

ПОЛУГРУППОВЫЕ И МЕТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЛОКАЛЬНО ПРИМИТИВНЫХ МАТРИЦ И ОРГРАФОВ^{*)}

В. М. Фомичёв^{1,2,3}

¹Финансовый университет при Правительстве РФ,
Ленинградский пр., 49, 125993 Москва, Россия

²Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, 115409 Москва, Россия

³Институт проблем информатики ФИЦ ИУ РАН,
ул. Вавилова, 44, корп. 2, 119333 Москва, Россия

E-mail: fomichev@nm.ru

Аннотация. Понятие локальной примитивности квадратной 0,1-матрицы порядка n обобщено на случай произвольной части матрицы, не обязательно являющейся прямоугольной подматрицей. Аналогичное обобщение выполнено для произвольного множества B пар начальных и конечных вершин путей в n -вершинном орграфе, $B \subseteq \{(i, j) \mid 1 \leq i, j \leq n\}$. Установлена связь локального B -экспонента матрицы (орграфа) с такими её характеристиками, как циклическая глубина и период, число не примитивных матриц и число неидемпотентных матриц в мультипликативной полугруппе всех квадратных 0,1-матриц порядка n и др. Для широкого класса орграфов, важного для криптографических приложений, получены критерии B -примитивности и верхняя оценка B -экспонента.

Введены новые метрические характеристики локально примитивного орграфа Γ : k, r -экспорадиус, k, r -экспоцентр, где $1 \leq k, r \leq n$, и матэкс — матрица порядка n всех локальных экспонентов орграфа Γ . Дан пример расчёта матэкса для n -вершинного орграфа Виландта. С использованием введённых характеристик предложена идея построения алгоритмически реализуемых s -боксов (элементов раундовых функций блочных шифров) с относительно широким диапазоном размеров. Табл. 2, ил. 1, библиогр. 13.

Ключевые слова: перемешивающая матрица, примитивная матрица, локально примитивная матрица, экспонент матрицы, циклическая полугруппа матриц.

^{*)}Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 16-01-00226).

Основные обозначения

В статье используются следующие обозначения: \mathbb{N} — множество натуральных чисел, $n \in \mathbb{N}$, $\mathbb{N}_n = \{1, \dots, n\}$, V_n — множество двоичных n -мерных векторов, $M_n^{0,1}$ — множество 0,1-матриц порядка $n > 1$, $\exp M$ ($\exp \Gamma$) — экспонент матрицы M (орграфа Γ), $[i, j]$ — путь в орграфе из вершины i в вершину j , $\rho[i, j]$ — длина кратчайшего пути из вершины i в вершину j , ксс — компонента сильной связности.

Введение

Для симметричных криптосистем, построенных на основе итераций преобразования g двоичного векторного пространства, положительным синтезным свойством является, как правило, существенная зависимость от определённого подмножества булевых входных переменных заданного подмножества координатных функций преобразования g^t , $t \in \mathbb{N}$. В рамках матрично-графового подхода (МГП) это свойство оценивается как положительность определённого множества элементов в степенях перемешивающей матрицы преобразования $M(g^t)$, $M(g^{t+1})$, ... (наличие определённого множества дуг в степенях перемешивающего орграфа $\Gamma(g^t)$, $\Gamma(g^{t+1})$, ...) для некоторого $t \in \mathbb{N}$. Применение МГП состоит в распознавании локальной примитивности матриц и графов и определении их экспонентов.

Следует отметить, что МГП активно применяется в криптографии, в частности, для исследования регистровых преобразований двоичных векторных пространств, соответствующих обобщённым сетям Фейстеля различных типов [7, 13]. С использованием результатов исследования перемешивающих графов оценены криптографические свойства блочных алгоритмов TWINE (2012 г.) и Lilliput (2016 г.), разработанных для защиты информации в условиях ограниченных ресурсов пользователя [6].

Первые результаты по обобщению понятия экспонента орграфа публиковались, начиная с 1990-х гг. [8, 11, 12]. Они относились только к примитивным орграфам и характеризовали длины путей из заданной вершины (или из некоторой вершины заданного множества) во все вершины орграфа. Дальнейшие обобщения такого рода исследованы в [9, 10].

