_1 . Поскольку π_1 — период орграфа Γ_1 , то в орграфе Γ_1 есть пути из вершины i в вершину $(i + t_1 + k_1 \pi_1) \bmod n$ длины t_1 для любых $t_1 \geq \theta_1$ и $k_1 \in \mathbb{N}_0$. Тогда в мультиграфе $\Gamma^{(p)}$ есть пути с меткой 1^{t_1} из вершины i в любую вершину множества $I_1 = \{(i + t_1 + k_1 \pi_1) \bmod n : k_1 \in \mathbb{N}_0\}$.

Пусть $i_1 \in I_1$. Повторив на втором шаге рассуждения для вершины i_1 , получаем, что в мультиграфе $\Gamma^{(p)}$ при $t_2 \geq \theta_2$ есть пути с меткой 2^{t_2} из вершины i_1 в любую вершину множества $I_2 = \{(i_1 + t_2 + k_2 \pi_2) \bmod n : k_2 \in \mathbb{N}_0\}$. Объединяя утверждения двух шагов, получаем, что в $\Gamma^{(p)}$ есть пути с меткой $1^{t_1} 2^{t_2}$ из вершины i в любую вершину множества $I_{12} = \{(i + t_1 + t_2 + k_1 \pi_1 + k_2 \pi_2) \bmod n : k_1, k_2 \in \mathbb{N}_0\}$ при $t_1 \geq \theta_1$ и $t_2 \geq \theta_2$.

Продолжая следующие шаги рассуждений, получаем, что в $\Gamma^{(p)}$ есть пути с меткой $1^{t_1} \dots \mu^{t_\mu}$ из i в любую вершину множества $I_{1\mu} = \{(i + t + k_1 \pi_1 + \dots + k_\mu \pi_\mu) \bmod n : k_1, \dots, k_\mu \in \mathbb{N}_0\}$, где $t = t_1 + \dots + t_\mu$, $t_1 \geq \theta_1, \dots, t_\mu \geq \theta_\mu$. В зависимости от чисел $k_1, \dots, k_\mu$ величина $k_1 \pi_1 + \dots + k_\mu \pi_\mu$ принимает любые значения, превышающие число Фробениуса $\Phi(\pi_1, \dots, \pi_\mu)$. Значит, множество $I_{1\mu}$ содержит полную систему вычетов по модулю n — множество $\{0, \dots, n-1\}$. Таким образом, построены пути с меткой $1^{t_1} \dots \mu^{t_\mu}$ из вершины i в любую вершину. Следовательно, орграф $\Gamma_1^{t_1} \dots \Gamma_\mu^{t_\mu}$ полный и множество $\hat{\Gamma}$ примитивное. Критерий доказан.

Получим оценку $\text{exp } \hat{\Gamma}$. Орграф $\Gamma_1^{t_1} \dots \Gamma_\mu^{t_\mu}$ полный при любых $t_\tau \geq \theta_\tau$, $\tau = 1, \dots, \mu$, следовательно, $\text{exp } \hat{\Gamma} \leq \theta_1 + \dots + \theta_\mu$. По следствию 1, $\theta_\tau \leq 2n - 1 - l_1^\tau + F(l_1^\tau, \dots, l_{m(\tau)}^\tau) + d_\tau$.

Тогда $\text{exp } \hat{\Gamma} \leq (2n - 1)\mu + \sum_{\tau=1}^{\mu} (F(l_1^\tau, \dots, l_{m(\tau)}^\tau) + d_\tau - l_1^\tau)$. ■

Примитивный орграф называется минимальным, если после удаления любой дуги нарушается свойство его примитивности [19]. Обозначим: $G(n, Z)$ — множество n -вершинных орграфов, имеющих гамильтонов контур Z , $\sigma(n, Z) = |G(n, Z)| = 2^{m-n}$, где $m = n^2$; $G^P(n, Z)$ — множество примитивных n -вершинных орграфов, имеющих гамильтонов контур Z , $\pi(n, Z) = |G^P(n, Z)|$; $G_{\min}^P(n, Z)$ — множество минимальных примитивных орграфов, имеющих гамильтонов контур Z , $\omega(n, Z) = |G_{\min}^P(n, Z)|$; $G_{\min}^P(n, Z) \subset G^P(n, Z) \subset G(n, Z)$. Множество примитивных n -вершинных орграфов, имеющих гамильтонов контур, представляет особый интерес при исследовании пере-

мешивающих свойств регистровых преобразований, в частности при $n = 2^\alpha$, $\alpha \in \mathbb{N}$. Следующая теорема устанавливает количество таких орграфов для примарного числа вершин n .

