ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 2017. Том 24, № 1. С. 97–119

УДК 519.17 DOI: 10.17377/daio.2017.24.519

ЛОКАЛЬНАЯ ПРИМИТИВНОСТЬ МАТРИЦ И ГРАФОВ

В. М. Фомичёв[1,2,a], *С. Н. Кяжин*[2,3,b]

[1]Финансовый университет при Правительстве РФ,
Ленинградский пр., 49, 125993 Москва, Россия
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, 115409 Москва, Россия
[3]Центр специальных разработок МО РФ,
ул. Свободы, 21, 125362 Москва, Россия
E-mail: [a]fomichev@nm.ru, [b]s.kyazhin@kaf42.ru

Аннотация. Развивается матрично-графовый подход к оценке коммуникативных свойств системы взаимосвязанных объектов, применяемый, в частности, для исследования перемешивающих свойств итеративных криптографических преобразований двоичных векторных пространств, т. е. для исследования зависимости битов выходных блоков от входных битов. В ряде прикладных задач насыщенность связей объектов соответствует требуемому уровню, если положительна моделирующая связи матрица или её определённая подматрица (полным является моделирующий связи граф или его определённый подграф).

Введены понятия локальной примитивности и локальных экспонентов неотрицательной матрицы (графа), обобщающие и расширяющие область применения по сравнению с известными понятиями примитивности и экспонента. Получены универсальный критерий локальной примитивности орграфа и оценки локальных экспонентов, как универсальная оценка, так и её уточнения для различных частных случаев. Результаты применены для оценки перемешивающих свойств криптографического генератора, построенного на основе последовательного соединения двух регистров сдвига. Табл. 2, библиогр. 12.

Ключевые слова: примитивная матрица, примитивный граф, экспонент, локальная примитивность матрицы (графа), локальный экспонент.

Основные обозначения

В статье используются следующие обозначения: $\mathbb{N}$ — множество натуральных чисел; $n \in \mathbb{N}$; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $\mathbb{N}_n = \{1, \ldots, n\}$; $V = \{0, 1\}$; $(a_1, \ldots, a_n)$ — наибольший общий делитель чисел $a_1, \ldots, a_n \in \mathbb{N}$; $\operatorname{lcm}\{a_1, \ldots, a_m\}$ — наименьшее общее кратное чисел $a_1, \ldots, a_m \in \mathbb{N}$; $\overline{J} = \mathbb{N}_n \setminus J$, где $J \subseteq \mathbb{N}_n$; Ω_n — множество всех непустых подмножеств множества $\mathbb{N}_n$; $\mathbb{Z}_d$ — кольцо вычетов по модулю $d \in \mathbb{N}$; $M_n^{0,1}$ — множество 0,1-матриц порядка $n > 1$; $\exp M$ ($\exp \Gamma$) — экспонент матрицы M (графа Γ); $[i, j]$ — путь в орграфе Γ из вершины i в вершину j, где $i, j \in \mathbb{N}_n$; $kC(i)$ — путь в Γ, являющийся k-кратно пройденным контуром C из вершины i, $k \geqslant 0$; $W(i, j)$ — множество путей в орграфе Γ из i в j; $\bullet$ — операция конкатенации путей в орграфе; $\operatorname{len} w$ — длина пути w в орграфе Γ, равная числу дуг, составляющих путь; ксс — компонента сильной связности орграфа.

Введение

Для изучения коммуникативных свойств системы n объектов, занумерованных числами $1, \ldots, n$, $n > 1$, используется 0,1-матрица $M = (m_{i,j})$ порядка n (или система матриц), кодирующая связи между объектами системы: $m_{i,j} = 1$, если имеется направленная связь от i-го объекта к j-му, и $m_{i,j} = 0$ в противном случае. Экстремальные коммуникативные свойства системы достигаются тогда, когда матрица M примитивна и имеет небольшой экспонент.

Вместо 0,1-матрицы M можно равносильным образом рассматривать орграф Γ, матрица смежности вершин которого совпадает с M. Экспонентам неотрицательных матриц и систем матриц (графов и систем графов) посвящено много работ. Обзор основных результатов по примитивности матриц и графов, полученных до 2012 г., дан в [1,5]. Ряд более поздних результатов опубликован в журнале «Прикладная дискретная математика».

Свойство примитивности матриц и графов в криптографических приложениях можно использовать для оценки перемешивающих свойств преобразований векторных пространств, где под перемешивающими свойствами понимается зависимость координат выходных векторов от координат входных векторов.

В криптографии гаммой принято называть ключевую последовательность знаков алфавита, так как исторически знаки последовательности обозначались греческой буквой γ. Для выработки таких последовательностей используются специальные технические устройства или программы, называемые *криптографическими генераторами*. Генераторы моде-

лируются конечными автономными автоматами, элементы которых зависят от ключа. Важным свойством генератора является зависимость знаков гаммы γ_i от всех знаков начального состояния при $i > i_0$, где i_0 определяет так называемую длину холостого хода генератора (i_0 значительно меньше длины периода гаммы).

Пусть $h\colon X^n \to X^n$ — преобразование множества состояний генератора, заданное системой координатных функций

$$\{h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n)\}.$$

Перемешивающим орграфом $\Gamma(h)$ *преобразования* h называется орграф с n вершинами, в котором имеется дуга (i, j), если и только если координатная функция h_j существенно зависит от переменной x_i. Матрица смежности такого графа называется *перемешивающей матрицей преобразования*. Тогда указанное свойство выполняется, если перемешивающий граф $\Gamma(h)$ преобразования h множества состояний генератора примитивный.

В некоторых приложениях важные свойства системы объектов достигаются тогда, когда положительной является не степень матрицы в целом, а лишь некоторая её часть, например, подматрица, получаемая удалением некоторых строк и столбцов. В частности, такая ситуация имеет место при исследовании зависимости знаков гаммы от знаков начального состояния генератора, когда каждый знак гаммы определяется собственным подмножеством множества знаков соответствующего промежуточного состояния.

В связи с этим в данной работе в порядке обобщения понятий примитивности и экспонента введены и исследованы понятия локальной примитивности и локальных экспонентов неотрицательной матрицы (графа). Введённые понятия распространяются на широкий класс непримитивных орграфов и матриц. Первые результаты в этом направлении представлены в [3]. Другие обобщения понятий примитивности и экспонента исследовались в [6–9, 11, 12].

1. Локальная примитивность неотрицательных матриц

Пусть $I = \{i_1, \ldots, i_k\}$, $J = \{j_1, \ldots, j_r\}$, $\varnothing \neq I, J \subseteq \mathbb{N}_n$, M — 0,1-матрица порядка $n > 1$, $M(I \times J)$ — её подматрица размера $k \times r$, полученная из M удалением строк с номерами $i \notin I$ и столбцов с номерами $j \notin J$. Матрицу $M(I \times J)$ обозначим через $M(J^2)$ при $I = J$, $M(*J)$ — при $I = \mathbb{N}_n$ и $M(I*)$ — при $J = \mathbb{N}_n$.

Матрица M называется *положительной* ($M > 0$), если положительны все её элементы. Матрица M называется $I \times J$*-положительной*

(*J^2-положительной* при $I = J$, *$*J$-положительной* при $I = \mathbb{N}_n$, *$I*$-положительной* при $J = \mathbb{N}_n$), если положительна матрица $M(I \times J)$. Матрица M называется *s-положительной* (*c-положительной*), если она не содержит нулевых строк (столбцов). Матрицу M назовём *$I \times J$-s-положительной* (*J^2-s-положительной* при $I = J$, *$*J$-s-положительной* при $I = \mathbb{N}_n$, *$I*$-s-положительной* при $J = \mathbb{N}_n$), если *s-положительна* матрица $M(I \times J)$. Обозначим множества s-, $I \times J$-s-, J^2-s-, $*J$-s-, $I*$-s-положительных матриц порядка n через M_n^s, $M_n^s(I \times J)$, $M_n^s(J^2)$, $M_n^s(*J)$, $M_n^s(I*)$ соответственно. Аналогично определяются $I \times J$-c-положительные матрицы. Через M_n^c, $M_n^c(I \times J)$, $M_n^c(J^2)$, $M_n^c(*J)$, $M_n^c(I*)$ обозначим соответствующие множества матриц.

Множество $M_n^{0,1}$ — моноид по умножению $\otimes$, где 0,1-матрица $M_1 \otimes M_2$ получена из целочисленной матрицы $M_1 M_2$ с помощью замены положительных элементов единицами.

Матрица M называется *$I \times J$-примитивной* (*J^2-примитивной* при $I = J$, *$*J$-примитивной* при $I = \mathbb{N}_n$, *$I*$-примитивной* при $J = \mathbb{N}_n$), если существует число $\gamma \in \mathbb{N}$ такое, что матрица $M^t(I \times J)$ ($M^t(J^2)$, $M^t(*J)$, $M^t(I*)$) положительна при любом $t \geqslant \gamma$. Наименьшее такое число γ назовём *$I \times J$-экспонентом* (*J^2-экспонентом*, *$*J$-экспонентом*, *$I*$-экспонентом*) матрицы M, обозначим через $I \times J\text{-}\exp M$ ($J^2\text{-}\exp M$, $*J\text{-}\exp M$, $I*\text{-}\exp M$). Далее $I \times J$-примитивные матрицы будем называть также *локально примитивными*, а их $I \times J$-экспоненты — *локальными экспонентами*.