В [1] представлены более общие определения локальной примитивности матриц и орграфов и связанные с этим обобщением первые результаты. Пусть $\emptyset \neq I, J \subseteq \mathbb{N}_n$, обозначим через $M(I \times J)$ матрицу, полученную из матрицы M удалением всех строк с номерами $i \notin I$ и всех столбцов с номерами $j \notin J$. Неотрицательная матрица M называется $I \times J$ -примитивной, если при некотором $\gamma \in \mathbb{N}$ для любого $t \geq \gamma$ положи-

тельна подматрица $M^t(I \times J)$ (орграф Γ называется $I \times J$ -примитивным, если при всех $t \geq \gamma$ в орграфе Γ имеется путь длины t из любой вершины множества I в любую вершину множества J). Наименьшее такое γ называется $I \times J$ -экспонентом матрицы M (орграфа Γ) и обозначается через $I \times J$ -ехр M ($I \times J$ -ехр Γ). Эти определения локальной примитивности и локального экспонента применимы и к не примитивным орграфам, а соответствующие орграфы названы *локально примитивными*. Результаты по локальной примитивности орграфов получили развитие в [4], в частности, для орграфов получены универсальный критерий локальной примитивности орграфа и оценка локального экспонента. Заметим, что матричная интерпретация этих результатов весьма сложна, несмотря на естественную биекцию множеств n -вершинных орграфов и 0,1-матриц порядка n (матриц смежности вершин графов).

В данной статье в отношении локальной примитивности и локальных экспонентов матриц и орграфов получено дальнейшее обобщение, связанное с произвольно заданным множеством элементов матрицы (пар конечных и начальных вершин путей в орграфе). Установлена связь локальных экспонентов неотрицательной матрицы с её полугрупповыми характеристиками. Введены новые метрические характеристики примитивных и локально примитивных орграфов: экспорадиус, экспоцентр и матэкс орграфа (неотрицательной матрицы), определяющий все локальные экспоненты. В качестве примера рассчитан матэкс n -вершинного орграфа Виландта. С использованием введённых характеристик изложена идея построения алгоритмически реализуемых s -боксов (раундовых функций блочных шифров). Некоторые результаты, связанные с новыми метрическими характеристиками локально примитивных орграфов, докладывались на конференции SIBECRYPT'17 [2].

1. Обобщение понятия локальной примитивности матрицы и связь локальных экспонентов матрицы с её полугрупповым типом

Пусть $\emptyset \neq B \subseteq \mathbb{N}_n^2$, $M = (m_{i,j})$. Без ограничения общности положим, что M есть 0,1-матрица порядка $n > 1$, $M(B) = \{m_{i,j} \mid (i,j) \in B\}$ — непустая часть матрицы M .

Матрица M *положительная* (записывается $M > 0$), если все её элементы положительны. Матрица M называется *B -положительной* (записывается $M(B) > 0$), если положительными являются все элементы множества $M(B)$. Матрица M называется *B -ненулевой* (записывается $M(B) \neq 0$), если множество $M(B)$ содержит положительные эле-

менты. Число различных B -положительных 0,1-матриц равно 2^h , где $h = n^2 - |B|$.

Далее рассматривается логическое умножение 0,1-матриц, т. е. результат умножения 0,1-матриц M_1 и M_2 получается из целочисленной матрицы $M_1 M_2$ с помощью замены положительных элементов единицами.

Введём следующие обозначения: $\langle M \rangle$ — циклическая полугруппа по умножению, порождённая матрицей M , G_M — максимальная подгруппа полугруппы $\langle M \rangle$, (d, p) — тип матрицы M , где d и p — циклическая глубина и период матрицы M соответственно.

Полугруппа $\langle M \rangle$ конечна для любой матрицы M [5, с. 74, 75]:

$$\begin{aligned}\langle M \rangle &= \{M^t, t = 1, \dots, d + p - 1\}, \\ G_M &= \{M^t, t = d, \dots, d + p - 1\}.\end{aligned}$$

Определяющее соотношение полугруппы $\langle M \rangle$ имеет вид

$$M^d = M^{d+p}. \quad (1)$$

Матрица M называется B -примитивной, если существует такое число $\gamma \in \mathbb{N}$, что матрица M^t является B -положительной при любом $t \geq \gamma$. Наименьшее такое число γ обозначим через B -ехр M (кратко γ_B , в частности, $\gamma_{i,j}$ при $B = \{(i, j)\}$) и назовём *локальным B -экспонентом*, или просто *B -экспонентом* матрицы M (в частности, *(i, j) -экспонентом*). Если матрица M не B -примитивная, то полагаем $\gamma_B = \infty$. В случае $B = I \times J$, где $I, J \subseteq \mathbb{N}_n$, $M(B) = M(I \times J)$, B -примитивность равносильна $I \times J$ -примитивности, определённой в [1]. Если $B = I^2$, то B -примитивность матрицы M равносильна её I^2 -примитивности.

