

УДК 519.17

**О ПРИМЕНЕНИИ УСЛОВИЙ ЛОКАЛЬНОЙ ПРИМИТИВНОСТИ
И ОЦЕНОК ЛОКАЛЬНЫХ ЭКСПОНЕНТОВ ОРГРАФОВ**

С. Н. Кязжин

*Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия
Центр специальных разработок МО РФ, г. Москва, Россия*

В развитие матрично-графового подхода к исследованию перемешивающих свойств итеративных преобразований С.Н. Кязжиным, В.М. Фомичевым были введены понятия локальной примитивности и локального экспонента орграфа, обобщающие известные понятия примитивности и экспонента и позволяющие расширить область приложений, и получены универсальный критерий $i \times j$ -примитивности и универсальная оценка $i \times j$ -экспонента орграфа. Однако применение данных результатов не всегда удобно, так как затруднено общностью математической модели. В данной работе для различных классов орграфов, определяемых взаимным расположением компонент сильной связности и их строением, получены условия $i \times j$ -примитивности и оценки (в ряде случаев точные значения) $i \times j$ -экспонента, улучшающие универсальную оценку. Условия локальной примитивности и величина оценок локальных экспонентов определяются свойствами множества длин путей из i в j в перемешивающем орграфе, а также длинами контуров, содержащихся в компонентах сильной связности, через которые проходят данные пути. Полученные результаты значительно упрощают для исследователя распознавание локальной примитивности и получение оценок локальных экспонентов конкретных перемешивающих орграфов преобразований, возникающих, в том числе, в криптографических приложениях.

Ключевые слова: *локальная примитивность, локальный экспонент, орграф, компонента сильной связности.*

DOI 10.17223/20710410/34/7

**ON ADAPTATION OF DIGRAPH LOCAL PRIMITIVENESS
CONDITIONS AND LOCAL EXPONENT ESTIMATIONS**

S. N. Kyazhin

*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow,
Russia*

*Special Development Center of the Ministry of Defence of the Russian Federation, Moscow,
Russia*

E-mail: s.kyazhin@kaf42.ru

For vertices i and j in a digraph Γ , the last is called $i \times j$ -primitive if for some $\gamma \in \mathbb{N}$ and any integer $t \geq \gamma$, there is a path of length t from i to j in Γ . The least such γ is called $i \times j$ -exponent of Γ and is noted as $i \times j$ -exp Γ . Because of mathematical model generality, it is not always easy to use the universal criterion of digraph $i \times j$ -primitiveness and the universal estimation of digraph $i \times j$ -exponent obtained by

S.N. Kyazhin and V.M. Fomichev. In the paper, some criteria of digraph $i \times j$ -primitiveness and an estimations of digraph $i \times j$ -exponent in two special cases are given.

For vertices i and j being achievable from each other, that is, belonging to a strongly connected component U , the graph Γ is $i \times j$ -primitive if and only if U is primitive. If Γ is $i \times j$ -primitive, then $i \times j\text{-exp } \Gamma \leq u(r-1) + G(\hat{C}) + \rho(i, \tilde{U}(\hat{C})) + \theta(\tilde{U}(\hat{C}), j) - \sum_{s=1}^r (l_s + (s-2)\lambda_s) + 1$, where u is the number of vertices in U ; $\hat{C}$ is a primitive system of k directed cycles in U of lengths $l_1, \dots, l_k$; $\tilde{U}(\hat{C})$ is the set of vertices of digraph $U(\hat{C}) = \bigcup_{C \in \hat{C}} C$ which contains r connected components, $r \leq k$; λ_s is the sum

of lengths of directed cycles in the s -th connected component in $U(\hat{C})$, $s = 1, \dots, r$; $G(\hat{C}) = g(l_1, \dots, l_k)$ is Frobenius number; $\rho(i, J)$ is the least distance between i and a subset J of vertices; $\theta(J, j)$ is the least distance between J and j .

For i not being achievable from j , the graph Γ is $i \times j$ -primitive if and only if for some $d \in \mathbb{N}$ and subset P of the set of paths from i to j , the set $\text{spc } P$ is d -full, and for some $a \in \mathbb{Z}$, $\text{spc } W(i, j) \supseteq \text{spc } P + \mathbb{Z}(a, d)$, where $\text{spc } W(i, j)$ is the set of path lengths from i to j ; $\text{spc } P$ is the set of path lengths in P ; d -full set is the complete residue system modulo d ; $\mathbb{Z}(a, d) = \{z \in \mathbb{Z} : z = a + kd, k \in \mathbb{N}\}$; $\text{spc } P + \mathbb{Z}(a, d) = \{x + y : (x, y) \in \text{spc } P \times \mathbb{Z}(a, d)\}$. If Γ is $i \times j$ -primitive, then $i \times j\text{-exp } \Gamma \leq \xi_d(\text{spc } P) + a + d$, where $\xi_d(\text{spc } P)$ is the minimal number in $\mathbb{N}$ such that, for all $a \in \{\xi_d(\text{spc } P), \xi_d(\text{spc } P) + 1, \dots, \xi_d(\text{spc } P) + d - 1\}$, there is $b \in \text{spc } P$ that $b \leq a$ and b is congruent to a modulo d . By means of the result the derivation of $i \times j$ -primitiveness conditions and $i \times j$ -exponent estimations for various classes of digraphs is reduced to the estimation of appropriate numbers a and d . The results simplify local primitiveness recognition for concrete mixing digraphs of cryptographic transformations.

Keywords: $i \times j$ -primitiveness, $i \times j$ -exponent, digraph, strongly connected component.

Введение

Будем использовать следующие обозначения:

- $\mathbb{N}$ — множество натуральных чисел;
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$;
- $\mathbb{N}_n = \{1, \dots, n\}$;
- $\mathbb{Z}$ — множество целых чисел;
- $\mathbb{Z}_d$ — кольцо вычетов по модулю d , $d \in \mathbb{N}$;
- $\gcd(a_1, \dots, a_n)$ — наибольший общий делитель натуральных чисел $a_1, \dots, a_n$;
- $\text{lcm}(a_1, \dots, a_n)$ — наименьшее общее кратное 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 ;
- $\langle i, j \rangle$ — кратчайший путь в орграфе Γ из вершины i в вершину j ;
- $tC(i)$ — t -кратно пройденный контур C , начиная из вершины i ;
- $W(i, j)$ — множество путей в орграфе Γ из i в j ;
- $P(i, j)$ — множество простых путей в орграфе Γ из i в j ;
- $\cdot$ — операция конкатенации путей в орграфе;
- $\text{len } w$ — длина пути w в орграфе Γ , равная числу дуг, составляющих путь;
- $\text{spc } W = \{\text{len } w : w \in W\}$;
- $\text{spc}_d W = \{\text{len } w \bmod d : w \in W\}$, $d \in \mathbb{N}$;
- $\overline{\text{spc}}_d W = \mathbb{Z}_d \setminus \text{spc}_d W$, $d \in \mathbb{N}$;
- $\tilde{U}$ — множество вершин орграфа U .

В [1] получен универсальный критерий локальной примитивности орграфа и универсальная оценка локального экспонента. Применение этих результатов сопровождается определёнными трудностями, связанными с необходимостью иметь дело с моделью вычислений в самом общем виде. В связи с этим представляется практически целесообразным спроецировать критерий локальной примитивности на некоторые частные классы орграфов, возникающие в криптографических приложениях. Важно также, что упрощение критерия в ряде частных случаев позволяет уточнить универсальную оценку локального экспонента.

1. Определяющие свойства локально примитивных орграфов

Рассмотрим n -вершинный орграф Γ и напомним основные определения [1]. Пусть $I, J \subseteq N_n$. Орграф Γ называется $I \times J$ -примитивным, если существует такое $\gamma \in \mathbb{N}$, что для любых $(i, j) \in I \times J$ и любого $t \geq \gamma$ в Γ имеется путь длины t из i в j . Наименьшее такое γ называется $I \times J$ -экспонентом, или локальным экспонентом орграфа Γ , обозначается $I \times J$ -exp Γ (кратко $\gamma_{I \times J}$ или $\gamma_{i \times j}$ в случае $I = \{i\}$, $J = \{j\}$).

Из определения локальной примитивности следует:

- 1) если Γ является $I \times J$ -примитивным, то $W(i, j) \neq \emptyset$ для любых $(i, j) \in I \times J$;
- 2) орграф Γ является $I \times J$ -примитивным тогда и только тогда, когда Γ является $i \times j$ -примитивным для любых $(i, j) \in I \times J$, при этом $\gamma_{I \times J} = \max_{(i, j) \in I \times J} \gamma_{i \times j}$.

В орграфе Γ компонента сильной связности (ксс) U называется i, j -связывающей (кратко i, j -ксс), если в $\tilde{U}$ найдётся вершина, через которую проходит некоторый путь из $W(i, j)$. Будем говорить, что путь w :

- 1) проходит через контур, если он проходит через все дуги контура один или более раз;
- 2) касается контура, если он не проходит через контур, но проходит через некоторую вершину контура один или более раз;
- 3) проходит через систему контуров, если он проходит через каждый контур этой системы один или более раз.