Теорема 5. Пусть $n = q^\alpha$, q — простое число, $\alpha \in \mathbb{N}$, $m = n^2$. Тогда

$$\pi(n, Z) = \frac{2^m - 2^{m/q}}{2^n}.$$

Доказательство. Любое число, не кратное q , взаимно просто с $n = q^\alpha$, $\alpha \in \mathbb{N}$. Тогда по условию минимальный примитивный орграф с гамильтоновым контуром Z имеет $n+1$ дугу, где дуги образуют простые контуры длин l и n , $1 \leq l < n$, $\text{НОД}(l, n) = 1$. Следовательно, любой примитивный гамильтонов орграф с числом дуг больше $n+1$ не минимальный.

Найдём $\omega(n, Z) = |G_{\min}^P(n, Z)|$. Обозначим $\Pi(n) = \{l_1, \dots, l_r\}$ — множество чисел, взаимно простых с n , где $r = q^\alpha - q^{\alpha-1} = n - n/q$ — значение функции Эйлера при $n = q^\alpha$. Существует n изоморфных орграфов множества $G_{\min}^P(n, Z)$, имеющих простой контур длины l_i , $i = 1, \dots, r$. Следовательно, $\omega(n, Z) = n(n - n/q)$.

Положим $G_{\min}^P(n, Z) = \{\Gamma_1, \dots, \Gamma_\omega\}$, где $\omega = \omega(n, Z)$, и рассмотрим множества $U_i = \{\Gamma: \Gamma \geq \Gamma_i\}$, $i = 1, \dots, \omega$. Тогда $G^P(n, Z) = U_1 \cup \dots \cup U_\omega$. Заметим, что $|U_{i_1} \cap \dots \cap U_{i_k}| = 2^{m-(n+k)}$ при любом $k = 1, \dots, \omega$. Используя принцип включения-исключения, найдём $|G^P(n, Z)|$:

$$\begin{aligned} \pi(n, Z) &= |G^P(n, Z)| = |U_1 \cup \dots \cup U_\omega| = \\ &= \sum_{k=1}^{\omega} (-1)^{k-1} C_{\omega}^k 2^{m-(n+k)} = 2^{m-n} \left(\sum_{k=1}^{\omega} (-1)^{k-1} C_{\omega}^k 2^{-k} \right). \end{aligned} \quad (4)$$

Применяя формулу бинома Ньютона, преобразуем (4) к виду $\pi(n, Z) = 2^{m-n}(1 - 2^{-\omega})$. Поскольку $\omega = n(n - n/q) = m - m/q$, $\pi(n, Z) = 2^{m-n}(1 - 2^{m/q-m}) = (2^m - 2^{m/q})/2^n$. ■

Пример 2. При $n = 4$ существует $2^{m-n} = 2^{12} = 4096$ орграфов с гамильтоновым контуром $Z = (0, 1, 2, 3)$. Из них, по теореме 5, 4080 орграфов — примитивные.

Обозначим $\beta(n, Z)$ число примитивных множеств n -вершинных орграфов с общим гамильтоновым контуром Z , в которых каждый орграф не примитивен.

Из критерия примитивности множества орграфов с общим гамильтоновым контуром и теорем 2 и 5 следует точное значение числа примитивных множеств орграфов с общим гамильтоновым контуром Z при $n = q^\alpha$, где q — простое число, $\alpha \in \mathbb{N}$.

Следствие 2. Пусть $n = q^\alpha$, q — простое число, $\alpha \in \mathbb{N}$, $m = n^2$. Тогда число примитивных множеств орграфов с общим гамильтоновым контуром Z равно

$$\eta(n, Z) = 2^\sigma - 2^\varepsilon,$$

где $\sigma = 2^{m-n}$; $\varepsilon = 2^{m/q-n}$.