По определению матрица M будет B -примитивной тогда и только тогда, когда M является (i, j) -примитивной при любой паре $(i, j) \in B$, при этом B -ехр $M = \max_{(i,j) \in B} (i, j)$ -ехр M .

Число единиц в непримитивной матрице M не больше $n^2 - n + 1$ (С. Н. Кяжин). Отсюда для непримитивных матриц M , являющихся B -примитивными, следует ограничение на $|B|$.

Утверждение 1. Если непримитивная матрица M является B -примитивной, то верна достижимая оценка $|B| \leq n^2 - n + 1$.

Оценка из утверждения 1 достигается, например, на множестве

$$B = \{(1, 1), (i, j), i = 2, \dots, n, j = 1, \dots, n\}.$$

Утверждение 2. Если $B = B_1 \cup \dots \cup B_k$, где $\emptyset \neq B_i \subset \mathbb{N}_n^2$ для $i = 1, \dots, k$, то матрица M является B -примитивной тогда и только тогда, когда M является B_i -примитивной, $i = 1, \dots, k$.

Характеристики примитивности и локальной примитивности матрицы связаны с её полугрупповым типом. Из определения примитивной матрицы M имеем $p = 1$ и с учётом универсальной оценки экспонента $d = \exp M \leq n^2 - 2n + 2$.

В моноиде $M_n^{0,1}$ введём следующие обозначения: π_n — число непримитивных 0,1-матриц, $\pi_n(B)$ — число непримитивных B -положительных матриц, I_n — число идемпотентов, $I_n(B)$ — число B -положительных идемпотентов.

Теорема 1. Пусть M — непримитивная матрица типа (d, p) . Тогда

(а) $d + p \leq \pi_n - I_n + 3$;

(б) M является B -примитивной тогда и только тогда, когда группа G_M состоит из B -положительных матриц, при этом $p \leq \pi_n(B) - I_n(B) + 2$ и $B\text{-exp } M$ равен наименьшему $\gamma \in \{1, \dots, d\}$ такому, что $M^r(B) > 0$, $r = \gamma, \dots, d$.

ДОКАЗАТЕЛЬСТВО. (а) Полугруппа $\langle M \rangle$ состоит из непримитивных матриц, иначе было бы противоречие с примитивностью матрицы M . Все матрицы полугруппы $\langle M \rangle$ различны в силу (1). Значит, $d + p - 1 \leq \pi_n$.

Уточним оценку. Для любой матрицы $M \in M_n^{0,1}$ полугруппа $\langle M \rangle$ содержит единственный непримитивный идемпотент, т. е. единственный идемпотент, отличный от матрицы, состоящей из единиц. Следовательно, $\text{ord } \langle M \rangle \leq \pi_n - (I_n - 2)$. Отсюда $d + p \leq \pi_n - I_n + 3$.

(б) В силу (1) последовательность матриц $\{M^t, t = 1, 2, \dots\}$ периодическая с длинами предпериода и периода $d - 1$ и p соответственно. Последовательность частей матриц $\{M^t(B), t = 1, 2, \dots\}$ также периодическая с длиной предпериода $d(B) - 1$, где $d(B) \leq d$, и с длиной периода $p(B)$, где $p(B)$ делит p [5, с. 135]. В случае B -примитивной матрицы M получаем, что $p(B) = 1$ и $B\text{-exp } M$ равен наименьшему числу γ из множества $\{1, \dots, d\}$ такому, что $M^t(B) > 0$ при $t = \gamma, \dots, d$, так как B -положительными могут быть матрицы M^t при некоторых $t < d$. Заметим, что матрица M является B -примитивной тогда и только тогда, когда группа G_M состоит из B -положительных 0,1-матриц. Поскольку G_M содержит единственный B -положительный непримитивный идемпотент, отличный от матрицы, состоящей из единиц, то

$$p \leq \pi_n(B) - (I_n(B) - 2) = \pi_n(B) - I_n(B) + 2.$$

Теорема 1 доказана.

Проиллюстрируем полученные оценки на примере.