Утверждение 1. *Множества $M_n^s(J^2)$ и $M_n^c(J^2)$ — моноиды по умножению, $n > 1$. Если $M \in M_n^s(I^2) \cup M_n^c(J^2)$ и число $\gamma \in N$ — наименьшее, при котором $M^\gamma(I \times J) > 0$, то матрица M $I \times J$-примитивна и $I \times J\text{-}\exp M = \gamma$* [3].

Рассмотрим частичные порядки на некоторых множествах.

Для $I, J, I', J' \subseteq \mathbb{N}_n$ положим

$$(I, J) \subseteq (I', J') \Leftrightarrow I \subseteq I', \quad J \subseteq J'.$$

Данное бинарное отношение $\subseteq$ является отношением частичного порядка на множестве Ω_n^2.

Определим отношение частичного порядка $\leqslant$ на множестве $M_n^{0,1}$. Для матриц A, B, где $A = (a_{i,j})$, $B = (b_{i,j})$, положим $A \leqslant B$ тогда и только тогда, когда $a_{i,j} \leqslant b_{i,j}$ для всех $i, j = 1, \ldots, n$. Если при этом существуют такие i и j, что $a_{i,j} < b_{i,j}$, то $A < B$. Для $M \in M_n^{0,1}$ при $t \in \mathbb{N}$ обозначим $M^t = \left(m_{i,j}^{(t)}\right)$, $M_{A,J} = \left\{B \in M_n^{0,1} : B(J^2) \geqslant A(J^2)\right\}$.

Локальный экспонент $I \times J$-$\exp M$ можно представить, с одной стороны, как функцию $\gamma' \colon M_n^{0,1} \to \mathbb{N}$ от матрицы M при фиксированных I, J, с другой стороны, как функцию $\gamma'' \colon \Omega_n^2 \to \mathbb{N}$ от множеств I, J при фиксированной M.

Утверждение 2. *При любых допустимых* I, J [3]

(i) $\gamma'(M)$ — *антиизотонная функция относительно отношения* $\leqslant$;

(ii) $\gamma''(I, J)$ — *изотонная функция относительно отношения* $\subseteq$ *при любой* $M \in M_n^{0,1}$;

(iii) $(M(J^2))^t \leqslant M^t(J^2)$ *при любой* $M \in M_n^{0,1}$, $t \geqslant 1$, *откуда*

$$J^2\text{-}\exp M \leqslant \exp M(J^2).$$

2. Локальная примитивность ориентированных графов

Пусть M — матрица смежности вершин орграфа Γ. Орграф Γ называется *примитивным* ($I \times J$-*примитивным*), если при некотором $\gamma \in \mathbb{N}$ для любых $i, j \in \mathbb{N}_n$ ($(i, j) \in I \times J$) в Γ имеются пути любой длины $t \geqslant \gamma$ из i в j, наименьшее такое t равно $\exp\Gamma$ ($I \times J$-$\exp\Gamma$). Орграф Γ примитивный тогда и только тогда, когда матрица M примитивная, $\exp M = \exp\Gamma$, $I \times J$-$\exp M = I \times J$-$\exp\Gamma$. Величины $I \times J$-экспонента будем называть также *локальными экспонентами* графа Γ, за исключением случая $I = J = \mathbb{N}_n$.

Сильно связный орграф является примитивным тогда и только тогда, когда взаимно просто множество длин всех его простых контуров [5, гл. IV, свойство 11]. Исследуем $I \times J$-примитивность графа Γ, полностью определяемую свойствами множества путей в Γ из вершин множества I в вершины множества J.

Операция конкатенации $\bullet$ определена на паре путей (u, v) орграфа Γ тогда и только тогда, когда конечная вершина пути u совпадает с начальной вершиной пути v. Если $w = u \bullet v$, то $\operatorname{len} w = \operatorname{len} u + \operatorname{len} v$.

Введём следующие обозначения для орграфа Γ: $K = I \cap J$; $\gamma_{I\times J} = I \times J$-$\exp\Gamma$ для $I \times J$-примитивного графа Γ, где $\gamma_{i\times j} = \gamma_{I\times J}$ при $I = \{i\}$, $J = \{j\}$; l_{ij} — длина кратчайшего пути из i в j; $\rho(I, J) = \min\limits_{(i,j)\in I\times J} l_{ij}$ — расстояние от множества I до множества J ($\rho(I, J) = 0$ при $I \cap J \neq \varnothing$, $\rho(i, J) = \rho(I, J)$ при $I = \{i\}$, $\rho(I, j) = \rho(I, J)$ при $J = \{j\}$); $\theta(I, J) = \max\limits_{i\in I} \rho(i, J)$ — расстояние достижимости из любой вершины множества I некоторой вершины множества J ($\theta(I, J) = 0$, если $I \subseteq J$); $\tau(I, J) = \max\limits_{j\in J} \rho(I, j)$ — расстояние достижимости из некоторой вершины множества I любой вершины множества J ($\tau(I, J) = 0$, если $J \subseteq I$); Γ_i — ксс, содержащая циклическую вершину i, $\Gamma_I = \bigcup\limits_{i\in I} \Gamma_i$.

Если вершины i и j взаимно достижимы в Γ при $i \neq j$, то $\Gamma_i = \Gamma_j$.

Для вершин i, j орграфа Γ ксс U орграфа Γ назовём *i, j-связывающей*, если в $W(i,j)$ есть путь, проходящий через некоторую вершину ксс U. Подмножество простых путей из $W(i,j)$, содержащих циклические вершины, обозначим через $P(i,j)$.

Утверждение 3. (i) *Орграф Γ $I \times J$-примитивный тогда и только тогда, когда Γ является $i \times j$-примитивным для любой пары вершин $(i,j) \in I \times J$, при этом $\gamma_{I\times J} = \max\limits_{(i,j)\in I\times J} \gamma_{i\times j}$.*

(ii) *Если орграф Γ $i \times j$-примитивный, то Γ содержит i, j-связывающую ксс* [3].

Теорема 1. *Орграф Γ $I \times J$-примитивный при $K \neq \varnothing$ тогда и только тогда, когда Γ_K — примитивная i, j-связывающая ксс для любой пары $(i,j) \in I \times J$. Если Γ $I \times J$-примитивный, то*

$$-\theta(I, \widetilde{\Gamma}_K) - \tau(\widetilde{\Gamma}_K, J) \leqslant \exp\Gamma_K - \gamma_{I\times J} \leqslant \theta(\widetilde{\Gamma}_K, K) + \tau(K, \widetilde{\Gamma}_K),$$

где $\widetilde{\Gamma}_K$ — множество вершин подграфа Γ_K.

Доказательство. Необходимость. Пусть орграф Γ $I \times J$-примитивный. Тогда по утверждению 3(i) Γ $i \times j$-примитивный для любой пары $(i,j) \in I \times J$, т. е. для любого $t \geqslant \gamma_{i\times j}$ в $W(i,j)$ имеется путь длины t, где $\gamma_{i\times j} \leqslant \gamma_{I\times J}$. Значит, все вершины из K (и из $\widetilde{\Gamma}_K$) взаимно достижимы, и для всех $(i,j) \in K^2$ в $W(i,j)$ имеется путь длины t для любого $t \geqslant \gamma_{I\times J}$. Следовательно, Γ_K есть ксс.

Для всех $\alpha, \beta \in \widetilde{\Gamma}_K$ путь $[\alpha, \beta]$ представим конкатенацией:

$$[\alpha, \beta] = [\alpha, i(\alpha)] \bullet [i(\alpha), j(\beta)] \bullet [j(\beta), \beta],$$

где путь $[\alpha, i(\alpha)]$ пустой тогда и только тогда, когда $\alpha \in I \cap \widetilde{\Gamma}_K$, иначе $i(\alpha)$ — ближайшая вершина множества K, достижимая из α, путь $[j(\beta), \beta]$ пустой тогда и только тогда, когда $\beta \in \widetilde{\Gamma}_K \cap J$, иначе $j(\beta)$ — ближайшая вершина множества K, из которой достижима β. Значит, имеется путь $[\alpha, \beta]$ длины t для любого $t \geqslant \theta(\alpha, K) + \gamma_{I\times J} + \tau(K, \beta)$. Тогда Γ_K — примитивная ксс и $\exp\Gamma_K \leqslant \theta(\widetilde{\Gamma}_K, K) + \gamma_{I\times J} + \tau(K, \widetilde{\Gamma}_K)$, откуда

$$\exp\Gamma_K - \gamma_{I\times J} \leqslant \theta(\widetilde{\Gamma}_K, K) + \tau(K, \widetilde{\Gamma}_K).$$

Достаточность. Пусть Γ_K — примитивная i, j-связывающая ксс для любой пары $(i,j) \in I \times J$ и $\exp\Gamma_K = \gamma$. Для любых $i \in I$, $j \in J$ путь $[i, j]$ представим конкатенацией

$$[i, j] = [i, \alpha(i)] \bullet [\alpha(i), \beta(j)] \bullet [\beta(j), j],$$

где путь $[i, \alpha(i)]$ пустой тогда и только тогда, когда $i \in I \cap \widetilde{\Gamma}_K$, иначе $\alpha(i)$ — ближайшая вершина ксс Γ_K, достижимая из i, путь $[\beta(j), j]$ пустой тогда и только тогда, когда $j \in \widetilde{\Gamma}_K \cap J$, иначе $\beta(j)$ — ближайшая вершина ксс Γ_K, из которой достижима j. Значит, Γ $I \times J$-примитивный, поскольку для любых $(i, j) \in I \times J$ имеется путь из i в j длины t при $t \geqslant \theta(i, \widetilde{\Gamma}_K) + \gamma + \tau(\widetilde{\Gamma}_K, j)$. Отсюда

$$\gamma_{I\times J} \leqslant \theta(I, \widetilde{\Gamma}_K) + \exp\Gamma_K + \tau(\widetilde{\Gamma}_K, J),\ \exp\Gamma_K - \gamma_{I\times J} \geqslant -\theta(I, \widetilde{\Gamma}_K) - \tau(\widetilde{\Gamma}_K, J).$$

Объединяя доказанные оценки, получаем нужную. Теорема 1 доказана.