Пусть $w = (i_0, i_1, \dots, i_t)$ — простой путь в орграфе Γ . Путь

$$e(w) = C_0(i_0) \cdot (i_0, i_1) \cdot C_1(i_1) \cdot \dots \cdot C_{t-1}(i_{t-1}) \cdot (i_{t-1}, i_t) \cdot C_t(i_t),$$

где $C_l(j)$ — контур (возможен пустой контур длины 0) в графе Γ , $l = 0, 1, \dots, t$, называется расширением пути w . Контур $C_0(i_0)$, $C_1(i_1)$, $\dots$, $C_t(i_t)$ называются расширяющими путь w . Дуги пути w являются дугами пути $e(w)$ и порядок их следования сохраняется. Таким образом, каждый непустой контур, расширяющий путь $w \in P(i, j)$, является частью некоторой i, j -ксс. Расширение $e(w)$ пути $w \in P(i, j)$, проходящее через непустую подсистему системы контуров $\hat{C}$, называется $\hat{C}$ -расширением пути w .

Утверждение 1.

- а) Если орграф $i \times j$ -примитивный, то он содержит i, j -ксс [2].
- б) Любой путь из $W(i, j)$ есть расширение некоторого пути из $P(i, j)$ [1].

В соответствии с утверждением 1, а свойство $i \times j$ -примитивности орграфа определяется бесконечным множеством чисел $\text{spr } W(i, j)$. В силу утверждения 1, б его можно описать с помощью конечного множества $\text{spr } P(i, j)$ и длин контуров, содержащихся в i, j -ксс.

Пусть $U^\rightarrow = (U_1, \dots, U_r)$ — последовательность ксс орграфа Γ , $r \in \mathbb{N}$. Обозначим u_s — множество вершин в ксс U_s ; d_s — наибольший общий делитель длин всех простых

контуров, содержащихся в ксс U_s , $s = 1, \dots, r$. Последовательность $U^\rightarrow$ назовём ксс-цепью длины r , если из вершин ксс U_{s-1} достижимы вершины ксс U_s , $s = 2, \dots, r$, при этом ксс $U_1, \dots, U_r$ называются звеньями ксс-цепи $U^\rightarrow$. Спецификацией ксс-цепи $U^\rightarrow$ назовём набор $(u_1, \dots, u_r) \in \mathbb{N}^r$. Индексом $\text{ind } U^\rightarrow$ ксс-цепи $U^\rightarrow$ назовём число $d = \gcd(d_1, \dots, d_r)$. Назовём $U^\rightarrow$ ксс-подцепью ксс-цепи $Z^\rightarrow$ и обозначим $U^\rightarrow \leq Z^\rightarrow$ ($U^\rightarrow < Z^\rightarrow$), если каждое звено ксс-цепи $U^\rightarrow$ есть звено ксс-цепи $Z^\rightarrow$ (и $U^\rightarrow \neq Z^\rightarrow$). В частности, ксс-цепь может быть цепью простых контуров.

В орграфе Γ ксс-цепь $U^\rightarrow$ назовём i, j -связывающей (кратко i, j -ксс-цепью), если из вершины i достижима ксс U_1 и из ксс U_r достижима вершина j . Если $U^\rightarrow$ есть i, j -ксс-цепь, то и любая её ксс-подцепь является i, j -ксс-цепью. Назовём i, j -ксс-цепь плотной, если не существует такой i, j -ксс-цепи $Z^\rightarrow$, что $U^\rightarrow < Z^\rightarrow$.

Наряду с i, j -ксс-цепями рассмотрим системы контуров в орграфе Γ , через которые проходят пути из i в j . Пусть $\hat{C} = \{C_1, \dots, C_k\}$ — система простых контуров длин $l_1, \dots, l_k$ соответственно. Индексом $\text{ind } \hat{C}$ системы контуров $\hat{C}$ назовём число $d = \gcd(l_1, \dots, l_k)$.

Утверждение 2 [1, теорема 2б]. Пусть путь $w \in P(i, j)$ в орграфе Γ проходит через i, j -ксс-цепь, содержащую систему контуров $\hat{C}$ индекса d , тогда

$$\text{len } e(w) \equiv \text{len } w \pmod{d}$$

для любого $\hat{C}$ -расширения $e(w)$ пути w .

При $r > 1$ множество ксс $\hat{U} = \{U_1, \dots, U_r\}$ орграфа Γ назовём ксс-антицепью порядка r , если из любой ксс множества $\hat{U}$ недостижимы вершины любой другой ксс множества $\hat{U}$. Спецификацией ксс-антицепи $\hat{U}$ назовём набор $(u_1, \dots, u_r)$. Индексом $\text{ind } \hat{U}$ ксс-антицепи $\hat{U}$ назовём число $d = \text{lcm}(d_1, \dots, d_r)$. Назовём ксс-антицепь i, j -связывающей в Γ (кратко i, j -ксс-антицепью), если U_s есть i, j -ксс, $s = 1, \dots, r$.

2. Условия локальной примитивности и оценки локального экспонента

Получим условия $i \times j$ -примитивности и оценки $i \times j$ -экспонентов орграфа в следующих случаях:

- вершины i, j взаимно достижимы;
- вершины i, j не принадлежат общей ксс и Γ содержит
 - i, j -ксс-цепь;
 - i, j -ксс-антицепь.

2.1. Вершины i и j взаимно достижимы

Пусть U — ксс орграфа Γ с множеством вершин порядка u .

Утверждение 3. Если $i, j \in \tilde{U}$, то $i \times j$ -примитивность ксс U и $i \times j$ -примитивность орграфа Γ равносильны примитивности ксс U .

Доказательство.

Достаточность следует из определения примитивности орграфа.

Необходимость. Пусть орграф Γ (ксс U) является $i \times j$ -примитивным при некоторых $i, j \in \tilde{U}$. Тогда в Γ имеется путь $w_t \in W(i, j)$ длины t при любом $t \geq \gamma_{i \times j}$. Отсюда для любых вершин α, β ксс U имеется путь $[\alpha, \beta] = [\alpha, i] \cdot w_t \cdot [j, \beta]$ длины $\text{len} \langle \alpha, i \rangle + t + \text{len} \langle j, \beta \rangle$ при любом $t \geq \gamma_{i \times j}$. Следовательно, ксс U примитивная, так как в U любая вершина достижима из любой за t шагов при любом $t \geq \gamma_{i \times j} + 2d$, где d — диаметр ксс U . ■

Обозначим $g(l_1, \dots, l_k)$ — число Фробениуса, где $\gcd(l_1, \dots, l_k) = 1$ (при $k > 1$ наибольшее число, не принадлежащее аддитивной полугруппе $\langle l_1, \dots, l_k \rangle$, порождённой натуральными взаимно простыми числами $l_1, \dots, l_k$; $g(1) = -1$).

Утверждение 4. Если $\gcd(l_1, \dots, l_k) = d$, то для любого $t \in \mathbb{N}$ существуют такие целые неотрицательные числа $a_1, \dots, a_k$, что $a_1 l_1 + \dots + a_k l_k = dg(l_1/d, \dots, l_k/d) + dt$.

Доказательство. Поскольку $\gcd(l_1, \dots, l_k) = d$, то $\gcd(l_1/d, \dots, l_k/d) = 1$. По определению числа Фробениуса любое натуральное число, большее $g(l_1/d, \dots, l_k/d)$, есть линейная комбинация чисел $l_1/d, \dots, l_k/d$ с некоторыми целыми неотрицательными коэффициентами $a_1, \dots, a_k$. Значит, подбирая данные коэффициенты, можно для любого $t \in \mathbb{N}$ получить равенство $a_1 l_1 + \dots + a_k l_k = dg(l_1/d, \dots, l_k/d) + dt$. ■

Для непустой системы простых контуров $\hat{C} = \{C_1, \dots, C_k\}$ длин $l_1, \dots, l_k$ соответственно обозначим $G(\hat{C}) = dg(l_1/d, \dots, l_k/d)$, где $d = \text{ind } \hat{C}$.

В примитивной ксс U имеется [3, с. 226] система контуров $\hat{C} = \{C_1, \dots, C_k\}$, где $l_1 < \dots < l_k$, $\text{ind } \hat{C} = 1$. Получим оценку локального экспонента с использованием системы контуров $\hat{C}$.

Рассмотрим орграф $U(\hat{C}) = C_1 \cup \dots \cup C_k$ (не обязательно связный), являющийся частью орграфа U . Обозначим: $\hat{C}_s$ — компонента связности орграфа $U(\hat{C})$; λ_s — сумма длин контуров системы $\hat{C}$, образующих $\hat{C}_s$, $s = 1, \dots, r$, где $1 \leq r \leq k$, $\lambda_1 \geq \dots \geq \lambda_r$; $\rho(i, J)$ — кратчайшее расстояние от вершины i до некоторой вершины множества вершин J ; $\theta(I, j)$ — расстояние достижимости вершины j из любой вершины множества вершин I .