Пример 1. Пусть

$$B = \{(1, 1), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}, \quad B' = \{(3, 4), (4, 3)\}.$$

Распознаем B -примитивность и B' -примитивность матрицы M , где

$$m_{1,1} = m_{1,3} = m_{2,2} = m_{2,4} = m_{3,4} = m_{4,3} = 1,$$

а остальные элементы равны 0. Вычислим несколько степеней матрицы M до первого повтора:

$$M = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad M^2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$M^4 = M^2.$$

Отсюда $d = p = 2$, $G_M = \{M^2, M^3\}$. Тогда по теореме 1 матрица M является B -примитивной и не является B' -примитивной, $B\text{-exp } M = 2$.

Пример 2. В таблице 1 приведены B -примитивные непримитивные матрицы M порядка 2 и их полугрупповые характеристики.

Т а б л и ц а 1

M	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$
(d, p)	(1,1)	(1,1)	(1,1)	(1,1)	(1,1)
B	$\{(1, 1)\}$	$\{(2, 2)\}$	$\{(1, 1), (1, 2)\}$	$\{(1, 1), (2, 2)\}$	$\{(1, 1), (2, 1)\}$
M	$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	
(d, p)	(1,1)	(1,1)	(1,1)	(1,1)	
B	$\{(1, 2), (2, 2)\}$	$\{(2, 1), (2, 2)\}$	$\{(1, 1), (2, 1), (2, 2)\}$	$\{(1, 1), (1, 2), (2, 2)\}$	

Расчёты показывают, что $\pi_2 = 13$, $I_2 = 11$. Следовательно, для каждой непримитивной матрицы порядка 2 выполнено неравенство (а) из теоремы 1: $d + p \leq \pi_2 - I_2 + 3 = 5$. Для каждой не примитивной, но B -примитивной матрицы порядка 2 при всех указанных B выполнено неравенство (б) из теоремы 1: $p \leq \pi_2(B) - I_2(B) + 2$.

2. Свойства B -примитивных матриц и орграфов

Введём следующие обозначения: $M^t = (m_{i,j}^{(t)})$, для $(i, j) \in B$

$$I(B, j) = \{\mu \in \mathbb{N}_n \mid (\mu, j) \in B\}, \quad J(B, i) = \{\nu \in \mathbb{N}_n \mid (i, \nu) \in B\},$$

$$I(B) = \bigcup_{j: (i,j) \in B} I(B, j), \quad J(B) = \bigcup_{i: (i,j) \in B} J(B, i),$$

\tilde{U}_B — m -вершинный орграф с множеством дуг B и множеством вершин $U = I(B) \cup J(B)$, $m \leq n$. Отсюда $I(B)$ и $J(B)$ суть наименьшие подмножества множества \mathbb{N}_n такие, что $B \subseteq I(B) \times J(B)$.

Утверждение 3. Все вершины орграфа \tilde{U}_B циклические тогда и только тогда, когда $I(B) = J(B)$.

ДОКАЗАТЕЛЬСТВО. Любая циклическая вершина i орграфа имеет входящую дугу и исходящую дугу, тогда (μ, i) и (i, ν) суть дуги орграфа \tilde{U}_B при любом $i \in I(B) \cup J(B)$ и при некоторых $\mu, \nu \in I(B) \cup J(B)$. Отсюда $i \in J(B, \mu) \cap I(B, \nu)$, следовательно, $i \in I(B)$ и $i \in J(B)$. В силу произвольности рассмотренной вершины i получаем, что $I(B) = J(B)$. В обратную сторону доказательство симметрично. Утверждение 3 доказано.

Следующая теорема является обобщением утверждения 1(а) в [1].

Теорема 2. Если матрица M для любой пары $(i, j) \in B$ является $J(B, i)$ -ненулевой или $I(B, j)$ -ненулевой, то матрица M является B -примитивной и B -exp M равен наименьшему натуральному числу γ , при котором $M^\gamma(B) > 0$.

ДОКАЗАТЕЛЬСТВО. По правилу умножения неотрицательных матриц имеем

$$m_{i,j}^{(t+1)} = m_{i,1}m_{1,j}^{(t)} + \cdots + m_{i,n}m_{n,j}^{(t)} \geq \sum_{s \in J(B,i)} m_{i,s}m_{s,j}^{(t)}, \quad t \geq 1, \quad (2)$$

$$m_{i,j}^{(t+1)} = m_{i,1}^{(t)}m_{1,j} + \cdots + m_{i,n}^{(t)}m_{n,j} \geq \sum_{s \in I(B,j)} m_{i,s}^{(t)}m_{s,j}, \quad t \geq 1. \quad (3)$$

Пусть $(i, j) \in B$. Если матрица M является $J(B, i)$ -ненулевой, то в множестве $\{m_{i,s} \mid s \in J(B, i)\}$ содержится положительное число. Тогда при $M^t(B) > 0$ в соответствии с (2) получаем $m_{i,j}^{(t+1)} > 0$. Если M является $I(B, j)$ -ненулевой, то в множестве $\{m_{s,j} \mid s \in I(B, j)\}$ содержится положительное число. Тогда при $M^t(B) > 0$ в соответствии с (3) получаем $m_{i,j}^{(t+1)} > 0$. Следовательно, $m_{i,j}^{(t+1)} > 0$ для любой пары $(i, j) \in B$.