Доказательство. Из теоремы 2 следует, что

$$\eta(n, Z) = 2^{\sigma(n, Z)} - 2^{\sigma(n, Z) - \pi(n, Z)} + \beta(n, Z).$$

Найдём $\beta(n, Z)$. При $n = q^\alpha$ если орграф Γ_i содержит гамильтонов контур Z и не примитивен, то длины всех простых контуров орграфа Γ_i кратны q , $i = 1, \dots, p$. Следовательно, длины всех простых контуров орграфа $U^{(p)}$ также кратны q и $U^{(p)}$ непримитивный. Тогда $\beta(n, Z) = 0$ согласно критерию теоремы 4. Значит, $\eta(n, Z) = 2^{\sigma(n, Z)} - 2^{\sigma(n, Z) - \pi(n, Z)}$, где $\sigma(n, Z) = \sigma = 2^{m-n}$, $\pi(n, Z) = (2^m - 2^{m/q})/2^n$ (по теореме 5). Тогда $\sigma(n, Z) - \pi(n, Z) = \varepsilon = 2^{m/q-n}$. ■

3. Критерий примитивности множества орграфов с общим множеством контуров

Обозначим: C^* — множество вершин контура C ; $\Gamma(\hat{C}) = C_1 \cup \dots \cup C_m$ — часть орграфа Γ ; $E(\hat{C})$ — множество дуг орграфа $\Gamma(\hat{C})$.

Воспользуемся терминами теории признаков в полугруппах [1, гл. 9]. Подмножество H полугруппы G , состоящее из всех элементов G , обладающих определённым свойством, называется признаком H (H -признаком) в полугруппе G . Если $H \leq G$ — подполугруппа, то H называется полугрупповым признаком в G . В полугруппе $\Gamma(n)$ полугрупповым признаком (обозначается $P_{\text{лоор}}$) является, в частности, множество всех орграфов, имеющих петли в каждой вершине множества P , $\emptyset \neq P \subseteq V$. Показателем $P_{\text{лоор}}$ -признака в полугруппе $\langle \Gamma \rangle$ называется наименьшее натуральное h , при котором $\Gamma^h \in P_{\text{лоор}}$ (обозначается $\text{rok}P_{\text{лоор}}$ или кратко l_P). В [20] получены оценки и точное значение показателя $P_{\text{лоор}}$ -признака.

Следующая теорема устанавливает критерий примитивности и оценку экспонента множества орграфов с общим множеством простых контуров.

Теорема 6. Пусть $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$ — множество орграфов с общим множеством контуров $\hat{C} = \{C_1, \dots, C_m\}$, $p, m > 1$, $C_1^* \cup \dots \cup C_m^* = V$. Множество $\hat{\Gamma}$ примитивное, если и только если оргграф $U^{(p)}$ примитивный. Для экспонента примитивного множества орграфов $\hat{\Gamma}$ верна оценка

$$\exp \hat{\Gamma} \leq ((\mu - 1)h + 1) \exp U^{(p)}, \quad (5)$$

где h — показатель $V_{\text{лоор}}$ -признака в полугруппе $\langle \Gamma(\hat{C}) \rangle$.

Доказательство. Необходимость критерия доказывается, как в теореме 4.

Достаточность. Рассмотрим неочевидный случай, когда все оргграфы множества $\hat{\Gamma}$ непримитивны. Обозначим $G_{1,r} = \Gamma_1^h \dots \Gamma_{r-1}^h \Gamma_r$. Докажем по индукции, что оргграф $U^{(r)}$ является частью оргграфа $G_{1,r}$, $1 < r \leq \mu$.

При $r = 2$ покажем, что $U^{(2)}$ — часть оргграфа $G_{1,2} = \Gamma_1^h \Gamma_2$, т.е. $G_{1,2}$ содержит все дуги оргграфов Γ_1 и Γ_2 . Поскольку $h = \text{rok}V_{\text{лоор}}$ в полугруппе $\langle \Gamma(\hat{C}) \rangle$ и оргграф Γ_1 содержит множество контуров $\hat{C}$, то оргграф Γ_1^h имеет петли во всех вершинах. Отсюда оргграф $G_{1,2}$ содержит все дуги оргграфа Γ_2 , в том числе множество общих контуров $\hat{C}$.

Пусть (i, j) — дуга оргграфа Γ_1 и $(i, j) \notin E(\hat{C})$. Покажем, что оргграф $G_{1,2}$ содержит дугу (i, j) . Из условия $C_1^* \cup \dots \cup C_m^* = V$ следует, что любая вершина оргграфа Γ_1 принадлежит хотя бы одному из контуров множества $\hat{C}$. Тогда в Γ_1 есть дуга $(a, j) \in E(\hat{C})$, $a \neq i$, такая, что из j в a в Γ_1 есть путь длины $h - 1$ (следует из определения показателя $V_{\text{лоор}}$ -признака). Тогда в оргграфе Γ_1^h есть дуга (i, a) . Оргграф Γ_2 имеет дугу (a, j) , поскольку множество $\hat{C}$ есть множество общих контуров и $(a, j) \in E(\hat{C})$. Тогда, в силу правила умножения оргграфов, оргграф $G_{1,2}$ содержит дугу (i, j) . Таким образом, $G_{1,2}$ содержит все дуги оргграфов Γ_1 и Γ_2 и, следовательно, $U^{(2)}$ является частью оргграфа $G_{1,2}$.