Следствие 1. Если ксс U примитивная, то для $i, j \in \tilde{U}$

$$\gamma_{i \times j} \leq u(r-1) + G(\hat{C}) + \rho(i, \tilde{U}(\hat{C})) + \theta(\tilde{U}(\hat{C}), j) - \sum_{s=1}^r (l_s + (s-1)\lambda_s) + 1.$$

Доказательство. По утверждению 3 орграф Γ является $i \times j$ -примитивным, так как ксс U примитивная. Оценку $\gamma_{i \times j}$ получим с помощью уточнения универсальной оценки В. М. Фомичева экспонентов орграфов [4, теорема 1]:

$$\exp U \leq u(r+1) + g(l_1, \dots, l_k) - \sum_{s=1}^r (l_s + (s-1)\lambda_s).$$

При доказательстве этой оценки построены пути $w \in W(i, j)$ вида

$$w = \langle i, \alpha_1 \rangle \cdot [\alpha_1, \alpha_r] \cdot \langle \alpha_r, j \rangle,$$

где $\langle i, \alpha_1 \rangle$ и $\langle \alpha_r, j \rangle$ — кратчайшие пути в U соответственно от вершины i до ближайшей вершины α_1 орграфа $U(\hat{C})$ и от некоторой вершины α_r орграфа $U(\hat{C})$ до вершины j . При этом использованы оценки $\text{len} \langle i, \alpha_1 \rangle \leq u - \lambda_1 - \dots - \lambda_r$ и $\text{len} \langle \alpha_r, j \rangle \leq u - 1$, которые в данном случае можно заменить на более точные оценки $\text{len} \langle i, \alpha_1 \rangle \leq \rho(i, \tilde{U}(\hat{C}))$ и $\text{len} \langle \alpha_r, j \rangle \leq \theta(\tilde{U}(\hat{C}), j)$. Следовательно, приведённая оценка верна. ■

Следствие 2. Если ксс U примитивная и орграф $U(\hat{C})$ связный, то для $i, j \in \tilde{U}$

$$\gamma_{i \times j} \leq G(\hat{C}) + \rho(i, \tilde{U}(\hat{C})) + \theta(\tilde{U}(\hat{C}), j) + \sum_{s=2}^k l_s + 1.$$

Доказательство. В оценке следствия 1 следует положить $r = 1$. ■

2.2. Вершина i недостижима из вершины j

Без ущерба для общности положим, что вершины i, j не принадлежат i, j -ксс.

Пусть $d \in \mathbb{N}$, $\emptyset \neq Y \subset \mathbb{Z}$. Множество Y , содержащее полную систему вычетов по модулю d , называется d -полным.

Замечание 1. d -Полнота множества равносильна d -полноте некоторого его подмножества.

Для d -полного множества Y обозначим $\xi_d(Y)$ — наименьшее натуральное число, такое, что для всех $a \in \{\xi_d(Y), \xi_d(Y) + 1, \dots, \xi_d(Y) + d - 1\}$ в Y имеется число $b \leq a$, сравнимое с a по модулю d (в частности, $\xi_1(Y) = \min Y$); Y_d — наименьший d -трансверсал множества Y , то есть подмножество, состоящее из наименьших чисел множества Y , образующих полную систему вычетов по модулю d .

Лемма 1. Для d -полного множества Y выполнено: $\xi_d(Y) = \max Y_d - d + 1$.

Доказательство. Пусть $\sigma = \max Y_d$. По определению множества Y_d для любого $a \in \{\sigma, \sigma - 1, \dots, \sigma - d + 1\}$ в Y имеется число $b \leq a$, сравнимое с a по модулю d . Отсюда $\xi_d(Y) \leq \sigma - d + 1$. Вместе с тем все числа, меньшие σ и сравнимые с σ по модулю d , не принадлежат Y . Значит, $\xi_d(Y) > \sigma - d$. Следовательно, $\xi_d(Y) = \sigma - d + 1$. ■

Для подмножеств $X, Y \subseteq \mathbb{Z}$ определим $X + Y = \{x + y : (x, y) \in X \times Y\}$. При $a \in \mathbb{Z}$ обозначим $Y(a, d)$ подмножество чисел из Y , сравнимых с a по модулю d и превышающих a , то есть $Y(a, d) = \{y \in Y : y = a + kd, k \in \mathbb{N}\}$.

Для рассматриваемого в данном разделе класса орграфов получим критерий локальной примитивности, который удобен для распознавания локальной примитивности орграфов, возникающих в ряде криптографических приложений.

Лемма 2. Орграф Γ является $i \times j$ -примитивным тогда и только тогда, когда при некотором $d \in \mathbb{N}$ множество $\text{spc } P(i, j)$ является d -полным и при некотором $a \in \mathbb{Z}$

$$\text{spc } W(i, j) \supseteq \text{spc } P(i, j) + \mathbb{Z}(a, d). \quad (1)$$

Если $P \subseteq P(i, j)$, множество $\text{spc } P$ является d -полным при некотором $d \in \mathbb{N}$ и $\text{spc } W(i, j) \supseteq \text{spc } P + \mathbb{Z}(a, d)$ при некотором $a \in \mathbb{Z}$, то орграф Γ является $i \times j$ -примитивным и $\gamma_{i \times j} \leq \xi_d(\text{spc } P) + a + d$. Эта оценка достигается, если

$$\text{spc } W(i, j) = \text{spc } P(i, j) + \mathbb{Z}(a, d). \quad (2)$$

Доказательство. Необходимость. Если Γ является $i \times j$ -примитивным, то при некотором $\gamma \in \mathbb{N}$ для любого $t \geq \gamma$ в $W(i, j)$ имеется путь длины t . Тогда в соответствии с принятыми обозначениями

$$\text{spc } W(i, j) \supseteq \mathbb{Z}(\gamma - 1, 1). \quad (3)$$

Отсюда множество $\text{spc } P(i, j)$ является d -полным при некотором $d \in \mathbb{N}$, поскольку в противном случае $\text{spc } P(i, j)$ при некотором $b \in \mathbb{Z}_d$ не содержит чисел, сравнимых с b по модулю d , тогда в силу утверждений 1, 6 и 2 в орграфе Γ не существует пути $w \in W(i, j)$, длина которого сравнима с b по модулю d , что противоречит (1). Тогда с учётом (3) включение (1) верно при $a = \gamma - d - l_0$, где l_0 — длина кратчайшего пути $w \in W(i, j)$.

Достаточность докажем для любого d -полного подмножества $P \subseteq P(i, j)$. Пусть $\text{spc } W(i, j) \supseteq \text{spc } P + \mathbb{Z}(a, d)$ при некоторых $d \in \mathbb{N}$ и $a \in \mathbb{Z}$. Тогда множество $\text{spc } W(i, j)$ также является d -полным и содержит все натуральные числа $t \geq \xi_d(\text{spc } P) + a + d$. Значит, орграф Γ является $i \times j$ -примитивным и $\gamma_{i \times j} \leq \xi_d(\text{spc } P) + a + d$.

Точность оценки. Пусть верно (2) и $\xi_d(\text{spc } P(i, j)) = p$. Если в Γ имеется путь $w \in W(i, j)$ длины $p + a + d - 1$, то $(p - 1) \in \text{spc } P(i, j)$ в силу (2), что противоречит равенству $\xi_d(\text{spc } P(i, j)) = p$. Следовательно, $\gamma_{i \times j} = \xi_d(\text{spc } P(i, j)) + a + d$. ■

Пусть далее $\hat{C} = \{C_1, \dots, C_k\}$ — непустая система простых контуров длин $l_1, \dots, l_k$ соответственно, $l_1 < \dots < l_k$.

Рассмотрим ксс U с множеством вершин порядка u , содержащую систему $\hat{C}$. В общем случае граф $U(\hat{C})$ имеет несколько компонент связности, обозначим их $U_1(\hat{C}), \dots, U_\tau(\hat{C})$, $\tau \leq k$. В [4] показано:

- 1) в компоненте связности $U_t(\hat{C})$ имеется контур Z_t длины λ_t , проходящий через подсистему всех контуров из $\hat{C}$, принадлежащих компоненте связности $U_t(\hat{C})$, $t = 1, \dots, \tau$;
- 2) длина λ_t контура Z_t равна сумме длин всех контуров из $\hat{C}$, принадлежащих компоненте связности $U_t(\hat{C})$, $t = 1, \dots, \tau$;
- 3) в ксс U имеется контур $Z(U, \hat{C})$, проходящий через систему контуров $\hat{C}$, где

$$\text{len } Z(U, \hat{C}) \leq u(\tau + 1) - \sum_{t=1}^{\tau} (l_t + (t-1)\lambda_t) \quad (4)$$

и $\lambda_1 \geq \dots \geq \lambda_\tau$. С помощью этих результатов оценим локальные экспоненты графов.

С л у ч а й 1. Γ содержит i, j -ксс-цепь.

Пусть i, j -ксс-цепь $U^\rightarrow = (U_1, \dots, U_r)$, имеющая спецификацию $(u_1, \dots, u_r)$, содержит систему контуров $\hat{C}$, где $\hat{C}_s$ — подсистема контуров системы $\hat{C}$, принадлежащих ксс U_s , $s = 1, \dots, r$, $1 \leq r \leq k$. Обозначим $L(U^\rightarrow, \hat{C}) = \sum_{s=1}^r \text{len } Z(U_s, \hat{C}_s)$.

Путь $w \in P(i, j)$ назовём ассоциированным с системой $\hat{C}$, если w проходит через все ксс, содержащие контуры из $\hat{C}$. Подмножество путей из $P(i, j)$, ассоциированных с системой контуров $\hat{C}$, обозначим $P_{\hat{C}}(i, j)$.