Отсюда если $M^\gamma(B) > 0$, то $M^t(B) > 0$ при любом $t \geq \gamma$. Теорема 2 доказана.

Пример 3. Для матрицы M и множества B из примера 1 вычислим

$$\begin{aligned} I(B, 1) &= \{1\}, & I(B, 2) &= \{2\}, & I(B, 3) &= \{1, 4\}, \\ I(B, 4) &= \{2, 3\}, & J(B, 1) &= \{1, 3\}, & J(B, 2) &= \{2, 4\}. \end{aligned}$$

Матрица M для пар $(1, 1)$, $(1, 3)$ и $(1, 4)$ является $J(B, 1)$ -ненулевой, а для пар $(2, 2)$, $(2, 3)$, $(2, 4)$ — $J(B, 2)$ -ненулевой. Тогда по теореме 2 матрица M будет B -примитивной. Поскольку M не B -положительная и $M^2(B) > 0$, то $B\text{-exp } M = 2$.

Получим достаточное условие B -примитивности орграфа. Допустим, что $Y \subseteq \mathbb{N}_n$. Обозначим через $D(\Gamma, i)$ и $D(\Gamma, Y)$ множества вершин орграфа Γ , из которых достижима вершина i и множество Y соответственно; через $D(j, \Gamma)$ и $D(Y, \Gamma)$ — множества вершин орграфа Γ , которые достижимы из вершины j и из некоторой вершины множества Y соответственно; через $\text{len } w$ — длину пути w в орграфе Γ ; через \bullet — операцию конкатенации путей в орграфе Γ , которая определена на паре путей (u, v) тогда и только тогда, когда конечная вершина пути u совпадает с начальной вершиной пути v , и если $w = u \bullet v$, то $\text{len } w = \text{len } u + \text{len } v$.

В орграфе Γ ксс U называется i, j -связывающей (кратко i, j -ксс), если имеется путь $[i, j]$, проходящий через некоторую вершину ксс U .

Вершину орграфа назовём *существенной*, если она или достижима из некоторой ксс или из неё достижима некоторая ксс. В противном случае вершину назовём *несущественной*. В ациклическом орграфе все вершины *несущественные*.

Теорема 3. (а) Если вершина i орграфа Γ несущественная, то Γ не является (i, j) -примитивным и (j, i) -примитивным при любой вершине j .

(б) Если орграф Γ (i, j) -примитивный, то Γ является (μ, j) -примитивным для любой $\mu \in D(\Gamma, i)$ и (i, ν) -примитивным для любой $\nu \in D(j, \Gamma)$, при этом $\gamma_{\mu, j} \leq \rho[\mu, i] + \gamma_{i, j}$ и $\gamma_{i, \nu} \leq \gamma_{i, j} + \rho[j, \nu]$.

(в) Орграф Γ (i, j) -примитивный, если найдётся такая вершина $\mu \in D(i, \Gamma) \cap D(\Gamma, j)$, что орграф Γ является (i, μ) -примитивным или (μ, j) -примитивным, при этом $\gamma_{i, j} \leq \gamma_{i, \mu} + \rho[\mu, j]$ или $\gamma_{i, j} \leq \rho[i, \mu] + \gamma_{\mu, j}$ соответственно.

ДОКАЗАТЕЛЬСТВО. (а) Если вершина i орграфа Γ несущественная, то Γ не содержит (i, j) -связывающей ксс при любой вершине j . Это

не совместимо с (i, j) -примитивностью и (j, i) -примитивностью при любой вершине j орграфа Γ .