Пусть утверждение доказано для $r = 2, \dots, q - 1$, где $2 < q \leq \mu$, докажем его для $r = q$. По условию $G_{1,q} = G_{1,q-1} \Gamma_q^{h-1}$. По предположению индукции оргграф $U^{(q-1)}$ является частью оргграфа $G_{1,q-1}$, т.е. $G_{1,q-1}$ содержит общее множество контуров $\hat{C}$ и все дуги оргграфов $\Gamma_1, \dots, \Gamma_{q-1}$. Рассмотрим оргграф $\Gamma = \Gamma_{q-1}^{h-1} \Gamma_q$. Поскольку $h = \text{rok}V_{\text{лоор}}$ в полугруппе $\langle \Gamma(\hat{C}) \rangle$ и оргграф $\Gamma(\hat{C})$ является общей частью Γ_{q-1} и Γ_q , оргграф Γ имеет петли во всех вершинах множества V . Отсюда $G_{1,q} = G_{1,q-1} \Gamma$ содержит все дуги оргграфа $G_{1,q-1}$. Таким образом, $G_{1,q}$ содержит все дуги оргграфов $\Gamma_1, \dots, \Gamma_{q-1}$.

Покажем, что оргграф $G_{1,q}$ содержит все дуги оргграфа Γ_q . Рассмотрим оргграф $\Gamma' = G_{1,q-1}\Gamma_{q-1}^{h-1} = \Gamma_1^h \dots \Gamma_{q-1}^h$. Оргграф $\Gamma(\hat{C})$ является общей частью оргграфов $\Gamma_1, \dots, \Gamma_{q-1}$, откуда следует, что Γ' имеет петли во всех вершинах. Тогда оргграф $G_{1,q} = \Gamma'\Gamma_q$ содержит все дуги оргграфа Γ_q .

Таким образом, $G_{1,q}$ содержит все дуги оргграфов $\Gamma_1, \dots, \Gamma_q$, т.е. оргграф $U^{(q)}$ является частью оргграфа $G_{1,q}$. Отсюда оргграф $U^{(\mu)}$, а следовательно, и $U^{(p)}$ являются частями оргграфа $G_{1,\mu} = \Gamma_1^h \dots \Gamma_{\mu-1}^h \Gamma_\mu$. Из примитивности оргграфа $U^{(p)}$ следует примитивность $G_{1,\mu}$ и $\exp G_{1,\mu} \leq \exp U^{(p)}$. Оргграф $G_{1,\mu}$ является словом в алфавите $\hat{\Gamma}$, следовательно, множество $\hat{\Gamma}$ примитивное и $\exp \hat{\Gamma} \leq ((\mu - 1)h + 1)\exp G_{1,\mu} \leq ((\mu - 1)h + 1)\exp U^{(p)}$. ■

Пример 3. На рис. 1 изображены множества оргграфов $\hat{\Gamma} = \{\Gamma_1, \Gamma_2\}$ с множеством вершин $\{0, \dots, 5\}$. На рис. 1, а оргграфы имеют общий гамильтонов контур $Z = (0, \dots, 5)$, на рис. 1, б множество общих контуров есть $\hat{C} = \{(0, 1, 2, 3), (0, 1), (2, 3), (4, 5)\}$. Оценки экспонентов и их точные значения приведены в табл. 2.