Лемма 3. Пусть в орграфе Γ имеется i, j -ксс-цепь $U^\rightarrow$, содержащая систему контуров $\hat{C}$ индекса d , тогда $\text{src } W(i, j) \supseteq \text{src } P_{\hat{C}}(i, j) + \mathbb{Z}(a, d)$, где

$$a = G(\hat{C}) + L(U^\rightarrow, \hat{C}). \quad (5)$$

Доказательство. Пусть $w \in P_{\hat{C}}(i, j)$. Тогда $\hat{C}$ -расширение $e(w)$ пути w представимо в виде

$$e(w) = [i, \alpha_1] \cdot Z'_1(\alpha_1) \cdot [\alpha_1, \alpha_2] \cdot Z'_2(\alpha_2) \cdot [\alpha_2, \alpha_3] \cdot \dots \cdot [\alpha_{r-1}, \alpha_r] \cdot Z'_r(\alpha_r) \cdot [\alpha_r, j],$$

где α_s — вершина ксс U_s , через которую проходит путь w ; Z'_s — контур в ксс U_s , проходящий через контуры системы $\hat{C}_s$ некоторое число раз, $s = 1, \dots, r$. Пусть без ущерба для общности $\hat{C}_1 = \{C_1, \dots, C_m\}$, $m \leq k$, и Z'_1 проходит через контуры $a_1, \dots, a_m$ раз соответственно. Тогда $\text{len } Z'_1 = a_1 l_1 + \dots + a_m l_m + \text{len } Z(U_1, \hat{C}_1)$ и

$$\sum_{s=1}^r \text{len } Z'_s = a_1 l_1 + \dots + a_k l_k + \sum_{s=1}^r \text{len } Z(U_s, \hat{C}_s).$$

Поскольку $\gcd(l_1, \dots, l_k) = d$, по утверждению 4 для любого $t \in \mathbb{N}$ имеются такие $a_1, \dots, a_k \in \mathbb{N}_0$, что $a_1 l_1 + \dots + a_k l_k = dg(l_1/d, \dots, l_k/d) + dt = G(\hat{C}) + dt$. Таким образом, длина $\hat{C}$ -расширения $e_t(w)$ пути w для любого $t \in \mathbb{N}$ при подходящих $a_1, \dots, a_k$ равна

$$\text{len } e_t(w) = \text{len } w + \sum_{s=1}^r \text{len } Z'_s = \text{len } w + G(\hat{C}) + L(U^\rightarrow, \hat{C}) + dt.$$

Следовательно, для любого $t \in \mathbb{N}$ имеется расширение $e_t(w)$ пути $w \in P_{\hat{C}}(i, j)$ длины $\text{len } w + a + dt$. Учитывая утверждение 1, б, получаем

$$\text{spc } W(i, j) \supseteq \text{spc } P_{\hat{C}}(i, j) + a + d\mathbb{N},$$

то есть лемма верна. ■

Теорема 1. Если в орграфе Γ имеется i, j -ксс-цепь $U^{\rightarrow}$, содержащая систему контуров $\hat{C}$ индекса d , и множество $\text{spc } P_{\hat{C}}(i, j)$ является d -полным, то Γ является $i \times j$ -примитивным и $\gamma_{i \times j} \leq \xi_d(\text{spc } P_{\hat{C}}(i, j)) + a + d$, где a определяется (5).

Доказательство. Следует из лемм 2 и 3. ■

Итак, получены достаточное условие $i \times j$ -примитивности орграфа Γ , содержащего i, j -ксс-цепь (наличие других i, j -ксс возможно), и оценка $i \times j$ -экспонента в этом случае. Для некоторых частных случаев получим критерий $i \times j$ -примитивности и уточним оценку $i \times j$ -экспонента.

Пусть $U'^{\rightarrow}$ — единственная плотная i, j -ксс-цепь в орграфе Γ , то есть любая ксс, через которую проходит путь из $P(i, j)$, содержится в $U'^{\rightarrow}$ (рис. 1). Обозначим $\Omega(U'^{\rightarrow})$ — множество всех непустых подцепей цепи $U'^{\rightarrow}$.

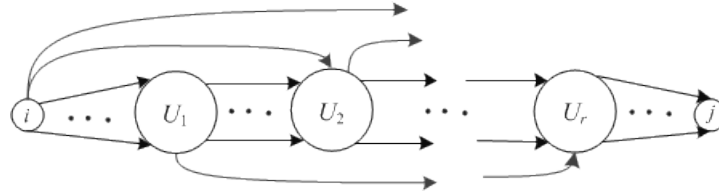


Рис. 1. i, j -ксс-цепь $U'^{\rightarrow} = (U_1, \dots, U_r)$

Следствие 3. Если $U'^{\rightarrow}$ — единственная плотная i, j -ксс-цепь в орграфе Γ , то Γ является $i \times j$ -примитивным тогда и только тогда, когда некоторая подцепь $U^{\rightarrow} \in \Omega(U'^{\rightarrow})$ содержит такую систему контуров $\hat{C}$ индекса d , что множество $\text{spc } P_{\hat{C}}(i, j)$ является d -полным.

Доказательство. По лемме 3 для любой подцепи $U^{\rightarrow} \in \Omega(U'^{\rightarrow})$ и любой содержащейся в ней системы контуров $\hat{C}$ индекса d справедливо

$$\text{spc } W(i, j) \supseteq \text{spc } P_{\hat{C}}(i, j) + \mathbb{Z}(a, d),$$

где a определяется (5). Согласно лемме 2 и замечанию 1, орграф Γ является $i \times j$ -примитивным тогда и только тогда, когда для некоторого d множество $\text{spc } P_{\hat{C}}(i, j)$ является d -полным. ■

Рассмотрим случай, когда Γ содержит i, j -ксс-цепь, обозначаемую $U_{\vec{C}}^{\rightarrow}$, звеньями которой являются простые контуры $C_1, \dots, C_r$ длин $l_1, \dots, l_r$ соответственно.

Утверждение 5. Если в орграфе Γ имеется i, j -ксс-цепь $U_{\vec{C}}^{\rightarrow}$ и существует такое подмножество $\hat{C} \subseteq U_{\vec{C}}^{\rightarrow}$, что множество $\text{spc } P_{\hat{C}}(i, j)$ является d -полным, где $d = \text{ind } \hat{C}$, то Γ является $i \times j$ -примитивным и $\gamma_{i \times j} \leq \xi_d(\text{spc } P_{\hat{C}}(i, j)) + G(\hat{C}) + d$.

Доказательство. Пусть $k = 2$. Любое расширение пути $w \in \text{spc } P_{\hat{C}}(i, j)$ проходит через вершины контуров C_1, C_2 и представимо в виде

$$e_{a_1, a_2}(w) = [i, \alpha_1] \cdot a_1 C_1(\alpha_1) \cdot [\alpha_1, \alpha_2] \cdot a_2 C_2(\alpha_2) \cdot [\alpha_2, j],$$

где α_s — вершина контура C_s , через которую проходит путь w , $s = 1, 2$, $a_1, a_2 \in \mathbb{N}_0$.

Поскольку $d = \gcd(l_1, l_2)$, по утверждению 4 расширение $e_{a_1, a_2}(w)$, обходящее контуры C_1 и C_2 соответственно a_1 и a_2 раз, имеет длину $\text{len } w + G(\hat{C}) + dt$, где $t \in \mathbb{N}$. Учитывая утверждение 1, б, $\text{spc } W(i, j) \supseteq \text{spc } P_{\hat{C}}(i, j) + G(\hat{C}) + d\mathbb{N}$, то есть

$$\text{spc } W(i, j) \supseteq \text{spc } P_{\hat{C}}(i, j) + \mathbb{Z}(a, d)$$

при $a = G(\hat{C})$. Поскольку множество $\text{spc } P_{\hat{C}}(i, j)$ является d -полным, по лемме 2 орграф Γ является $i \times j$ -примитивным и $\gamma_{i \times j} \leq \xi_d(\text{spc } P_{\hat{C}}(i, j)) + G(\hat{C}) + d$.

Обобщение для $k > 2$ очевидно. ■

Пусть $U_{\vec{C}} \rightarrow$ — единственная плотная i, j -ксс-цепь в орграфе Γ , то есть любой контур, через который проходит путь из $P(i, j)$, содержится в $U_{\vec{C}} \rightarrow$ (аналогично рис. 1). Для такого случая аналогично следствию 3 можно получить критерий $i \times j$ -примитивности.

Следствие 4. Если $U_{\vec{C}} \rightarrow$ — единственная плотная i, j -ксс-цепь в орграфе Γ , то Γ является $i \times j$ -примитивным тогда и только тогда, когда существует такое $\hat{C} \subseteq U_{\vec{C}} \rightarrow$, что множество $\text{spc } P_{\hat{C}}(i, j)$ является d -полным, где $d = \text{ind } \hat{C}$.

Замечание 2. Если $U_{\vec{C}} \rightarrow$ — единственная плотная i, j -ксс-цепь в орграфе Γ и любой путь из $P(i, j)$ проходит через все ксс из цепи $U_{\vec{C}} \rightarrow$, то множество $P(i, j)$ совпадает с множеством $P_{\hat{C}}(i, j)$ для любой системы контуров $\hat{C} \subseteq U_{\vec{C}} \rightarrow$. В таком случае $i \times j$ -примитивность Γ равносильна d -полноте множества $\text{spc } P(i, j)$, где $d = \text{ind } U_{\vec{C}} \rightarrow$.

Пусть для определённости $\hat{C} = U_{\vec{C}} \rightarrow$. Получим точное значение $i \times j$ -экспонента для данного случая.