Замечание 1. При $K \neq \varnothing$ $I \times J$-примитивный орграф Γ является $I \times \widetilde{\Gamma}_K$- и $\widetilde{\Gamma}_K \times J$-примитивным.

Следствие 1. *В условиях теоремы* 1 $I \times J$*-примитивный граф* Γ *примитивен тогда и только тогда, когда* Γ *сильно связен. Если* Γ *примитивен, то*

$$0 \leqslant \exp\Gamma - \gamma_{I\times J} \leqslant \theta(\widetilde{\Gamma}_K, K) + \tau(K, \widetilde{\Gamma}_K).$$

Доказательство. По теореме 1 в $I \times J$-примитивном графе Γ имеется примитивная ксс Γ_K, где $K \subseteq \widetilde{\Gamma}_K$. Тогда в Γ_K и, значит, в Γ имеются циклы взаимно простых длин. Отсюда орграф Γ примитивен. Для получения оценок $\exp\Gamma_K - \gamma_{I\times J}$ следует в оценках теоремы 1 положить $\Gamma_K = \Gamma$. Сильная связность необходима по определению примитивного графа. Следствие 1 доказано.

Исследуем условия $I \times J$-примитивности графа Γ в случае $K = \varnothing$, полностью определяемые свойствами множества $W(i, j)$. В силу утверждения 3(i) достаточно рассмотреть условия $i \times j$-примитивности графа Γ при $i \neq j$. Сложность данной задачи обусловлена необходимостью учёта различных видов размещения i, j-связывающих ксс в графе Γ, так как две ксс либо соединяются последовательно, либо размещены параллельно, т. е. не взаимно достижимы.

Приведём вначале простейшие достаточные условия.

В n-вершинном орграфе циклической вершине r соответствует множество простых контуров, проходящих через r. Обозначим множество длин этих контуров через $L(r)$, $r = 1, \ldots, n$. Циклическую вершину r назовём *узловой*, если НОД$\{l \in L(r)\} = 1$. В частности, если r — вершина с петлёй, то она узловая и $1 \in L(r)$.

Введём следующее обозначение: $g(a_1, \ldots, a_m)$ — число Фробениуса, где $(a_1, \ldots, a_m) = 1$ (при $m > 1$ наибольшее число, не принадлежащее аддитивной полугруппе $\langle a_1, \ldots, a_m\rangle$, порождённой натуральными взаимно простыми числами $a_1, \ldots, a_m$); $g(1) = -1$.

Утверждение 4. *Если в орграфе* Γ *путь* $[i,j]$ *проходит через узловую вершину* r*, то* Γ $i\times j$*-примитивный и*

$$\gamma_{i\times j}\leqslant \operatorname{len}[i,j]+g(L(r))+1.$$

Доказательство. Путь $[i,j]$ представим конкатенацией

$$[i,j]=[i,r]\bullet C(r)\bullet[r,j],$$

где $C(r)$ — контур, проходящий через вершину r. Если r — вершина с петлёй, то в $W(i,j)$ имеются пути любой длины, большей или равной $\operatorname{len}[i,j]$ (в этом случае $g(L(r))=-1$). Если в r нет петли, то в соответствии с определением числа Фробениуса, варьируя кратность обхода контуров, проходящих через r, можно построить контур $C(r)$, длина которого принимает любое значение, большее $g(L(r))$. Утверждение 4 доказано.

Для получения критерия $i\times j$-примитивности графа Γ при $i\neq j$ введём ряд определений.

Ксс U назовём *смежной с путём* w, если w проходит через некоторые вершины U. Контур орграфа Γ назовём *смежным с путём* w, если контур принадлежит ксс, смежной с путём w. Систему контуров назовём *смежной с путём* w, если каждый контур системы смежен с путём w. *Индексом* смежной с путём w системы контуров $\widehat{C}(w)=\{C_1^w,\dots,C_m^w\}$ с множеством длин $l_1^w,\dots,l_m^w$ назовём число $\operatorname{ind}(\widehat{C}(w))=\bigl(l_1^w,\dots,l_m^w\bigr)$.

Обозначим через $F(w)$ класс всех систем простых контуров, смежных с путём w; $F(w)$ образует решётку относительно включения систем. Если орграф Γ $i\times j$-примитивен, то $F(w)\neq\varnothing$ для любого пути $w\in P(i,j)$ в силу утверждения 3(ii). *Индексом пути* $w\in P(i,j)$ назовём индекс системы всех простых смежных с w контуров, т. е. индекс максимальной системы из $F(w)$.

Пусть $w=(i_0,i_1,\dots,i_l)\in P(i,j)$, т. е. $i_0=i$, $i_l=j$. Путь $v(w)\in W(i,j)$ назовём *расширением пути* w, если

$$v(w)=C_0\bullet(i_0,i_1)\bullet C_1\bullet\cdots\bullet C_{l-1}\bullet(i_{l-1},i_l)\bullet C_l,$$

где C_k — контур (возможен пустой контур длины 0), обход которого начинается из вершины i_k, $k=0,1,\dots,l$. Дуги пути w являются дугами пути $v(w)$, и порядок их следования сохраняется в пути $v(w)$.

Если орграф Γ содержит ксс U и ксс U' и из вершин ксс U достижимы вершины ксс U', то ксс U из ксс U' не достижима, иначе U и U'

не являются ксс. При $r \geqslant 1$ последовательность ксс $\widehat{U} = \{U_1, \ldots, U_r\}$ орграфа Γ назовём *ксс-цепью длины* r в Γ, если $r = 1$ или при $r > 1$ из вершин ксс U_{s-1} достижимы вершины ксс U_s, $s = 2, \ldots, r$. *Спецификацией ксс-цепи* $\widehat{U}$ назовём набор $(u_1, \ldots, u_r)$, где u_s — число вершин ксс U_s, $s = 1, \ldots, r$. Назовём ксс-цепь $\widehat{U}$ *i, j-связывающей в* Γ, если из вершины i достижима ксс U_1 и из ксс U_r достижима вершина j. Для i, j-связывающих цепей $\widehat{U}, \widehat{U}'$ положим $\widehat{U} \leqslant \widehat{U}'$, если каждое звено цепи $\widehat{U}$ является звеном цепи $\widehat{U}'$. Назовём i, j-связывающую ксс-цепь $\widehat{U}$ *плотной*, если не существует i, j-связывающей ксс-цепи $\widehat{U}'$ такой, что $\widehat{U} \leqslant \widehat{U}'$ и $\widehat{U} \neq \widehat{U}'$. Плотную i, j-связывающую ксс-цепь назовём *смежной с простым путём* $w \in P(i, j)$, если w проходит через каждое звено цепи.

Теорема 2. *В орграфе* Γ *для любого пути* $w \in P(i, j)$ *индекса* d *верны следующие утверждения*:

(i) *длина любого контура, смежного с путём* w, *делится на* d;

(ii) $\operatorname{len} v(w) \equiv \operatorname{len} w \pmod{d}$ *для любого расширения* $v(w)$ *пути* w;

(iii) *имеется единственная плотная* i, j*-связывающая ксс-цепь, смежная с путём* w;

(iv) *любой путь из* $W(i, j)$ *есть расширение некоторого пути из* $P(i, j)$.

Доказательство. (i) Из любого контура C можно последовательным удалением простых контуров получить простой контур за конечное число шагов. Тогда длина контура C есть сумма длин нескольких простых контуров. Значит, если контур C смежен с путём w, то длина каждого простого контура, составляющего C, и длина самого контура C делится на d.

(ii) Пусть $w = (i_0, i_1, \ldots, i_l)$, где $i_0 = i$, $i_l = j$. Тогда любое расширение $v(w)$ пути w имеет вид

$$v(w) = C_0 \bullet (i_0, i_1) \bullet C_1 \bullet \cdots \bullet C_{l-1} \bullet (i_{l-1}, i_l) \bullet C_l,$$

где C_k — контур (возможен пустой контур длины 0), обход которого начинается из вершины i_k, $k = 0, 1, \ldots, l$. Тогда $\operatorname{len} v(w) = \operatorname{len} w + \sum\limits_{k=0}^{l} \operatorname{len} C_k$. Контуры $C_0, C_1, \ldots, C_l$ смежны с путём w, значит, их длины кратны d. Тем самым $\operatorname{len} v(w) \equiv \operatorname{len} w \pmod{d}$.