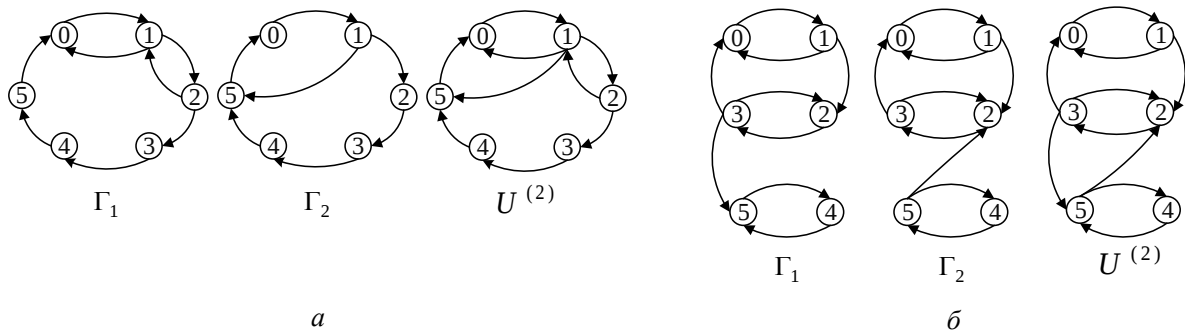


Рис. 1. Множества $\hat{\Gamma} = \{\Gamma_1, \Gamma_2\}$ и соответствующие оргграфы $U^{(2)}$

Т а б л и ц а 2

$\hat{\Gamma}$	Универсальная оценка (1)	Улучшенная оценка (2)	Оценка (3)	Оценка (5)	$\exp \hat{\Gamma}$
<i>a</i>	$\exp \hat{\Gamma} \leq 115$	$\exp \hat{\Gamma} \leq 73$	$\exp \hat{\Gamma} \leq 17$	$\exp \hat{\Gamma} \leq 63$	11
<i>б</i>			—	$\exp \hat{\Gamma} \leq 21$	8

Заключение

Исследованы условия примитивности и оценки экспонентов множества оргграфов с множеством общих контуров, в частности с общим гамильтоновым контуром. Данные классы множеств содержат классы множеств перемешивающих оргграфов регистров сдвига, широко используемых для построения систем защиты информации. Получен существенно более простой (по сравнению с общим случаем) критерий примитивности множества оргграфов, имеющих семейство общих контуров, содержащих все n вершин, в частности имеющих общий гамильтонов контур.

Критерий примитивности множества оргграфов с общим гамильтоновым контуром позволил получить точное значение числа примитивных множеств таких оргграфов для примарного числа вершин. В случае когда n — степень числа 2, этот результат имеет прикладное значение для исследования регистровых преобразований.

На примере множеств из двух орграфов с общими контурами показана возможность получения более точных оценок (3) и (5) по сравнению с универсальными оценками (1) и (2). Если общее множество контуров содержит гамильтонов контур, оценка (3) существенно уточняет оценку (5).

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: Изд-во «ЮРАЙТ», 2016. 209 с.
3. *Frobenius G.* Uber Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss., 1912. P. 456–477.
4. *Dulmage A. L. and Mendelsohn N. S.* The exponent of a primitive matrix // Canad. Math. Bull. 1962. No. 5. P. 241–244.
5. *Harary F.* Graph Theory. Addison-Wesley Publ., 1969. 275 p.
6. *Perkins P.* A theorem on regular graphs // Pacific J. Math. 1912. V. II. P. 1529–1533.
7. *Протасов Ю. В.* Полугруппы неотрицательных матриц // Успехи математических наук. 2010. Т. 65. Вып. 6(396). С. 191–192.
8. *Cohen J. E. and Sellers P. H.* Sets of nonnegative matrices with positive inhomogeneous products // Linear Algebra Appl. 1982. V. 47. P. 185–192.
9. *Olesky D. D., Shader B., and van den Driessche P.* Exponents of tuples of nonnegative matrices // Linear Algebra Appl. 2002. V. 356. No. 1–3. P. 123–134.
10. *Авезова Я. Э.* О примитивности некоторых множеств перемешивающих орграфов регистровых преобразований // Прикладная дискретная математика. Приложение. 2017. № 10. С. 60–62.
11. *Авезова Я. Э., Фомичев В. М.* Условия примитивности и оценки экспонентов множеств ориентированных графов // Прикладная дискретная математика. 2017. № 35. С. 89–101.
12. *Авезова Я. Э.* Критерий примитивности и оценки экспонентов множества орграфов с общим множеством контуров // Прикладная дискретная математика. Приложение. 2018. № 11. С. 102–104.
13. *Кяжсин С. Н.* Весовые свойства примитивных матриц // Прикладная дискретная математика. Приложение. 2018. № 11. С. 10–12.
14. *Protasov V. Yu. and Voynov A. S.* Sets of nonnegative matrices without positive products // Linear Algebra Appl. 2012. V. 437. No. 3. P. 749–765.
15. *Voynov A. S.* Shortest positive products of nonnegative matrices // Linear Algebra Appl. 2013. V. 439. No. 6. P. 1627–1634.
16. *Blondel V. D., Jungers R. M., and Olshevsky A.* On primitivity of sets of matrices // Automatica. 2015. V. 61. P. 80–88.
17. *Фомичев В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.
18. *Авезова Я. Э., Фомичев В. М.* Комбинаторные свойства систем разноразмерных 0,1-матриц // Прикладная дискретная математика. 2014. № 2(24). С. 5–11.
19. *Фомичев В. М.* Свойства минимальных примитивных орграфов // Прикладная дискретная математика. 2015. № 2(28). С. 86–96.
20. *Авезова Я. Э., Фомичев В. М.* Об одном наследственном признаке в циклических полугруппах графов // Прикладная дискретная математика. Приложение. 2016. № 9. С. 105–109.