(б) В орграфе Γ из любой вершины μ множества $D(\Gamma, i)$ имеется путь $[\mu, i]$. Если орграф Γ (i, j) -примитивный, то в нём имеются пути w_t длины t из i в j для любого $t \geq \gamma_{i,j}$. Используя конкатенацию путей, получаем, что для любой вершины μ множества $D(\Gamma, i)$ в Γ имеются пути $[\mu, i] \bullet w_t$ длины $\rho[\mu, i] + t$ из μ в j при любом $t \geq \gamma_{i,j}$. Отсюда

$$\gamma_{\mu,j} \leq \rho[\mu, i] + \gamma_{i,j}.$$

Свойство (i, μ) -примитивности для любого $\mu \in D(j, \Gamma)$ и неравенство $\gamma_{i,\mu} \leq \gamma_{i,j} + \rho[j, \mu]$ доказываются двойственно.

(в) Если орграф Γ (i, μ) -примитивный для некоторого $\mu \in D(i, \Gamma) \cap D(\Gamma, j)$, то в Γ существуют пути w_t длины t из i в μ для любого $t \geq \gamma_{i,\mu}$ и путь $[\mu, j]$ длины $\rho[\mu, j]$. Значит, в Γ имеются пути $w_t \bullet [\mu, j]$ длины $t + \rho[\mu, j]$ при любом $t \geq \gamma_{i,\mu}$. Отсюда орграф Γ является (i, j) -примитивным и

$$\gamma_{i,j} \leq \gamma_{i,\mu} + \rho[\mu, j].$$

В случае (μ, j) -примитивности орграфа Γ для $\mu \in D(i, \Gamma) \cap D(\Gamma, j)$ неравенство $\gamma_{i,j} \leq \rho[i, \mu] + \gamma_{\mu,j}$ доказывается двойственно. Теорема 3 доказана.

Следствие 1. Если сильно связный орграф Γ (i, j) -примитивен при некоторых $i, j \in \mathbb{N}_n$, то Γ примитивный.

ДОКАЗАТЕЛЬСТВО. Если орграф Γ сильно связный, то $D(\Gamma, i) = D(j, \Gamma) = \mathbb{N}_n$ при указанных i, j . Следовательно, по теореме 3(б) орграф Γ является (μ, ν) -примитивным для любых $\mu, \nu \in \mathbb{N}_n$. Следствие 1 доказано.

Из теоремы 3 следует, что локальная примитивность орграфа обладает свойством транзитивности.

Следствие 2. Если орграф Γ является (i, μ) -примитивным и (μ, j) -примитивным, то Γ (i, j) -примитивен и

$$\gamma_{i,j} \leq \min\{\gamma_{i,\mu} + \rho[\mu, j], \rho[i, \mu] + \gamma_{\mu,j}\}.$$

ДОКАЗАТЕЛЬСТВО. В данных условиях $\mu \in D(i, \Gamma) \cap D(\Gamma, j)$. Стало быть, по теореме 3(в) $\gamma_{i,j} \leq \gamma_{i,\mu} + \rho[\mu, j]$ и $\gamma_{i,j} \leq \rho[i, \mu] + \gamma_{\mu,j}$. Следствие 2 доказано.

3. Условия B -примитивности орграфа для некоторого класса множеств B

Орграф назовём *существенным*, если все его вершины существенные. Компоненту связности существенного орграфа назовём *существенной компонентой связности* (скс).

Множество вершин орграфа \widetilde{W} обозначим через W .

Лемма 1. *Существенный орграф Γ , состоящий из скс $\widetilde{W}_1, \dots, \widetilde{W}_r$, $1 \leq r \leq n$, (i, j) -примитивен тогда и только тогда, когда существует единственное $k \in \{1, \dots, r\}$ такое, что скс \widetilde{W}_k является (i, j) -примитивной и содержит i, j -ксс $\widetilde{S}_{1,k}, \dots, \widetilde{S}_{l(k),k}$, $l(k) \geq 1$, при этом $(i, j) \in D(\widetilde{W}_k, S_k) \times D(S_k, \widetilde{W}_k)$, где $S_k = S_{1,k} \cup \dots \cup S_{l(k),k}$.*

ДОКАЗАТЕЛЬСТВО. В силу определения скс и (i, j) -примитивности орграфа вершины i и j принадлежат только одной скс орграфа Γ , пусть эта скс есть \widetilde{W}_k . По определению скс \widetilde{W}_k содержит i, j -ксс, не обязательно единственную. Если Γ (i, j) -примитивен, то в соответствии с [1, с. 73] в скс \widetilde{W}_k существует путь $[i, j]$, проходящий через некоторую вершину множества S_k . Значит, указанное включение пары (i, j) следует из того, что множество S_k достижимо только из множества $D(\widetilde{W}_k, S_k)$ и из множества S_k достижимы только вершины множества $D(S_k, \widetilde{W}_k)$. Лемма 1 доказана.