(iii) Пусть $w = (i_0, i_1, \ldots, i_l) \in P(i, j)$, где $i_0 = i$, $i_l = j$. По условию либо все вершины пути циклические, либо $(i_0, i_1, \ldots, i_l)$ есть конкатенация слов $w_1 \bullet \cdots \bullet w_r$ в алфавите $\mathbb{N}_n$, где $1 < r \leqslant l$, каждое слово состоит только из циклических вершин или только из ациклических вершин и слова обоих типов чередуются. Слова из циклических вершин однозначно разбиваются на подслова по принадлежности вершин общей ксс,

т. е. пути w однозначно соответствует не содержащая повторений последовательность ксс (обозначим её через $\widehat{U}(w)$). Действительно, если ксс U и ксс U' различны и в пути w вершина $\alpha' \in U'$ следует за вершиной $\alpha \in U$, а вершина α'' следует за вершиной α', то $\alpha'' \notin U$, иначе U и U' не являются ксс, так как они взаимно достижимы. Значит, $\widehat{U}(w)$ есть ксс-цепь, она i,j-связывающая по построению и смежная с w. Любая циклическая вершина пути w содержится в звеньях ксс-цепи, значит, ксс-цепь плотная.

(iv) Пусть $w = (i_0, i_1, \dots, i_l) \in W(i,j)$, где $i_0 = i$, $i_l = j$. Представим w как конкатенацию контуров и дуг, не лежащих на контуре. Если $i_0 \neq i_t$ при $t = 1, \dots, l$, то дуга (i_0, i_1) не лежит на контуре и переходим к вершине i_1, в противном случае имеем контур $(i_0, i_1, \dots, i_t)$, где t — наибольший номер, при котором $i_0 = i_t$, дуга (i_t, i_{t+1}) не лежит на контуре, и переходим к вершине i_{t+1}. Продолжая аналогичные рассуждения для вершины i_1 или i_{t+1}, получаем за конечное число шагов нужную конкатенацию. Удаляя из неё все контуры, получаем путь из $P(i,j)$. Теорема 2 доказана.

Далее $\widehat{U}(w) = \{U_1(w), \dots, U_{r(w)}(w)\}$ — плотная i,j-связывающая ксс-цепь длины $r(w) \geqslant 1$, смежная с путём $w \in P(i,j)$. Ксс-цепь $\widehat{U}(w)$ однозначно разбивает систему $\widehat{C}(w)$ не более чем на $r(w)$ подсистем по принадлежности звеньям ксс-цепи $\widehat{U}(w)$. Обозначим порядки подсистем через $\lambda_1^w, \dots, \lambda_{r(w)}^w$ соответственно, $\lambda_1^w + \dots + \lambda_{r(w)}^w = m$, $\lambda_s^w \geqslant 0$, $s = 1, \dots, r(w)$. Через $\overline{g}(a_1, \dots, a_m) = g(a_1, \dots, a_m) - a_1 - \dots - a_m$ обозначим смещённое число Фробениуса.

Теорема 3. *В орграфе* Γ *для любого пути* $w \in P(i,j)$ *индекса* d *если ксс-цепь* $\widehat{U}(w) = \{U_1(w), \dots, U_{r(w)}(w)\}$ *со спецификацией* $\big(u_1^w, \dots, u_{r(w)}^w\big)$ *разбивает смежную с* w *систему контуров* $\widehat{C}(w) = \big\{C_1^w, \dots, C_m^w\big\}$ *с длинами* $l_1^w, \dots, l_m^w$ *на подсистемы порядка* $\lambda_1^w, \dots, \lambda_{r(w)}^w$, *то в* Γ *имеются расширения пути* w *с множеством длин* $\operatorname{len} w + dt_w + d\mathbb{N}$, *где*

$$t_w = \left\lfloor \left(\sum_{s=1}^{r(w)} \big(\lambda_s^w + 1\big) u_s^w - r(w) \right) / d \right\rfloor + \overline{g}\big(l_1^w/d, \dots, l_m^w/d\big).$$

Доказательство. Так как путь w и система $\widehat{C}(w)$ фиксированы, без ущерба для строгости не будем указывать зависимости некоторых величин от w и $\widehat{C}(w)$.

По условию $\big(l_1^w/d, \dots, l_m^w/d\big) = 1$. Тогда по свойству чисел Фробениуса любое натуральное число, большее $g\big(l_1^w/d, \dots, l_m^w/d\big)$, есть линейная комбинация чисел $l_1^w/d, \dots, l_m^w/d$ с некоторыми целыми неотрицательными

коэффициентами $e_1, \dots, e_m$. Значит, подбирая коэффициенты $e_1, \dots, e_m$, можно для любого $t \in \mathbb{N}$ получить равенство

$$e_1 l_1^w + \dots + e_m l_m^w = dg\big(l_1^w/d, \dots, l_m^w/d\big) + dt.$$

Следовательно, расширение v_t пути w, проходящее через все контуры системы $\widehat{C}(w)$ и обходящее e_k-кратно контур C_k^w, $k = 1, \dots, m$, в зависимости от коэффициентов имеет длину $\operatorname{len} v_t$, равную

$$\operatorname{len} w + e_1 l_1^w + \dots + e_m l_m^w + z_t = \operatorname{len} w + dg\big(l_1^w/d, \dots, l_m^w/d\big) + z_t + dt, \quad (1)$$

где $t \in \mathbb{N}$, $z_t = z_{t,1} + \dots + z_{t,r(w)}$, $z_{t,s}$ — длина контура $Z_{t,s}$ в ксс $U_s(w)$, имеющего общие вершины с w и со всеми контурами системы $\widehat{C}(w)$ из ксс $U_s(w)$, $s = 1, \dots, r(w)$.

Оценим z_t. Пусть контур $Z_{t,s}$ проходит через вершину α_0^s пути w и через вершины контуров $C_{s,1}^w, \dots, C_{s,\lambda(s)}^w$ ксс $U_s(w)$ с длинами $l_{s,1}^w, \dots, l_{s,\lambda(s)}^w$ соответственно, где $(s, j) \in \{1, \dots, m\}$ при $j = 1, \dots, \lambda(s)$. Тогда $Z_{t,s}$ есть конкатенация путей

$$\big[\alpha_0^s, \alpha_1^s\big] \bullet \dots \bullet \big[\alpha_{\lambda(s)-1}^s, \alpha_{\lambda(s)}^s\big] \bullet \big[\alpha_{\lambda(s)}^s, \alpha_0^s\big],$$

где $\big[\alpha_{\mu-1}^s, \alpha_\mu^s\big]$ — кратчайший путь из вершины $\alpha_{\mu-1}^s$ до ближайшей вершины α_μ^s, принадлежащей контуру $C_{s,\mu}^w$, $\mu = 1, \dots, \lambda(s)$, $\big[\alpha_{\lambda(s)}^s, \alpha_0^s\big]$ — кратчайший путь из $\alpha_{\lambda(s)}^s$ в α_0^s. В n-вершинном графе расстояние от любой вершины до контура длины l не больше $n-l$, поэтому $\operatorname{len}\big[\alpha_{\mu-1}^s, \alpha_\mu^s\big] \leqslant u_s^w - l_{s,\mu}^w$, $\operatorname{len}\big[\alpha_{\lambda(s)}^s, \alpha_0^s\big] \leqslant u_s^w - 1$. Тогда

$$z_{t,s} \leqslant (\lambda(s) + 1)u_s^w - 1 - \sum_{\mu=1}^{\lambda(s)} l_{s,\mu}^w.$$

Так как ксс-цепь $\widehat{U}(w)$ разбивает систему контуров $\widehat{C}(w)$ на блоки, имеем

$$\sum_{s=1}^{r(w)} \sum_{\mu=1}^{\lambda(s)} l_{s,\mu}^w = l_1^w + \dots + l_m^w,$$

откуда получаем

$$z_t \leqslant \sum_{s=1}^{r(w)} (\lambda(s) + 1)u_s^w - r(w) - \sum_{s=1}^{m} l_s^w.$$

Контуры $Z_{t,s}$ смежны с путём w, стало быть, по теореме 2(i) d делит $z_{t,s}$, $s = 1, \dots, r(w)$, а значит, d делит z_t. Так как d делит числа $l_1^w, \dots, l_m^w$,

$$dg\big(l_1^w/d, \dots, l_m^w/d\big) + z_t \leqslant dt_w.$$

Тем самым из (1) следует, что для любого $t \in \mathbb{N}$ подбором коэффициентов получаем $\operatorname{len} v_t$, равную $\operatorname{len} w + dt_w + dt$. Теорема 3 доказана.

Следствие 2. *Если* $\max\big\{u_1^w, \dots, u_{r(w)}^w\big\} = u^w$, *то*

$$t_w \leqslant \lfloor mu^w/d \rfloor + \overline{g}\big(l_1^w/d, \dots, l_m^w/d\big).$$

Доказательство вытекает из условия $\lambda_1^w + \dots + \lambda_{r(w)}^w = m$ и определения числа t_w. Следствие 2 доказано.