REFERENCES

1. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MIFI Publ., 2010. 424 p. (in Russian)
2. *Fomichev V. M. and Mel'nikov D. A.* Kriptograficheskie metody zashchity informatsii. Ch. 1. Matematicheskie aspekty [Cryptographic Methods of Information Security. P. 1. Mathematical Aspects]. Moscow, YuRAYT Publ., 2016. 209 p. (in Russian)
3. *Frobenius G.* Uber Matrizen aus nicht negativen Elementen. Sitzungsber K. Preuss. Akad. Wiss., 1912, pp. 456–477.
4. *Dulmage A. L. and Mendelsohn N. S.* The exponent of a primitive matrix. Canad. Math. Bull., 1962, no. 5, pp. 241–244.
5. *Harary F.* Graph Theory. Addison-Wesley Publ., 1969. 275 p.
6. *Perkins P.* A theorem on regular graphs. Pacific J. Math., 1961, vol. II, pp. 1529–1533.
7. *Protasov Yu. V.* Semigroups of non-negative matrices. Russian Math. Surveys, 2010, vol. 65, no. 6, pp. 1186–1188.
8. *Cohen J. E. and Sellers P. H.* Sets of nonnegative matrices with positive inhomogeneous products. Linear Algebra Appl., 1982, vol. 47, pp. 185–192.
9. *Olesky D. D., Shader B., and van den Driessche P.* Exponents of tuples of nonnegative matrices. Linear Algebra Appl., 2002. vol. 356, no. 1–3, pp. 123–134.
10. *Avezova Y. E.* O primitivnosti nekotorykh mnozhestv peremeshivayushchikh orgrafov registrovkh preobrazovaniy [On primitivity of some shift registers mixing digraphs sets]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2017, no. 10, pp. 60–62. (in Russian)
11. *Avezova Y. E. and Fomichev V. M.* Usloviya primitivnosti i otsenki eksponentov mnozhestv oriyeirovannykh grafov [Conditions of primitivity and exponent bounds for sets of digraphs]. Prikladnaya Diskretnaya Matematika, 2017, no. 35, pp. 89–101. (in Russian)
12. *Avezova Y. E.* Kriteriy primitivnosti i otsenki eksponentov mnozhestva orgrafov s obshchim mnozhestvom konturov [The criterion of primitivity and exponent bounds for a set of digraphs with common cycles]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2018, no. 11, pp. 102–104. (in Russian)
13. *Kyazhin S. N.* Vesovye svoystva primitivnykh matrirts [Weight properties of primitive matrices]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2018, no. 11, pp. 10–12. (in Russian)
14. *Protasov V. Yu. and Voynov A. S.* Sets of nonnegative matrices without positive products. Linear Algebra Appl., 2012, vol. 437, no. 3, pp. 749–765.
15. *Voynov A. S.* Shortest positive products of nonnegative matrices. Linear Algebra Appl., 2013, vol. 439, no. 6, pp. 1627–1634.
16. *Blondel V. D., Jungers R. M., and Olshevsky A.* On primitivity of sets of matrices. Automatica, 2015, vol. 61. pp. 80–88.
17. *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)
18. *Avezova Y. E. and Fomichev V. M.* Kombinatornyye svoystva sistem raznorazmernykh 0,1-matrirts [Combinatorial properties of rectangular 0,1-matrix systems]. Prikladnaya Diskretnaya Matematika, 2014, no. 2(24), pp. 5–11. (in Russian)
19. *Fomichev V. M.* Svoystva minimal'nykh primitivnykh orgrafov [Properties of minimal primitive digraphs]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 86–96. (in Russian)

20. *Avezova Y. E. and Fomichev V. M.* Ob odnom nasledstvennom priznake v tsiklicheskikh polugruppakh grafov [About one heritable character in cyclic semigroups of graphs]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2016, no. 9, pp. 105–109. (in Russian)