Следствие 5. Если $U_{\vec{C}} \rightarrow$ — единственная плотная i, j -ксс-цепь в орграфе Γ и любой путь из $P(i, j)$ проходит через все ксс из цепи $U_{\vec{C}} \rightarrow$, то в случае $i \times j$ -примитивности Γ имеет место $\gamma_{i \times j} = \xi_d(\text{spc } P(i, j)) + G(\hat{C}) + d$, где $d = \text{ind } U_{\vec{C}} \rightarrow$.

Доказательство. Любое расширение $e(w)$ пути $w \in P(i, j)$ проходит через вершины всех контуров $C_1, \dots, C_r$ и по утверждению 4 имеет длину $\text{len } w + dg(l_1/d, \dots, l_r/d) + dt$, где $t \in \mathbb{N}$. Тогда, согласно утверждению 1, б, $\text{spc } W(i, j) = \text{spc } P(i, j) + \mathbb{Z}(a, d)$ при $a = G(\hat{C})$. В соответствии с леммой 2 следствие верно. ■

Пример 1. Рассмотрим орграф Γ_1 , изображённый на рис. 2. Покажем его 1×7 -примитивность.

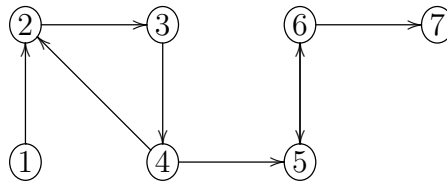


Рис. 2. Орграф Γ_1

В графе имеется единственная плотная $1, 7$ -ксс-цепь (C_1, C_2) , где $\tilde{C}_1 = \{2, 3, 4\}$, $\tilde{C}_2 = \{5, 6\}$. Используя введённые обозначения, получим: $r = 2$, $l_1 = 3$, $l_2 = 2$, $d = \gcd(3, 2) = 1$, $\text{spc } P(i, j) = \{6\}$. Поскольку $\text{spc } P(i, j)$ является 1 -полным, то, согласно следствию 4 (замечанию 2), орграф Γ_1 является 1×7 -примитивным, и по следствию 5 имеем $1 \times 7\text{-exp } \Gamma_1 = g(3, 2) + 1 + \xi_1(\text{spc } P(i, j)) = 8$.

Пусть в орграфе Γ имеется единственная i -вершинная i, j -ксс U . В общем случае можно воспользоваться теоремой 1 и следствием 3, положив $r = 1$.

Следствие 6. Если в орграфе Γ имеется единственная i, j -ксс U , то Γ является $i \times j$ -примитивным тогда и только тогда, когда U содержит такую систему контуров $\hat{C}$ индекса d , что множество $\text{spr } P(i, j)$ является d -полным, при этом $\gamma_{i \times j} \leq \xi_d(\text{spr } P(i, j)) + a + d$, где

$$a = G(\hat{C}) + \text{len } Z(U, \hat{C}). \quad (6)$$

Получим критерии $i \times j$ -примитивности и точные значения $i \times j$ -экспонента для некоторых частных случаев орграфов, содержащих единственную i, j -ксс U .

Пусть U состоит лишь из контуров системы $\hat{C}$. Рассмотрим случай, когда контуры C_s, C_t имеют одну общую вершину лишь при $t = s + 1, s = 1, \dots, k - 1$, и все пути из $P(i, j)$ проходят через вершины всех контуров $C_1, \dots, C_k$. Обозначим такой граф $\Gamma^{(1)}$ (рис. 3).

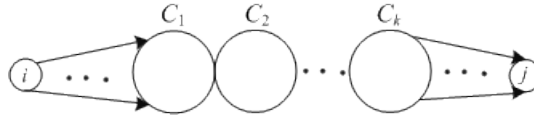


Рис. 3. Орграф $\Gamma^{(1)}$

В графе $\Gamma^{(1)}$ любое расширение пути $w \in P(i, j)$ проходит через вершины всех контуров $C_1, \dots, C_k$ и по утверждению 4 имеет длину $\text{len } w + G(\hat{C}) + dt$, где $t \in \mathbb{N}$. Следовательно, критерий $i \times j$ -примитивности и оценка $i \times j$ -экспонента графа $\Gamma^{(1)}$ определяются следствием 4 (замечанием 2) и следствием 5.

Пример 2. Рассмотрим орграф Γ_2 , изображённый на рис. 4. Покажем его 1×7 -примитивность.

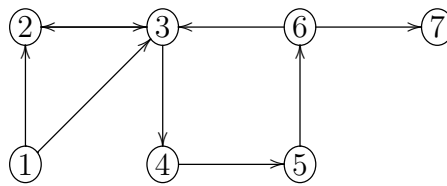
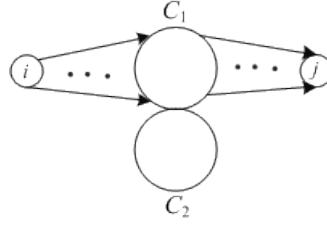


Рис. 4. Орграф Γ_2

В графе имеется единственная $1, 7$ -ксс, состоящая из двух простых контуров $C_1 = \{2, 3\}$, $C_2 = \{3, 4, 5, 6\}$. Используя введённые обозначения, получим $l_1 = 2$, $l_2 = 4$, $d = \gcd(2, 4) = 2$, $\text{spr } P(i, j) = \{5, 6\}$. Множество $\text{spr } P(i, j)$ является 2 -полным, и по лемме 1 $\xi_2(\text{spr } P(i, j)) = 5$. Согласно следствию 4 (замечанию 2), орграф Γ_2 является 1×7 -примитивным, и по следствию 5 имеем $1 \times 7\text{-exp } \Gamma_2 = 2(g(1, 2) + 1) + \xi_2(\text{spr } P(i, j))$. Поскольку $g(1, 2) = -1$, то $1 \times 7\text{-exp } \Gamma_2 = 5$.

Пусть теперь $\hat{C} = \{C_1, C_2\}$, причём контуры имеют одну общую вершину, пути из вершины i в вершины контура C_2 и из вершин контура C_2 в вершину j проходят через вершины контура C_1 . Обозначим такой граф $\Gamma^{(2)}$ (рис. 5).

Рис. 5. Оргграф $\Gamma^{(2)}$

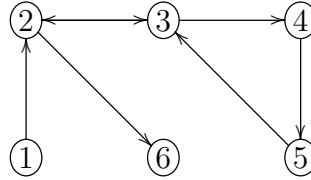
Следствие 7. Оргграф $\Gamma^{(2)}$ является $i \times j$ -примитивным тогда и только тогда, когда множество $\text{spr } P(i, j)$ является d -полным, где $d = \gcd(l_1, l_2)$, в случае $i \times j$ -примитивности $\gamma_{i \times j} = \xi_d(\text{spr } P(i, j)) + G(\hat{C}) + d + l_1$.

Доказательство. Пусть α_1 — ближайшая к i вершина контура C_1 , через которую проходит путь $w \in P(i, j)$, тогда w можно представить конкатенацией $w = [i, \alpha_1] \cdot [\alpha_1, j]$. Любое расширение пути w проходит через вершины контуров C_1 и C_2 . Расширение $e_{a_1, a_2}(w)$, обходящее контуры соответственно a_1 и a_2 раз, $a_1, a_2 \in \mathbb{N}_0$, представимо в виде

$$e_{a_1, a_2}(w) = [i, \alpha_1] \cdot a_1 C_1(\alpha_1) \cdot \langle \alpha_1, \alpha_2 \rangle \cdot a_2 C_2(\alpha_2) \cdot \langle \alpha_2, \alpha_1 \rangle \cdot [\alpha_1, j],$$

где α_2 — общая вершина контуров C_1 и C_2 . Поскольку $\langle \alpha_1, \alpha_2 \rangle \cdot \langle \alpha_2, \alpha_1 \rangle = C_1$ и $d = \gcd(l_1, l_2)$, по утверждению 4 расширение $e_{a_1, a_2}(w)$ имеет длину $\text{len } w + G(\hat{C}) + l_1 + dt$, $t \in \mathbb{N}$. Таким образом, по утверждению 1, б $\text{spr } W(i, j) = \text{spr } P(i, j) + \mathbb{Z}(a, d)$ при $a = G(\hat{C}) + l_1$. Согласно лемме 2 и замечанию 1, следствие верно. ■

Пример 3. Рассмотрим оргграф Γ_3 , изображённый на рис. 6. Покажем его 1×6 -примитивность.

Рис. 6. Оргграф Γ_3

В графе имеется единственная $1, 6$ -ксс, состоящая из двух простых контуров $C_1 = \{2, 3\}$, $C_2 = \{3, 4, 5\}$, причём Γ_3 обладает свойствами графа $\Gamma^{(2)}$. Используя введённые обозначения, получим $l_1 = 2$, $l_2 = 3$, $d = \gcd(2, 3) = 1$, $\text{spr } P(i, j) = \{2\}$. Поскольку $\text{spr } P(i, j)$ является 1 -полным, согласно следствию 7, оргграф Γ_3 является 1×6 -примитивным и 1×6 -ехр $\Gamma_3 = g(2, 3) + 1 + 2 + \xi_1(\text{spr } P(i, j))$. Поскольку $g(2, 3) = 1$, то 1×6 -ехр $\Gamma_3 = 6$.

Наконец, рассмотрим наиболее простой случай: единственная i, j -ксс представляет собой один простой контур.