Пути $w, w' \in P(i,j)$ назовём *индексно эквивалентными*, если $\operatorname{ind} w = \operatorname{ind} w'$. Класс эквивалентных путей из $P(i,j)$ индекса d обозначим через $P^{(d)}(i,j)$. Множество путей $P(i,j)$ однозначно разбивается на классы эквивалентности в соответствии с их индексами $d_1, \dots, d_k$:

$$P(i,j) = P^{(d_1)}(i,j) \cup \dots \cup P^{(d_k)}(i,j). \tag{2}$$

Индексом множества $P(i,j)$ назовём величину

$$\operatorname{ind} P(i,j) = \operatorname{lcm}\{d_1, \dots, d_k\}.$$

Спектром множества путей W графа Γ назовём множество длин $\operatorname{spc} W = \{\operatorname{len} w : w \in W\}$, и $\operatorname{spc} W$, приведённый $\operatorname{mod} d$, определим как $\operatorname{spc}_d W = \{\operatorname{len} w \pmod d : w \in W\}$; $\overline{\operatorname{spc}}_d W = \mathbb{Z}_d \setminus \operatorname{spc}_d W$ и

$$H(P(i,j)) = \overline{\operatorname{spc}}_{d_1}(P^{(d_1)}(i,j)) \times \dots \times \overline{\operatorname{spc}}_{d_k}(P^{(d_k)}(i,j))$$

в соответствии с (2).

Пусть $d \in \mathbb{N}$, $Y \subset \mathbb{N}$. Множество Y, содержащее полную систему вычетов по модулю d, называется *d-полным*. Для d-полного множества Y обозначим через $\xi_d(Y)$ наименьшее натуральное число такое, что для любого $a \in \{\xi_d(Y), \xi_d(Y)+1, \dots, \xi_d(Y)+d-1\}$ в Y имеется число b такое, что $b \leqslant a$, $b \equiv a \pmod d$.

Лемма 1. *Для d-полного множества Y число $\xi_d(Y)$ — наименьшее, при котором множество $\{b \in Y : b \leqslant \xi_d(Y)\} + d\mathbb{N}_0$ покрывает все натуральные числа, не меньшие $\xi_d(Y)$. Для числа $\xi_d(Y)$ верны оценки*

$$\min Y \leqslant \xi_d(Y) \leqslant \max Y - d + 1.$$

Докажем универсальный критерий локальной примитивности орграфов. Используем обозначения теоремы 3 и для краткости положим $P = P(i,j)$, $P(d) = P^{(d)}(i,j)$, $P(d_\theta) = P^{(d_\theta)}(i,j)$, $\theta = 1,\dots,k$.

Теорема 4. *Орграф* Γ $i \times j$*-примитивен тогда и только тогда, когда выполнено одно из условий*:

(i) *при некотором* $d \in \{d_1,\dots,d_k\}$ *множество* $\{\operatorname{len} w : w \in P(d)\}$, *где* $P(d)$ *определяется разложением* (2), *является* d*-полным, кроме того*

$$\gamma_{i\times j} \leqslant d + \xi_d\Big(\bigcup_{w\in P(d)} \{\operatorname{len} w + dt_w\}\Big);$$

(ii) *при любом наборе чисел* $(b_1,\dots,b_k) \in H(P)$ *система сравнений*

$$\{x \equiv b_\theta \pmod{d_\theta},\ \theta = 1,\dots,k\} \tag{3}$$

не имеет решений по модулю $\delta = \operatorname{ind} P$, *кроме того,*

$$\gamma_{i\times j} \leqslant \xi_\delta\left(\bigcup_{\theta=1}^{k}\ \bigcup_{w_\theta\in P(d_\theta)}\ \bigcup_{\tau=1}^{\delta/d_\theta} \{\operatorname{len} w_\theta + d_\theta(t_{w_\theta} + \tau)\}\right),$$

где $d_\theta = \big(l_1^{w_\theta},\dots,l_{m_\theta}^{w_\theta}\big)$,

$$t_{w_\theta} = \left\lfloor \left(\sum_{s=1}^{r(w_\theta)} \big(\lambda_s^{w_\theta}+1\big)u_s^{w_\theta} - r(w_\theta)\right)/d_\theta \right\rfloor + \overline{g}\big(l_1^{w_\theta}/d_\theta,\dots,l_{m_\theta}^{w_\theta}/d_\theta\big).$$

Доказательство. Пусть в орграфе Γ множество $\{\operatorname{len} w : w \in P(d)\}$ d-полно при некотором $d \in \{d_1,\dots,d_k\}$ (это свойство равносильно равенству $H(P) = \varnothing$). В соответствии с определением индекса пути для каждого $w \in P(d)$ в Γ имеется смежная с путём w система контуров $\widehat{C}(w)$ индекса d. По теореме 3 в Γ есть расширения путей $w \in P(d)$ такие, что объединение множеств их длин покрывает d-полное множество L, где

$$L = \bigcup_{w\in P(d)} \{\operatorname{len} w + dt_w + d\mathbb{N}\} = \bigcup_{w\in P(d)} \{\operatorname{len} w + dt_w\} + d\mathbb{N}.$$

Тогда множество $\bigcup\limits_{w\in P(d)} \{\operatorname{len} w + dt_w\}$ также d-полное, и по лемме 1

$$\gamma_{i\times j} \leqslant \xi_d(L) = d + \xi_d\Big(\bigcup_{w\in P(d)} \{\operatorname{len} w + dt_w\}\Big).$$

Если при любом $d \in \{d_1, \ldots, d_k\}$ множество $\{\operatorname{len} w : w \in P(d)\}$ не d-полное, то $H(P) \neq \varnothing$. Если $b_s \in \overline{\operatorname{spc}}_{d_s}(P(d_s))$, то множество решений сравнения $x \equiv b_\theta \pmod{d_\theta}$ есть множество чисел, не содержащихся в множестве длин путей из $P(d_\theta)$. Тогда $P(d_\theta)$ не содержит путей, длина которых сравнима с $b_\theta + \tau d_\theta$ по модулю $\delta = \operatorname{lcm}\{d_1, \ldots, d_k\}$, $\tau = 0, \ldots, \delta/d_\theta - 1$. Объединяя эти утверждения по $\theta = 1, \ldots, k$, получаем, что множество решений системы сравнений (3) есть множество чисел, не содержащихся в множестве длин путей из $P(i, j)$, т. е. $i \times j$-примитивность графа Γ равносильна при $H(P) \neq \varnothing$ тому, что система (3) не имеет решений при любом наборе $(b_1, \ldots, b_k) \in H(P)$.

Получим оценку $\gamma_{i\times j}$. По теореме 3 в Γ для путей $w_\theta \in P(d_\theta)$ имеются такие расширения, что объединение множеств их длин покрывает множество $\Lambda_\theta = \bigcup\limits_{w_\theta \in P(d_\theta)} \{\operatorname{len} w_\theta + d_\theta t_{w_\theta} + d_\theta \mathbb{N}\}$. В силу теоремы 2(iv) и $i \times j$-примитивности орграфа Γ множество $\bigcup\limits_{\theta=1}^{k} \Lambda_\theta$ δ-полное и $\gamma_{i\times j} \leqslant \xi_\delta\left(\bigcup\limits_{\theta=1}^{k} \Lambda_\theta\right)$ по лемме 1. Используем при $\theta = 1, \ldots, k$ разложения $\Lambda_\theta = \bigcup\limits_{w_\theta \in P(d_\theta)} \bigcup\limits_{\tau=1}^{\delta/d_\theta} \{\operatorname{len} w_\theta + d_\theta(t_{w_\theta} + \tau) + \delta\mathbb{N}_0\}$. Тогда

$$\bigcup_{\theta=1}^{k} \Lambda_\theta = \bigcup_{\theta=1}^{k} \bigcup_{\tau=1}^{\delta/d_\theta} \{\operatorname{len} w_\theta + d_\theta(t_{w_\theta} + \tau) + \delta\mathbb{N}_0\} = \Phi + \delta\mathbb{N}_0,$$

где $\Phi = \bigcup\limits_{\theta=1}^{k} \bigcup\limits_{\tau=1}^{\delta/d_\theta} \{\operatorname{len} w_\theta + d_\theta(t_{w_\theta} + \tau)\}$. Отсюда Φ δ-полное и $\xi_\delta\left(\bigcup\limits_{\theta=1}^{k} \Lambda_\theta\right) = \xi_\delta(\Phi)$. Теорема 4 доказана.

Замечание 2. Система сравнений (3) имеет решение по модулю $\delta = \operatorname{lcm}\{d_1, \ldots, d_k\}$ тогда и только тогда, когда (d_i, d_j) делит разность $b_i - b_j$ для любой пары $i, j \in \{1, \ldots, k\}$ при $i \neq j$ [4].

3. О величине оценки локального экспонента

Теоремы 3 и 4 дают оценку $\gamma_{i\times j}$, зависящую от путей $w \in P(i, j)$ и смежных с ними систем контуров. Отметим свойства полученной оценки.