Для $I, J \subseteq \mathbb{N}_n$ обозначим через $\rho[I, J] = \min_{(i,j) \in I \times J} \rho[i, j]$ расстояние от множества I до множества J ($\rho[I, J] = 0$ при $I \cap J \neq \emptyset$, $\rho[i, J] = \rho[I, J]$ при $I = \{i\}$, $\rho[I, j] = \rho[I, J]$ при $J = \{j\}$); через $\theta[I, J] = \max_{i \in I} \rho[i, J]$ — расстояние достижимости из любой вершины множества I некоторой вершины множества J ($\theta[I, J] = 0$, если $I \subseteq J$); через $\tau[I, J] = \max_{j \in J} \rho[I, j]$ — расстояние достижимости из некоторой вершины множества I любой вершины множества J ($\tau[I, J] = 0$, если $J \subseteq I$).

Пусть $i \in I \subseteq \mathbb{N}_n$. Введём следующие обозначения: $\Gamma(I)$ — подграф орграфа Γ с множеством вершин I , $V(i) = \{i\}$, если i — ациклическая вершина, и $V(i) = Z$, если i — вершина ксс \widetilde{Z} орграфа Γ , $V(I) = \bigcup_{i \in I} V(i)$.

Теорема 4. *Если орграф \widetilde{U}_B существенный, связный и содержит единственную ксс \widetilde{S}_B , то орграф Γ является B -примитивным тогда и только тогда, когда орграф $\Gamma(V(U_B))$ есть скс, содержащая примитивную ксс \widetilde{Z}_B , где $S_B \subseteq Z_B$. В случае B -примитивности имеем*

$$\begin{aligned}\gamma_B &\leq \max_{(i,j) \in B} \min_{(\mu,\nu) \in Z^2} (\rho[i, \mu] + \rho[\nu, j] + \gamma_{\mu,\nu}) \\ &\leq \exp \tilde{Z}_B + \theta[U_B, Z_B] + \tau[Z_B, U_B].\end{aligned}$$

ДОКАЗАТЕЛЬСТВО. НЕОБХОДИМОСТЬ. Пусть орграф Γ B -примитивный. Тогда для любой пары $(i, j) \in B$ орграф Γ является (i, j) -примитивным, следовательно, в Γ вершина j достижима из вершины i . Значит, достижимость j из i в \tilde{U}_B распространяется на Γ (т. е. имеется и в Γ), более того, Γ является (i, j) -примитивным по следствию 2. Стало быть, орграф $\tilde{Z}_B = \Gamma(V(S_B))$, являющийся частью орграфа $\Gamma(V(U_B))$, представляет собой ксс, так как по условию \tilde{S}_B есть ксс. Заметим, что по построению $S_B \subseteq Z_B$.

По условию в существенном связном орграфе \tilde{U}_B для любой вершины $\mu \in U_B$ либо μ достижима из S_B , либо из μ достижимо множество S_B . Значит, в силу указанного распространения достижимости в Γ для любой вершины $\mu \in V(U_B)$ либо μ достижима из Z_B , либо из μ достижимо множество Z_B . Отсюда $\Gamma(V(U_B))$ есть ксс, содержащая ксс \tilde{Z}_B .

Из B -примитивности орграфа Γ следует его (μ, ν) -примитивность для любой дуги (μ, ν) ксс \tilde{S}_B . Поскольку $S_B \subseteq Z_B$, ксс \tilde{Z}_B примитивная в силу следствия 1.

Оценим γ_B . Если $(i, j) \in B$, то в Γ имеются пути $[i, j] = [i, \mu] \bullet w_t \bullet [\nu, j]$, где $[i, \mu]$ — кратчайший путь от i до Z_B , $[\nu, j]$ — кратчайший путь от Z_B до j , w_t — путь длины t из μ в ν ; такие пути имеются в Γ при любом $t \geq \gamma_{\mu,\nu}$. Следовательно,

$$\gamma_{i,j} \leq \min_{(\mu,\nu) \in Z^2} (\rho[i, \mu] + \rho[\nu, j] + \gamma_{\mu,\nu}).$$

ДОСТАТОЧНОСТЬ. Допустим, что орграф $\Gamma(V(U_B))$ есть ксс, содержащая примитивную ксс \tilde{Z}_B , где $S_B \subseteq Z_B$. Тогда из существования путей $[i, j] = [i, \mu] \bullet w_t \bullet [\nu, j]$ длины $\rho[i, \mu] + \rho[\nu, j] + t$ при любом $t \geq \exp \tilde{Z}_B$ следует, что для любой пары $(i, j) \in B$ орграф Γ является B -примитивным.