Лемма 4. Если в оргграфе Γ имеется единственная i, j -ксс, представляющая собой простой контур C длины l , то $\text{spr } W(i, j) = \text{spr } P(i, j) + l\mathbb{N}_0$.

Доказательство. Любое расширение пути $w \in P(i, j)$ проходит через вершины контура C . Расширение $e_t(w)$, обходящее t -кратно контур C , представимо как

конкатенация $e_t(w) = [i, \mu] \cdot tC(\mu) \cdot [\mu, j]$, где μ — вершина контура C , принадлежащая пути w , $t \in \mathbb{N}_0$. Отсюда $\text{len } e_t(w) = \text{len } w + lt$, и с учётом утверждения 1,6 $\text{sprc } W(i, j) = \text{sprc } P(i, j) + l\mathbb{N}_0$. ■

Следствие 8. Если в орграфе Γ имеется единственная i, j -ксс, представляющая собой простой контур C длины l , то Γ является $i \times j$ -примитивным тогда и только тогда, когда множество $\text{sprc } P(i, j)$ является l -полным, в случае $i \times j$ -примитивности $\gamma_{i \times j} = \xi_l(\text{sprc } P(i, j))$.

Доказательство. Следует из лемм 2, 4. ■

С л у ч а й 2. Γ содержит i, j -ксс-антицепь.

Пусть i, j -ксс-антицепь $\hat{U} = \{U_1, \dots, U_r\}$ (рис. 7) имеет спецификацию $(u_1, \dots, u_r)$, $2 \leq r \leq k$. Тогда верны разбиения

$$W(i, j) = W_1(i, j) \cup \dots \cup W_r(i, j); \quad P(i, j) = P_1(i, j) \cup \dots \cup P_r(i, j),$$

где $W_s(i, j)$ ($P_s(i, j)$) — подмножество путей из $W(i, j)$ ($P(i, j)$), проходящих через ксс U_s , $s = 1, \dots, r$.

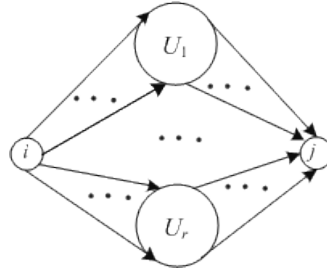


Рис. 7. i, j -ксс-антицепь $\hat{U} = \{U_1, \dots, U_r\}$

Обозначим: $\hat{C}_s$ — множество всех простых контуров ксс U_s ; $d_s = \text{ind } \hat{C}_s$, $s = 1, \dots, r$; $\delta = \text{ind } \hat{U} = \text{lcm}(d_1, \dots, d_r)$; $H(P(i, j)) = \overline{\text{sprc}}_{d_1}(P_1(i, j)) \times \dots \times \overline{\text{sprc}}_{d_r}(P_r(i, j))$;

$$\Psi(\hat{U}) = \bigcup_{s=1}^r \left(\text{sprc } P_s(i, j) + \bigcup_{\theta=1}^{\delta/d_s} \{a_s + d_s \theta\} \right),$$

где a_s определяется (6) при $U = U_s$, $\hat{C} = \hat{C}_s$, $s = 1, \dots, r$.

Если хотя бы одно из множеств $\text{sprc}_{d_s} P_s(i, j)$ является d_s -полным, $s \in \mathbb{N}_r$, то по теореме 1 орграф Γ является $i \times j$ -примитивным. В противном случае множество $H(P(i, j))$ непусто.

Лемма 5 [1]. Для любого $(b_1, \dots, b_r) \in H(P(i, j))$ множество решений системы

$$\{x \equiv b_s \pmod{d_s}, \quad s = 1, \dots, r\} \quad (7)$$

есть множество чисел, не содержащихся в множестве длин путей из $P(i, j)$.

Теорема 2. Если орграф Γ содержит i, j -ксс-антицепь $\hat{U}$ и для любого $(b_1, \dots, b_r) \in H(P(i, j))$ система (7) не имеет решений по модулю δ , то Γ является $i \times j$ -примитивным, в случае $i \times j$ -примитивности $\gamma_{i \times j} \leq \xi_\delta(\Psi(\hat{U}))$.

Доказательство. Из леммы 5 следует, что при отсутствии решений системы (7) орграф Γ является $i \times j$ -примитивным.

Оценим величину $\gamma_{i \times j}$. Согласно лемме 3, $\text{spc } W_s(i, j) \supseteq \text{spc } P_s(i, j) + a_s + d_s \mathbb{N}$, где a_s определяется (6) при $U = U_s$, $\hat{C} = \hat{C}_s$, $s = 1, \dots, r$.

Обозначим $\Lambda_s = \text{spc } P_s(i, j) + a_s + d_s \mathbb{N}$, $s = 1, \dots, r$. Поскольку $\delta = \text{lcm}(d_1, \dots, d_r)$, в силу $i \times j$ -примитивности Γ множество $\Lambda_1 \cup \dots \cup \Lambda_r$ является δ -полным. Для любого $s = 1, \dots, r$ верно

$$\Lambda_s = \text{spc } P_s(i, j) + \bigcup_{\theta=1}^{\delta/d_s} \{a_s + d_s \theta\} + \delta \mathbb{N}_0.$$

Тогда $\Lambda_1 \cup \dots \cup \Lambda_r = \Psi(\hat{U}) + \delta \mathbb{N}_0$. Следовательно, множество $\Psi(\hat{U})$ также δ -полное и $\gamma_{i \times j} \leq \xi_\delta(\Psi(\hat{U}))$. ■

Итак, получены достаточное условие $i \times j$ -примитивности орграфа Γ , содержащего i, j -ксс-антицепь (наличие других i, j -ксс возможно), и оценка $i \times j$ -экспонента в этом случае. Для некоторых частных случаев получим критерий $i \times j$ -примитивности и уточним оценку $i \times j$ -экспонента.

Следствие 9. Если $\hat{U}$ — единственная i, j -ксс-антицепь в орграфе Γ , то Γ является $i \times j$ -примитивным тогда и только тогда, когда для любого $(b_1, \dots, b_r) \in H(P(i, j))$ система (7) не имеет решений по модулю $\delta = \text{ind } \hat{U}$.

Доказательство. Если $\hat{U}$ — единственная i, j -ксс-антицепь в орграфе Γ , то в силу леммы 5 $i \times j$ -примитивность орграфа Γ равносильна отсутствию решений системы (7). ■

Следствие 10. Если $\hat{U} = \{U_1, U_2\}$ — единственная i, j -ксс-антицепь в орграфе Γ и $\gcd(d_1, d_2) = 1$, то Γ не является $i \times j$ -примитивным.

Доказательство. Система сравнений $\{x \equiv b_s \pmod{d_s}, s = 1, 2\}$ имеет решение по модулю δ тогда и только тогда, когда $\gcd(d_1, d_2)$ делит разность $b_1 - b_2$ [1, замечание 2]. Следовательно, если $\gcd(d_1, d_2) = 1$, то при любом $(b_1, \dots, b_r) \in H(P(i, j))$ система имеет решение и в соответствии со следствием 9 орграф Γ не является $i \times j$ -примитивным. ■

Рассмотрим случай, когда Γ содержит i, j -ксс-антицепь, обозначаемую $\hat{U}^{(1)}$, элементами которой являются простые контуры $C_1, \dots, C_r$ длин $l_1, \dots, l_r$ соответственно.

Если хотя бы одно из множеств $\text{spc}_{l_s} P_s(i, j)$ является l_s -полным, $s \in \mathbb{N}_r$, то по следствию 8 орграф Γ , содержащий $\hat{U}^{(1)}$, является $i \times j$ -примитивным. В противном случае $H(P(i, j))$ непусто. Для проверки $i \times j$ -примитивности орграфа можно воспользоваться теоремой 2 (следствием 9). Получим точное значение величины $\gamma_{i \times j}$.

Следствие 11. Если $\hat{U} = \hat{U}^{(1)}$ и Γ является $i \times j$ -примитивным, то

$$\gamma_{i \times j} = \xi_\delta \left(\bigcup_{s=1}^r \left(\text{spc } P_s(i, j) + \bigcup_{\theta=1}^{\delta/d_s} \{l_s(\theta - 1)\} \right) \right),$$

где $\delta = \text{ind } \hat{U}$.

Доказательство. Согласно лемме 4, $\text{spc } W_s(i, j) = \text{spc } P_s(i, j) + l_s \mathbb{N}_0$, $s = 1, \dots, r$. В силу $i \times j$ -примитивности Γ множество $\text{spc } W(i, j)$ является δ -полным. Для любого $s = 1, \dots, r$ верно

$$\text{spc } W_s(i, j) = \text{spc } P_s(i, j) + \bigcup_{\theta=1}^{\delta/l_s} \{l_s(\theta - 1)\} + \delta \mathbb{N}_0.$$

Тогда $\text{spr } W(i, j) = \Phi + \delta\mathbb{N}_0$, где $\Phi = \bigcup_{s=1}^r \left(\text{spr } P_s(i, j) + \bigcup_{\theta=1}^{\delta/l_s} \{l_s(\theta - 1)\} \right)$. Значит, Φ δ -полное и $\gamma_{i \times j} = \xi_\delta(\Phi)$. ■

Пример 4. Рассмотрим оргграф Γ_4 , изображённый на рис. 8. Покажем его 1×8 -примитивность.