Утверждение 5. *Если* $\widehat{C}_1, \widehat{C}_2 \in F(w)$, $\operatorname{ind}\widehat{C}_1 = \operatorname{ind}\widehat{C}_2$ *и* $\widehat{C}_1 \subseteq \widehat{C}_2$, *то* $t_w(\widehat{C}_1) \leqslant t_w(\widehat{C}_2)$.

Доказательство. Пусть без ограничения общности $\widehat{C}_1 = \{l_1^w, \dots, l_m^w\}$, $\widehat{C}_2 = \{l_1^w, \dots, l_\mu^w\}$, где $m < \mu$. Пусть $\operatorname{ind}\widehat{C}_1 = \operatorname{ind}\widehat{C}_2 = d$, тогда числа $l_{m+1}^w, \dots, l_\mu^w$ суть линейные комбинации чисел $l_1^w, \dots, l_m^w$. Следовательно, $g(l_1^w/d, \dots, l_m^w/d) = g(l_1^w/d, \dots, l_\mu^w/d)$ и

$$\overline{g}(l_1^w/d, \dots, l_m^w/d) = \overline{g}(l_1^w/d, \dots, l_\mu^w/d) + l_{m+1}^w/d + \dots + l_\mu^w/d.$$

Пусть ксс-цепь $\widehat{U}(w) = \{U_1(w), \dots, U_{r(w)}(w)\}$, имеющая спецификацию $(u_1^w, \dots, u_{r(w)}^w)$, разбивает системы контуров $\widehat{C}_1$ и $\widehat{C}_2$ на подсистемы порядков $\lambda_1^w, \dots, \lambda_{r(w)}^w$ и $\beta_1^w, \dots, \beta_{r(w)}^w$ соответственно, где $\lambda_i^w \leqslant \beta_i^w$, $i = 1, \dots, r(w)$ и $\beta_1^w + \dots + \beta_{r(w)}^w - \lambda_1^w - \dots - \lambda_{r(w)}^w = \mu - m$. Тогда

$$\begin{aligned} t_w(\widehat{C}_2) - t_w(\widehat{C}_1) &= \overline{g}(l_1^w/d, \dots, l_\mu^w/d) - \overline{g}(l_1^w/d, \dots, l_m^w/d) \\ &+ \left\lfloor \left(\sum_{s=1}^{r(w)} (\beta_s^w + 1) u_s^w - r(w) \right)/d \right\rfloor - \left\lfloor \left(\sum_{s=1}^{r(w)} (\lambda_s^w + 1) u_s^w - r(w) \right)/d \right\rfloor \\ &\geqslant \left\lfloor \left(- l_{m+1}^w/d - \dots - l_\mu^w/d + \sum_{s=1}^{r(w)} (\beta_s^w - \lambda_s^w) u_s^w \right)/d \right\rfloor. \end{aligned}$$

Сумма $\sum\limits_{s=1}^{r(w)} (\beta_s^w - \lambda_s^w) u_s^w$ состоит из $\mu - m$ слагаемых вида u_s^w, где u_s^w не меньше длины любого контура из ксс $U_s(w)$, $s = 1, \dots, r(w)$. Следовательно, $t_w(\widehat{C}_2) - t_w(\widehat{C}_1) \geqslant 0$. Утверждение 5 доказано.

Для любого пути $w \in P^{(d)}(i, j)$ множество смежных с w систем контуров индекса d образует верхнюю подполурешётку решётки $F(w)$, множество минимальных элементов подполурешётки обозначим через $F_{\min}^{(d)}(w)$. Из утверждения 5 следует, что оценки $\gamma_{i\times j}$, данные в теореме 4, являются более точными при минимальных системах контуров $\widehat{C} \in F_{\min}^{(d)}(w)$.

Утверждение 6. *Оценка локального экспонента $\gamma_{i\times j}$, полученная в теореме 4 с помощью системы контуров $\widehat{C}(w)$ для пути w индекса d_w с множеством длин $l_1^w, \dots, l_m^w$, при $n \to \infty$ по порядку величины не превосходит $O\big(\max\{mn, d_w \overline{g}(l_1^w/d_w, \dots, l_m^w/d_w)\}\big)$.*

Доказательство. Поскольку $\xi_d(Y) \leqslant \max Y - d + 1$ для любого d-полного множества Y, с учетом теоремы 4 и следствия 2 имеем

$$\gamma_{i\times j} \leqslant 1 + \max_{w\in Q} \{ \operatorname{len} w + m u^w + d_w \overline{g}(l_1^w/d_w, \dots, l_m^w/d_w) \},$$

где $Q = P(d)$, если множество $\{\operatorname{len} w : w \in P(d)\}$ d-полное при некотором $d \in \{d_1, \ldots, d_k\}$, и $Q = P$, если при любом наборе $(b_1, \ldots, b_k) \in H(P)$ система сравнений (3) не имеет решений по $\operatorname{mod}\delta$. В n-вершинном орграфе длина простого пути, число вершин в ксс и величины $d_1, \ldots, d_k$ не превышают n. Значит, при $n \to \infty$ величина оценки $\gamma_{i\times j}$ не превосходит $O\big(\max\{mn, d_w\overline{g}(l_1^w/d_w, \ldots, l_m^w/d_w)\}\big)$. Утверждение 6 доказано.

Замечание 3. Из условия $l_1^w < l_m^w \leqslant n$ и оценки $g(a_1, \ldots, a_m) \leqslant a_1a_m - a_1 - a_m$ [10, теорема 3.1.1] имеем

$$d_w\overline{g}\big(l_1^w/d_w, \ldots, l_m^w/d_w\big) \leqslant l_1^w l_m^w/d_w - l_1^w - l_m^w + d_w - \sum_{s=1}^{m} l_s^w < l_1^w l_m^w/d_w < n^2/d_w.$$

В графе Γ систему $\widehat{C}$ простых контуров длин $l_1, \ldots, l_m$ назовём *примитивной* (*минимальной примитивной*), если $\operatorname{ind}\widehat{C} = 1$ (если любая её собственная подсистема не примитивна). Если система $\widehat{C}$ минимальная примитивная, то $l_j \notin \langle l_1, \ldots, l_{j-1}\rangle$ при $l_1 < \cdots < l_m$, $j = 2, \ldots, m$, иначе $(l_1, \ldots, l_{j-1}) = (l_1, \ldots, l_j)$. Оценим наибольшее возможное число m контуров в минимальной системе.

Пусть $p_1, p_2, \ldots$ — последовательность всех простых чисел в порядке возрастания, т. е. p_i — простое число с номером $i = 1, 2, \ldots$ ($p_1 = 2$, $p_2 = 3$ и т. д.).

Теорема 5. *В n-вершинном примитивном орграфе Γ при $n > 2$ минимальная примитивная система имеет не более m контуров, где m — наибольший номер, при котором $p_2 \ldots p_m \leqslant n$. При $n \to \infty$ справедливо $m = o(\ln n/\ln\ln n)$.*

Доказательство. Числа $l_1, \ldots, l_m$ — длины контуров в n-вершинном примитивном орграфе, т. е. $l_1 < \cdots < l_m \leqslant n$. Наибольшее значение m достигается при наименьших значениях взаимно простых чисел $l_1, \ldots, l_m$. В соответствии с [2, с. 9, 10] m наименьших взаимно простых чисел имеют вид $l_i = p_1 \ldots p_m/p_{m-i+1}$, $i = 1, \ldots, m$. Тогда $l_m = p_2 \ldots p_m \leqslant n$. Из этого неравенства и оценок $p_i > i\ln i$, $i \geqslant 2$, получаем $m!\psi(m) \leqslant n$, где $\psi(m) = \prod\limits_{k=2}^{m} \ln k$. Тогда по формуле Стирлинга имеем $\sqrt{2\pi m}(m/e)^m\psi(m) \leqslant n$. Отсюда $\sqrt{m}(m/e)^m < n$.

При $m = \ln n/\ln\ln n$ и $n \to \infty$ величина $\sqrt{m}(m/e)^m$ растёт быстрее n, значит, $m = o(\ln n/\ln\ln n)$. Теорема 5 доказана.

Из табл. 1 допустимых значений m для некоторых n следует, что $m \leqslant \lceil \ln n \rceil$ при $n \geqslant 3$.

Т а б л и ц а 1

$3 \leqslant n \leqslant 14$	$m = 2$
$15 \leqslant n \leqslant 104$	$m \leqslant 3$
$105 \leqslant n \leqslant 1154$	$m \leqslant 4$
$1155 \leqslant n \leqslant 15014$	$m \leqslant 5$
$15015 \leqslant n \leqslant 255254$	$m \leqslant 6$
$255255 \leqslant n \leqslant 4849844$	$m \leqslant 7$

4. Оценки локальных экспонентов перемешивающего графа преобразования последовательного соединения регистров сдвига

Оценим зависимость выходных знаков от знаков начального состояния для преобразования h генератора, построенного на основе последовательного соединения двоичных регистров правого сдвига длин m и n с булевыми функциями обратной связи $f_1(x_1, \ldots, x_m)$ и $f_2(x_{m+1}, \ldots, x_{m+n})$ соответственно, где $m, n > 1$.

Обозначим через $S(f)$ множество номеров существенных переменных функции f и положим $S(f_1) = \{b_1, \ldots, b_\nu\}$, $S(f_2) = \{c_1, \ldots, c_\mu\}$, где $1 \leqslant b_1 < \cdots < b_{\nu-1} < b_\nu = m$, $m+1 \leqslant c_1 < \cdots < c_{\mu-1} < c_\mu = m+n$, $(b_1, \ldots, b_\nu) = d_1$, $(c_1 - m, \ldots, c_\mu - m) = d_2$. Преобразование h множества V^{m+n} состояний генератора зададим системой булевых координатных функций $\{h_1(x_1, \ldots, x_{m+n}), \ldots, h_{m+n}(x_1, \ldots, x_{m+n})\}$, где

$$h_1(x_1, \ldots, x_{m+n}) = f_1(x_1, \ldots, x_m),$$
$$h_{m+1}(x_1, \ldots, x_{m+n}) = x_m \oplus f_2(x_{m+1}, \ldots, x_{m+n}),$$
$$h_i(x_1, \ldots, x_{m+n}) = x_{i-1}, \quad i = 2, \ldots, m, m+2, \ldots, m+n;$$

в общем случае вместо $\oplus$ может быть использована другая бинарная операция, существенно зависящая от обеих переменных. Таким образом,

$$S(h_1) = S(f_1),\ S(h_{m+1}) = S(f_2) \cup \{m\},$$
$$S(h_i) = \{i-1\}, \quad i = 2, \ldots, m, m+2, \ldots, m+n.$$

Эти равенства определяют множество дуг $(m+n)$-вершинного перемешивающего орграфа $\Gamma(h)$.

Обозначим $I = \{1, \ldots, m\}$, $J = \{m+1, \ldots, m+n\}$. Граф $\Gamma(h)$ есть плотная ксс-цепь $\{\Gamma_I, \Gamma_J\}$ со спецификацией (m, n), где ксс Γ_I содержит контуры длин $b_1, \ldots, b_\nu$, ксс Γ_J содержит контуры длин $c_1 - m, \ldots, c_\mu - m$. Кроме того, в $\Gamma(h)$ имеется дуга $(m, m+1)$.

При начальном состоянии $(x_1, \ldots, x_{m+n})$ генератора i-й знак гаммы равен $\gamma_i = h^i_{m+n}(x_1, \ldots, x_{m+n})$, где $h^i_{m+n}(x_1, \ldots, x_{m+n})$ — булева функция, определяющая $(m+n)$-ю координату преобразования h^i, $i = 1, 2, \ldots$. Исследуем $\mathbb{N}_{m+n} \times \{m+n\}$-примитивность и $I \times \{m+n\}$-примитивность графа $\Gamma(h)$.

Утверждение 7. *Орграф $\Gamma(h)$ $\mathbb{N}_{m+n} \times \{m+n\}$-примитивен тогда и только тогда, когда $d_2 = 1$. В случае $\mathbb{N}_{m+n} \times \{m+n\}$-примитивности верна оценка*

$$\mathbb{N}_{m+n} \times \{m+n\}\text{-}\exp\Gamma(h) \leqslant n + \max\{m, \rho_2\} + g(c_1 - m, \ldots, c_\mu - m),$$

где $\rho_2 = \max\limits_{l \in \mathbb{N}_\mu}\{c_l - c_{l-1}\}$, $c_0 = m$.

Доказательство. В соответствии с теоремой 1 и используемыми в ней обозначениями $K = \{m+n\}$, $\Gamma_K = \Gamma_J$, орграф $\Gamma(h)$ $\mathbb{N}_{m+n} \times \{m+n\}$-примитивен тогда и только тогда, когда ксс Γ_J примитивна. Согласно универсальному критерию примитивности орграфов [10, гл. IV, свойство 11] это равносильно тому, что $d_2 = 1$.

Оценим $\mathbb{N}_{m+n} \times \{m+n\}\text{-}\exp\Gamma(h)$. При $d_2 = 1$ вершина $m+1$ узловая, и в $\Gamma(h)$ для любого $i \in \mathbb{N}_{m+n}$ имеется путь $[i, m+n]$, проходящий через вершину $m+1$. Тогда согласно утверждению 4

$$i \times (m+n)\text{-}\exp\Gamma(h) \leqslant \operatorname{len}[i, m+n] + g(c_1 - m, \ldots, c_\mu - m) + 1.$$

Пусть $[i, m+n] = [i, m+1] \bullet [m+1, m+n]$. Длина кратчайшего пути $[m+1, m+n]$ равна $n-1$ и $\max\limits_{i \in \mathbb{N}_{m+n}} \operatorname{len}[i, m+1] = \max\{m, \rho_2\}$. Тогда

$$\max_{i \in \mathbb{N}_{m+n}} \operatorname{len}[i, m+n] = n - 1 + \max\{m, \rho_2\}.$$

Отсюда и из утверждений 3(i) и 4 получаем нужную оценку. Утверждение 7 доказано.

Следствие 3. *Если $c_1 = m+1$, то $\Gamma(h)$ $\mathbb{N}_{m+n} \times \{m+n\}$-примитивен и*

$$\mathbb{N}_{m+n} \times \{m+n\}\text{-}\exp\Gamma(h) = n - 1 + \max\{m, \rho_2\}.$$

Доказательство. В вершине $m+1$ имеется петля, следовательно, $g(1, c_2 - m, \ldots, c_\mu - m) = -1$. Оценка достигается для вершины 1, если $m \geqslant \rho_2$, и для вершины $c_j + 1$ в противном случае, где $c_j < m+n$ и $c_{j+1} - c_j = \rho_2$. Следствие 3 доказано.

Утверждение 8. *Орграф* $\Gamma(h)$ $I\times\{m+n\}$*-примитивен тогда и только тогда, когда* $(d_1,d_2)=1$. *В случае* $I\times\{m+n\}$*-примитивности верна оценка*

$$I\times\{m+n\}\text{-}\exp\Gamma(h)\leqslant m+n+\rho_1+g(b_1,\dots,b_\nu,c_1-m,\dots,c_\mu-m),$$

где $\rho_1=\max\limits_{l\in\mathbb{N}_\nu}\{b_l-b_{l-1}\}$, $b_0=1$.

Доказательство. При любом $i\in I$ для всех путей $w\in P(i,m+n)$ имеется единственная плотная $i\times(m+n)$-связывающая ксс-цепь $\{\Gamma_I,\Gamma_J\}$ со спецификацией (m,n), смежная с w. Все простые пути $w\in P(i,m+n)$ имеют индекс $d=(d_1,d_2)$. Следовательно, соответствующее разбиение (2) содержит единственный класс эквивалентности. Тогда по теореме 4 для любого $i\in I$ орграф $\Gamma(h)$ $i\times(m+n)$-примитивен в том и только том случае, когда множество $\operatorname{spc}P(i,m+n)$ d-полное. Поскольку все пути $w\in W(i,m+n)$ проходят через контуры ксс Γ_I, Γ_J и только через них, множество $\operatorname{spc}P(i,m+n)$ d-полно лишь при $d=1$. Значит, по утверждению 3(i) граф $\Gamma(h)$ $I\times\{m+n\}$-примитивен тогда и только тогда, когда $d=(d_1,d_2)=1$.

Оценим величину $I\times\{m+n\}\text{-}\exp\Gamma(h)$. Заметим, что через вершину 1 проходят контуры длин $b_1,\dots,b_\nu$, через вершину $m+1$ проходят контуры длин $c_1-m,\dots,c_\mu-m$. Тогда путь $[i,m+n]$ при любом $i\in I$ построим с помощью конкатенации путей:

$$[i,m+n]=[i,1]\bullet C(1)\bullet[1,m+1]\bullet C(m+1)\bullet[m+1,m+n],\qquad(4)$$

где $C(1)$ и $C(m+1)$ — конкатенации некоторого числа простых контуров длин $b_1,\dots,b_\nu$ и $c_1-m,\dots,c_\mu-m$ соответственно. Заметим, что $\max\limits_{i\in I}\operatorname{len}[i,1]=\rho_1$, $\operatorname{len}[1,m+1]=m$, $\operatorname{len}[m+1,m+n]=n-1$ и при $d=1$ величина $\operatorname{len}C(1)+\operatorname{len}C(m+1)$ с помощью варьирования кратностей прохождения простых контуров может принимать любое значение, большее $g(b_1,\dots,b_\nu,c_1-m,\dots,c_\mu-m)$. Следовательно, в соответствии с (4) $\operatorname{len}[i,m+n]$ при всех $i\in I$ с помощью варьирования кратностей прохождения простых контуров может принимать любое значение $t\geqslant g(b_1,\dots,b_\nu,c_1-m,\dots,c_\mu-m)+m+n+\rho_1$. Утверждение 8 доказано.

Следствие 4. (i) *Если* $b_1=1$, *то орграф* $\Gamma(h)$ $I\times\{m+n\}$*-примитивен и*

$$I\times\{m+n\}\text{-}\exp\Gamma(h)=\rho_1+m+n-1.$$

(ii) *Если* $c_1=m+1$, *то орграф* $\Gamma(h)$ $I\times\{m+n\}$*-примитивен и*

$$I\times\{m+n\}\text{-}\exp\Gamma(h)=m+n-1.$$

Доказательство. (i) Если $b_1 = 1$, то в вершине 1 имеется петля и $g(b_1, \ldots, b_\nu,\, c_1 - m, \ldots, c_\mu - m) = -1$. Значение локального экспонента $\rho_1 + m + n - 1$ достигается для вершины $b_j + 1$, где $b_j < m$ и $b_{j+1} - b_j = \rho_1$.