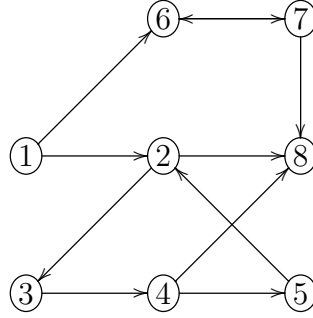


Рис. 8. Оргграф Γ_4

В графе имеется $1, 8$ -ксс-антицепь $\{C_1, C_2\}$, где $\tilde{C}_1 = \{2, 3, 4, 5\}$, $\tilde{C}_2 = \{6, 7\}$. Используя введённые обозначения, получим $r = 2$, $l_1 = 4$, $l_2 = 2$, $\delta = \text{lcm}(2, 4) = 4$, $\text{spr } P_1(i, j) = \{2, 4\}$, $\text{spr } P_2(i, j) = \{3\}$, $H(P(i, j)) = \{(1, 0), (3, 0)\}$. Системы сравнений

$$\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 0 \pmod{2} \end{cases} \quad \text{и} \quad \begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 0 \pmod{2} \end{cases}$$

не имеют решений по модулю 4. Согласно следствию 11, оргграф Γ_4 является 1×8 -примитивным и $1 \times 8\text{-exp } \Gamma_4 = \xi_4 \left(\bigcup_{s=1}^2 \left(\text{spr } P_s(i, j) + \bigcup_{\theta=1}^{\delta/l_s} \{l_s(\theta - 1)\} \right) \right) = \xi_4(\{2, 3, 4, 5\}) = 2$.

Рассмотрим наиболее простой случай, когда i, j -ксс-антицепь состоит из контуров $C_1, \dots, C_r$ одинаковой длины l . Обозначим такую ксс-антицепь $\hat{U}^{(2)}$.

Следствие 12. Если $\hat{U} = \hat{U}^{(2)}$, то Γ является $i \times j$ -примитивным тогда и только тогда, когда множество $\text{spr } P(i, j)$ является l -полным, в случае $i \times j$ -примитивности $\gamma_{i \times j} = \xi_l(\text{spr } P(i, j))$.

Доказательство. Согласно лемме 4, $\text{spr } W_s(i, j) = \text{spr } P_s(i, j) + l\mathbb{N}_0$, $s = 1, \dots, r$. Тогда $\text{spr } W(i, j) = \text{spr } P(i, j) + l\mathbb{N}_0 = \text{spr } P(i, j) - l + l\mathbb{N}$ и, согласно лемме 2, утверждение верно. ■

3. Перемешивающие свойства двухкаскадного генератора, построенного на основе последовательно-параллельного соединения регистров сдвига

Важным свойством генератора гаммы является зависимость знаков гаммы γ_t от всех знаков начального состояния при $t > t_0$, где t_0 определяет длину холостого хода генератора. Для этого свойства необходима примитивность (локальная примитивность) перемешивающего графа преобразования множества состояний генератора. Приведём пример оценки данного свойства с использованием полученных результатов.

Рассмотрим двухкаскадный генератор, построенный на основе двоичных регистров правого сдвига: управляющего длины m и двух генерирующих длин n и r ,

соединённых параллельно. Пусть управляющий регистр имеет функцию обратной связи $f_0(x_1, \dots, x_m)$, генерирующие регистры имеют по две функции обратной связи: $f_{11}(x_{m+1}, \dots, x_{m+n})$, $f_{12}(x_{m+1}, \dots, x_{m+n})$, $f_{21}(x_{m+n+1}, \dots, x_{m+n+r})$, $f_{22}(x_{m+n+1}, \dots, x_{m+n+r})$. Значения функций обратной связи складываются по модулю 2 со значением, снимаемым с крайней ячейки управляющего регистра, и записываются соответственно в ячейки с номерами $m+1$, $m+n'$, $m+n+1$, $m+n+r'$. Будем считать, что сумма значений, снимаемых с крайних ячеек генерирующих регистров, записывается в отдельную ячейку с номером $m+n+r+1$, откуда снимается гамма. Уравнения гаммообразования для данного генератора имеют вид

$$\gamma_t = h_{m+n+r+1}^t(x_1, \dots, x_{m+n+r+1}),$$

где h — преобразование множества состояний генератора, $h_{m+n+r+1}^t$ — $(m+n+r+1)$ -я координатная функция преобразования h^t , $t = 1, 2, \dots$. Таким образом, для анализа свойств гаммы генератора представляет интерес $\mathbb{N}_m \times \{m+n+r+1\}$ -примитивность перемешивающего орграфа $\Gamma(h)$.

Пусть $S(f_0) = \{g_1, \dots, g_\theta\}$, $S(f_{11}) = \{c_1^1, \dots, c_{\mu_1}^1\}$, $S(f_{12}) = \{c_1^2, \dots, c_{\mu_2}^2\}$, $S(f_{21}) = \{b_1^1, \dots, b_{\sigma_1}^1\}$, $S(f_{22}) = \{b_1^2, \dots, b_{\sigma_2}^2\}$, где $S(f)$ — множество номеров существенных переменных функции f ; $2 = g_1 < \dots < g_\theta = m$; $m+2 = c_1^1 < \dots < c_{\mu_1}^1 = m+n$; $m+2 = c_1^2 < \dots < c_{\mu_2}^2 = m+n$; $m+n+2 = b_1^1 < \dots < b_{\sigma_1}^1 = m+n+r$; $m+n+2 = b_1^2 < \dots < b_{\sigma_2}^2 = m+n+r$. Обозначим $d_0 = \gcd(g_1, \dots, g_\theta)$, $d'_1 = \gcd(c_1^1 - m, \dots, c_{\mu_1}^1 - m, c_1^2 - m, \dots, c_{\mu_2}^2 - m)$, $d'_2 = \gcd(b_1^1 - m - n, \dots, b_{\sigma_1}^1 - m - n, b_1^2 - m - n, \dots, b_{\sigma_2}^2 - m - n)$, $\gcd(d_0, d'_1) = d_1$, $\gcd(d_0, d'_2) = d_2$, $\gcd(d'_1, d'_2) = d$.

Преобразование h множества состояний генератора задано системой булевых координатных функций $\{h_1(x_1, \dots, x_{m+n+r+1}), \dots, h_{m+n+r+1}(x_1, \dots, x_{m+n+r+1})\}$, где

$$\begin{aligned} S(h_1) &= S(f_0); S(h_i) = \{i-1\}, i = 2, \dots, m; \\ S(h_{m+1}) &= S(f_{11}) \cup \{m\}; S(h_i) = \{i-1\}, i = m+2, \dots, m+n'-1; \\ S(h_{m+n'}) &= S(f_{12}) \cup \{m\}; S(h_i) = \{i-1\}, i = m+n'+1, \dots, m+n; \\ S(h_{m+n+1}) &= S(f_{21}) \cup \{m\}; S(h_i) = \{i-1\}, i = m+n+2, \dots, m+n+r'-1; \\ S(h_{m+n+r'}) &= S(f_{22}) \cup \{m\}; S(h_i) = \{i-1\}, i = m+n+r'+1, \dots, m+n+r; \\ S(h_{m+n+r+1}) &= \{m+n, m+n+r\}. \end{aligned}$$

Данные равенства полностью определяют множество дуг $(m+n+r+1)$ -вершинного орграфа $\Gamma(h)$.

Утверждение 6. Орграф $\Gamma(h)$ является $N_m \times \{m+n+r+1\}$ -примитивным тогда и только тогда, когда выполнено одно из следующих условий:

а) $d_1 = 1$, тогда

$$\gamma_{\mathbb{N}_m \times \{m+n+r+1\}} \leq 3(m+n-1) + g(g_1, \dots, g_\theta, c_1^1 - m, \dots, c_{\mu_1}^1 - m, c_1^2 - m, \dots, c_{\mu_2}^2 - m),$$

или $d_2 = 1$, тогда

$$\gamma_{\mathbb{N}_m \times \{m+n+r+1\}} \leq 3(m+r-1) + g(g_1, \dots, g_\theta, b_1^1 - m - n, \dots, b_{\sigma_1}^1 - m - n, b_1^2 - m - n, \dots, b_{\sigma_2}^2 - m - n);$$

б) $d_1 = 2$ при чётном n' , тогда

$$\begin{aligned} \gamma_{\mathbb{N}_m \times \{m+n+r+1\}} &\leq 3(m+n-1) + \\ &+ 2g(g_1/2, \dots, g_\theta/2, (c_1^1 - m)/2, \dots, (c_{\mu_1}^1 - m)/2, (c_1^2 - m)/2, \dots, (c_{\mu_2}^2 - m)/2), \end{aligned}$$

или $d_2 = 2$ при чётном r' , тогда

$$\gamma_{\mathbb{N}_m \times \{m+n+r+1\}} \leq 3(m+r-1) + 2g(g_1/2, \dots, g_\theta/2, (b_1^1 - m - n)/2, \dots, (b_{\sigma_1}^1 - m - n)/2, (b_1^2 - m - n)/2, \dots, (b_{\sigma_2}^2 - m - n)/2);$$

в) $d_1 = d_2 = 2$ и $n', r', (n-r)$ нечётные, тогда

$$\gamma_{\mathbb{N}_m \times \{m+n+r+1\}} \leq \xi_2(\{m+n+a_1, m+n-n'+a_1+1, m+r+a_2, m+r-r'+a_2+1\}),$$

где

$$a_1 = 2n + 2g((c_1^1 - m)/2, \dots, (c_{\mu_1}^1 - m)/2, (c_1^2 - m)/2, \dots, (c_{\mu_2}^2 - m)/2), \\ a_2 = 2r + 2g((b_1^1 - m - n)/2, \dots, (b_{\sigma_1}^1 - m - n)/2, (b_1^2 - m - n)/2, \dots, (b_{\sigma_2}^2 - m - n)/2).$$

Доказательство. Из вида графа $\Gamma(h)$ следует, что $\mathbb{N}_m \times \{m+n+r+1\}$ -примитивность орграфа равносильна $1 \times (m+n+r+1)$ -примитивности, при этом $\mathbb{N}_m \times \{m+n+r+1\}$ -exp $\Gamma(h) = 1 \times (m+n+r+1)$ -exp $\Gamma(h)$.