(ii) Если $c_1 = m + 1$, то в вершине $m + 1$ имеется петля и упрощается формула (4):

$$[i, m+n] = [i, m+1] \bullet C(m+1) \bullet [m+1, m+n],$$

где $C(m+1)$ — контур, полученный при кратном прохождении петли в вершине $m+1$. Отсюда $\operatorname{len}[i, m+n] \leqslant m + n - i$ и максимум по всем $i \in I$, равный $m+n-1$, достигается для вершины 1. Следствие 4 доказано.

Рассмотрим числовые примеры. Используем утверждения 7, 8 и следствия 3, 4 для получения верхних оценок локальных экспонентов $\Gamma(h)$ (табл. 2).

Таблица 2

	$m = 18,\ n = 25,$ $S(f_1) = \{2, 18\},$ $S(f_2) = \{23, 43\}$	$m = 20,\ n = 25,$ $S(f_1) = \{3, 20\},$ $S(f_2) = \{30, 45\}$
$(\rho_2, d_2, g(c_1 - m, c_2 - m))$	$(20, 5, *)$	$(15, 5, *)$
$\mathbb{N}_{m+n} \times \{m+n\}\text{-}\exp\Gamma(h)$	∞	∞
$(\rho_1, d_1, g(b_1, b_2, c_1 - m, c_2 - m))$	$(16, 2, 3)$	$(17, 1, 17)$
$I \times \{m+n\}\text{-}\exp\Gamma(h)$	$\leqslant 62$	$\leqslant 79$
	$m = 20,\ n = 25,$ $S(f_1) = \{10, 20\},$ $S(f_2) = \{23, 45\}$	$m = 20,\ n = 25,$ $S(f_1) = \{10, 20\},$ $S(f_2) = \{21, 45\}$
$(\rho_2, d_2, g(c_1 - m, c_2 - m))$	$(22, 1, 47)$	$(24, 1, -1)$
$\mathbb{N}_{m+n} \times \{m+n\}\text{-}\exp\Gamma(h)$	$\leqslant 94$	$\leqslant 48$
$(\rho_1, d_1, g(b_1, b_2, c_1 - m, c_2 - m))$	$(10, 10, 17)$	$(10, 10, -1)$
$I \times \{m+n\}\text{-}\exp\Gamma(h)$	$\leqslant 72$	$= 44$

В статье изложены свойства локальной примитивности матриц и орграфов. Получен критерий локальной примитивности орграфа, который определяется свойствами соответствующих ксс-цепей. Получены оценки локальных экспонентов. На основе данных результатов получены критерий локальной примитивности и оценки локальных экспонентов для перемешивающего графа преобразования последовательного соединения регистров сдвига. Изложенные результаты могут быть использованы в том числе при исследовании перемешивающих свойств других криптографических преобразований.

ЛИТЕРАТУРА

1. **Когос К. Г., Фомичёв В. М.** Положительные свойства неотрицательных матриц // Прикл. дискрет. математика. 2012. № 4. С. 5–13.
2. **Кяжин С. Н., Фомичёв В. М.** О примитивных наборах натуральных чисел // Прикл. дискрет. математика. 2012. № 2. С. 5–14.
3. **Кяжин С. Н., Фомичёв В. М.** Локальная примитивность графов и неотрицательных матриц // Прикл. дискрет. математика. 2014. № 3. С. 68–80.
4. **Окунев Л. Я.** Краткий курс теории чисел. М.: Учпедгиз, 1956. 239 с.
5. **Сачков В. Н., Тараканов В. Е.** Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 269 с.
6. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. No. 14. P. 483–499.
7. **Huang Y., Liu B.** Generalized r-exponents of primitive digraphs // Taiwanese J. Math. 2011. Vol. 15, No. 5. P. 1999–2012.
8. **Liu B.** Generalized exponents of Boolean matrices // Linear Algebra Appl. 2003. No. 373. P. 169–182.
9. **Miao Z., Zhang K.** The local exponent sets of primitive digraphs // Linear Algebra Appl. 2000. No. 307. P. 15–33.
10. **Ramírez Alfonsín J. L.** The Diophantine Frobenius problem. Oxford: Oxf. Univ. Press, 2005. 243 p. (Oxf. Lect. Ser. Math. Appl.; Vol. 30).
11. **Shao J., Wang J., Li G.** Generalized primitive exponents with the complete characterization of the extremal digraphs // Chinese J. Contemp. Math. 1994. Vol. 15, No. 4. P. 317–324.
12. **Shen J., Neufeld S.** Local exponents of primitive digraphs // Linear Algebra Appl. 1998. Vol. 268. P. 117–129.

Фомичёв Владимир Михайлович,
Кяжин Сергей Николаевич

Статья поступила
7 декабря 2015 г.

Исправленный вариант —
9 июня 2016 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
January–March 2017. Volume 24, No. 1. P. 97–119

UDC 519.17 DOI: 10.17377/daio.2017.24.519

LOCAL PRIMITIVITY OF MATRICES AND GRAPHS

V. M. Fomichev[1,2,a], *S. N. Kyazhin*[2,3,b]

[1]Financial University under the Government of the Russian Federation,
49 Leningradsky Ave., 125993 Moscow, Russia,
[2]National Research Nuclear University MEPhI,
31 Kashirskoe Highway, 115409 Moscow, Russia,
[3]Special Development Center of the Ministry of Defence of the Russian Federation,
21 Svobody St., 125362 Moscow, Russia
E-mail: [a]fomichev@nm.ru, [b]s.kyazhin@kaf42.ru

Abstract. We develop a matrix-graph approach to the estimation of the communicative properties of a system of connected objects. In particular, this approach can be applied to analyzing the mixing properties of iterative cryptographic transformations of binary vector spaces, i. e. dependence of the output block bits on the input bits. In some applied problems, the saturation of the connections between the objects corresponds to the required level if the matrix modeling the connections or its certain submatrix is positive (the graph modeling the connections or its certain subgraph is complete). The concepts of local primitivity and local exponents of a nonnegative matrix (graph) are introduced. These concepts generalize and expand the area of application as compared to the familiar concepts of primitivity and exponent. We obtain a universal criterion for the local primitivity of a digraph and both a universal bound for the local exponents and its refinements for various particular cases. The results are applied to analyzing the mixing properties of a cryptographic generator constructed on the basis of two shift registers. Tab. 2, bibliogr. 12.

Keywords: primitive matrix, primitive graph, exponent, local primitivity of a matrix (graph), local exponent.

REFERENCES

1. **K. G. Kogos** and **V. M. Fomichev,** Positive properties of nonnegative matrices, *Prikl. Diskretn. Mat.,* No. 4, 5–13, 2012 [Russian].
2. **S. N. Kyazhin** and **V. M. Fomichev,** On primitive sets of natural numbers, *Prikl. Diskretn. Mat.,* No. 2, 5–14, 2012 [Russian].
3. **S. N. Kyazhin** and **V. M. Fomichev,** Local primitiveness of graphs and nonnegative matrices, *Prikl. Diskretn. Mat.,* No. 3, 68–80, 2014 [Russian].

4. **L. Ya. Okunev,** *Kratkii kurs teorii chisel* (A Brief Course in Number Theory), Uchpedgiz, Moscow, 1956 [Russian].
5. **V. N. Sachkov** and **V. E. Tarakanov,** *Kombinatorika neotritsatel'nykh matrits,* TVP, Moscow, 2000 [Russian]. Translated under the title *Combinatorics of nonnegative matrices,* AMS, Providence, 2002 (Transl. Math. Monogr., Vol. 213).
6. **R. A. Brualdi** and **B. Liu,** Generalized exponents of primitive directed graphs, *J. Graph Theory,* **14**, 483–499, 1990.
7. **Y. Huang** and **B. Liu,** Generalized r-exponents of primitive digraphs, *Taiwan. J. Math.,* **15**, No. 5, 1999–2012, 2011.
8. **B. Liu,** Generalized exponents of Boolean matrices, *Linear Algebra Appl.,* **373**, 169–182, 2003.
9. **Z. Miao** and **K. Zhang,** The local exponent sets of primitive digraphs, *Linear Algebra Appl.,* **307**, 15–33, 2000.
10. **J. L. Ramírez Alfonsín,** *The Diophantine Frobenius Problem,* Oxf. Univ. Press, Oxford, 2005 (Oxf. Lect. Ser. Math. Appl., Vol. 30).
11. **J. Shao, J. Wang,** and **G. Li,** Generalized primitive exponents with complete characterizations of the extreme digraphs, *Chin. Ann. Math., Ser. A,* **15**, No. 5, 518–523, 1994 [Chinese]. Translated in *Chin. J. Contemp. Math.,* **15**, No. 4, 317–324, 1994.
12. **J. Shen** and **S. Neufeld,** Local exponents of primitive digraphs, *Linear Algebra Appl.,* **268**, 117–129, 1998.

Vladimir M. Fomichev,
Sergey N. Kyazhin

Received
7 December 2015

Revised
9 June 2016