В орграфе $\Gamma(h)$ имеется три ксс U_0, U_1, U_2 порядка m, n, r соответственно, образующие две $1 \times (m+n+r+1)$ -ксс-цепи $U_1^{\rightarrow} = (U_0, U_1), U_2^{\rightarrow} = (U_0, U_2)$ со спецификациями (m, n) и (m, r) соответственно и одну $1 \times (m+n+r+1)$ -ксс-антицепь $\hat{U} = \{U_1, U_2\}$ со спецификацией (n, r) .

Ксс U_0 содержит систему контуров $\hat{C}_0$ длин $g_1, \dots, g_\theta$, ксс U_1 — систему контуров $\hat{C}_1$ длин $c_1^1 - m, \dots, c_{\mu_1}^1 - m, c_1^2 - m, \dots, c_{\mu_2}^2 - m$, ксс U_2 — систему контуров $\hat{C}_2$ длин $b_1^1 - m - n, \dots, b_{\sigma_1}^1 - m - n, b_1^2 - m - n, \dots, b_{\sigma_2}^2 - m - n$.

Через звенья цепи $U_1^{\rightarrow}$ проходят два пути из множества $P(1, m+n+r+1)$ длины $m+n$ и $m+n-n'+1$ (спс $P_1(1, m+n+r+1) = \{m+n, m+n-n'+1\}$), через звенья цепи $U_2^{\rightarrow}$ — два пути из $P(1, m+n+r+1)$ длины $m+r$ и $m+r-r'+1$ (спс $P_2(1, m+n+r+1) = \{m+r, m+r-r'+1\}$). Поскольку $g_1 = 2, c_1^1 = c_1^2 = m+2, b_1^1 = b_1^2 = m+n+2$, то $d_1, d_2, d'_1, d'_2 \in \{1, 2\}$.

а) Пусть $d_1 = 1$, то есть индекс системы контуров, входящих в ксс $U_1^{\rightarrow}$, равен 1. Тогда, согласно теореме 1, орграф $\Gamma(h)$ является $1 \times (m+n+r+1)$ -примитивным, поскольку множество спс $P_1(1, m+n+r+1)$ является 1-полным.

Воспользуемся оценкой локального экспонента из теоремы 1:

$$\gamma_{1 \times (m+n+r+1)} \leq \xi_1(\text{спс } P_1(1, m+n+r+1)) + a + 1,$$

где $a = g(g_1, \dots, g_\theta, c_1^1 - m, \dots, c_{\mu_1}^1 - m, c_1^2 - m, \dots, c_{\mu_2}^2 - m) + \text{len } Z(U_0, \hat{C}_0) + \text{len } Z(U_1, \hat{C}_1)$.

По лемме 1 $\xi_1(\text{спс } P_1(1, m+n+r+1)) = m+n$. В соответствии с (4), $\text{len } Z(U_0, \hat{C}_0) \leq m(1+1) - 2 = 2m - 2, \text{len } Z(U_1, \hat{C}_1) \leq n(1+1) - 2 = 2n - 2$, следовательно,

$$\gamma_{1 \times (m+n+r+1)} \leq 3(m+n-1) + g(g_1, \dots, g_\theta, c_1^1 - m, \dots, c_{\mu_1}^1 - m, c_1^2 - m, \dots, c_{\mu_2}^2 - m).$$

Случай $d_2 = 1$ доказывается аналогично.

б) Пусть $d_1 = 2$ и n' чётное. Тогда индекс системы контуров, входящих в ксс $U_1^{\rightarrow}$, равен 2 и множество спс $P_1(1, m+n+r+1)$ состоит из чётного и нечётного числа, то есть является 2-полным. Значит, по теореме 1 орграф $\Gamma(h)$ является $1 \times (m+n+r+1)$ -примитивным.

Воспользуемся оценкой локального экспонента из теоремы 1:

$$\gamma_{1 \times (m+n+r+1)} \leq \xi_2(\text{спс } P_1(1, m+n+r+1)) + a + 2,$$

где $a = 2g(g_1/2, \dots, g_\theta/2, (c_1^1 - m)/2, \dots, (c_{\mu_1}^1 - m)/2, (c_1^2 - m)/2, \dots, (c_{\mu_2}^2 - m)/2) + \text{len } Z(U_0, \hat{C}_0) + \text{len } Z(U_1, \hat{C}_1)$.

По лемме 1 $\xi_2(\text{spc } P_1(1, m + n + r + 1)) = m + n - 1$, и величины $\text{len } Z(U_0, \hat{C}_0)$, $\text{len } Z(U_1, \hat{C}_1)$ оцениваются аналогично п. а. Тогда

$$\gamma_{1 \times (m+n+r+1)} \leq 3(m + n - 1) + 2g(g_1/2, \dots, g_\theta/2, (c_1^1 - m)/2, \dots, (c_{\mu_1}^1 - m)/2, (c_1^2 - m)/2, \dots, (c_{\mu_2}^2 - m)/2).$$

В случае $d_2 = 2$ и чётном r' доказательство аналогично.

в) Если условия «а» и «б» не выполнены, то множество $\text{spc } P_1(1, m + n + r + 1)$ не содержит число $m + n + 1$ и множество $\text{spc } P_2(1, m + n + r + 1)$ не содержит число $m + r + 1$. Если $d_1 = d_2 = 2$, то $d'_1 = d'_2 = 2$. Таким образом, множество $H(P(1, m + n + r + 1))$ непусто и содержит элемент $(\pi_1, \pi_2) = ((m + n + 1) \bmod 2, (m + r + 1) \bmod 2)$. Согласно теореме 2, орграф $\Gamma(h)$ $1 \times (m + n + r + 1)$ -примитивный, если система сравнений

$$\begin{cases} x \equiv \pi_1 \pmod{d'_1}, \\ x \equiv \pi_2 \pmod{d'_2} \end{cases}$$

не имеет решений по модулю $\delta = \text{lcm}(d'_1, d'_2) = 2$. В силу [1, замечание 2] это равносильно тому, что $(\pi_1 - \pi_2) = (n - r) \bmod 2$ не делится на $d = \text{gcd}(d'_1, d'_2) = 2$. Поскольку $\hat{U}$ — единственная $1 \times (m + n + r + 1)$ -ксс-антицепь в орграфе $\Gamma(h)$, по следствию 9 данные условия являются необходимыми и достаточными.

Воспользуемся оценкой локального экспонента из теоремы 2:

$$\gamma_{1 \times (m+n+r+1)} \leq \xi_2 \left(\bigcup_{s=1}^2 (\text{spc } P_s(1, m + n + r + 1) + \{a_s + d'_s\}) \right).$$

Используя введенные обозначения, имеем

$$d'_1 = d'_2 = 2,$$

$$a_1 = 2g((c_1^1 - m)/2, \dots, (c_{\mu_1}^1 - m)/2, (c_1^2 - m)/2, \dots, (c_{\mu_2}^2 - m)/2) + 2n - 2,$$

$$a_2 = 2g((b_1^1 - m - n)/2, \dots, (b_{\sigma_1}^1 - m - n)/2, (b_1^2 - m - n)/2, \dots, (b_{\sigma_2}^2 - m - n)/2) + 2r - 2.$$

Следовательно, $\gamma_{1 \times (m+n+r+1)} \leq \xi_2(\{m + n + a_1 + 2, m + n - n' + a_1 + 3, m + r + a_2 + 2, m + r - r' + a_2 + 3\})$. ■

Выводы

Получены условия (во многих случаях критерии) локальной примитивности для различных классов орграфов (в том числе для орграфов, возникающих в ряде криптографических приложений), применение которых проще по сравнению с универсальным критерием [1]. Некоторые из этих условий позволяют получить точные значения локальных экспонентов орграфов.

ЛИТЕРАТУРА

1. Фомичев В. М., Кяжсин С. Н. Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1.
2. Кяжсин С. Н., Фомичев В. М. Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
3. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
4. Фомичев В. М. Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.

REFERENCES

1. *Fomichev V. M. and Kyazhin S. N.* Lokal'naya primitivnost' matrits i grafov [Local primitiveness of graphs and matrices]. Diskretn. Anal. Issled. Oper., 2017, vol. 24, no. 1. (in Russian)
2. *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)
3. *Sachkov V. N. and Tarakanov V. E.* Kombinatorika neotritsatel'nykh matrits [Combinatorics of Non-Negative Matrices]. Moscow, TVP Publ., 2000. (in Russian)
4. *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)