Для доказательства второго неравенства возьмём такие μ и ν , что

$$\rho[i, \mu] = \rho[i, Z_B], \quad \rho[\nu, j] = \rho[Z_B, j].$$

Тогда $\gamma_{\mu,\nu} \leq \exp \tilde{Z}_B$ и из первого неравенства следует, что

$$\begin{aligned}\gamma_B &\leq \max_{(i,j) \in B} (\rho[i, Z_B] + \rho[Z_B, j]) + \exp \tilde{Z}_B \\ &\leq \exp \tilde{Z}_B + \theta[U_B, Z_B] + \tau[Z_B, U_B].\end{aligned}$$

Теорема 4 доказана.

Следствие 3. Если орграф \tilde{U}_B сильно связный, то орграф Γ является B -примитивным тогда и только тогда, когда $U_B \subseteq Z_B$, где \tilde{Z}_B — примитивная ксс в Γ . В случае B -примитивности верны оценки:

$$\gamma_B \leq \max_{(i,j) \in B} \min_{\nu \in Z} (\gamma_{i,\nu} + \rho[\nu, j]), \quad \gamma_B \leq U_B^2\text{-exp } \tilde{Z}_B.$$

ДОКАЗАТЕЛЬСТВО. В данных условиях $\tilde{Z} = \Gamma(V(U_B))$ и $U_B \subseteq Z_B$, где ксс \tilde{Z}_B примитивная. Полагая $i = \mu$, $\rho[i, \mu] = 0$, из первой оценки теоремы 4 для γ_B получаем $\gamma_B \leq \max_{(i,j) \in B} \min_{\nu \in Z} (\gamma_{i,\nu} + \rho[\nu, j])$.

По условию $B \subseteq U_B^2$, откуда

$$\gamma_B = \max_{(i,j) \in B} \gamma_{i,j} \leq \max_{(i,j) \in U^2} \gamma_{i,j} = U_B^2\text{-exp } \tilde{Z}_B.$$

Следствие 3 доказано.

Из утверждения 2 вытекает, что в формулировке теоремы 4 ограничения на число скс и ксс орграфа Γ непринципиальны, т. е. теорема 4 с соответствующими поправками может быть распространена на класс всех существенных орграфов \tilde{U}_B .

4. Метрические характеристики локально примитивного орграфа

Элементарным экспонентом матрицы (орграфа) называется её (его) (i, j) -экспонент, где $(i, j) \in \mathbb{N}_n^2$. Если орграф Γ не (i, j) -примитивный, то положим $(i, j)\text{-exp } \Gamma = \gamma_{i,j} = \infty$.

Из множества элементарных (i, j) -экспонентов матрицы M (орграфа Γ) составим квадратную матрицу $\mathfrak{M}(M) = ((i, j)\text{-exp } M)$ (матрицу $\mathfrak{M}(\Gamma) = ((i, j)\text{-exp } \Gamma)$) порядка n , которую назовём *матрицей элементарных экспонентов*, кратко *матэксом*, матрицы M (орграфа Γ).

Отметим свойства матэкса $\mathfrak{M}(M)$.

1. Матэкс $\mathfrak{M}(M)$ определяет все локальные экспоненты M :

$$B\text{-exp } M = \max_{(i,j) \in B} (i, j)\text{-exp } M,$$

в частности, $\text{exp } M = \max_{1 \leq i, j \leq n} (i, j)\text{-exp } M$.

2. Если $M \geq M'$, то $\mathfrak{M}(M) \leq \mathfrak{M}(M')$, где неравенство матриц понимается как аналогичное неравенство соответствующих элементов.

Пример 4. Оценочная матрица для матэкса n -вершинного орграфа Виландта. Пусть орграф Виландта Γ с множеством вершин $\{0, \dots, n-1\}$ содержит гамильтонов контур $C = (0, \dots, n-1)$ и дугу $(n-1, 1)$. Тогда (i, j) -ехр $\Gamma \leq n^2 - 3n + 2 + \rho(i, j)$, где $\rho(i, j)$ — длина кратчайшего пути в Γ из i в j , проходящего через одну из вершин множества $\{1, \dots, n-1\}$, т. е.

$$\rho(i, j) = \begin{cases} n, & i = j = 0, \\ 0, & i = j > 0, \\ (j - i) \bmod n, & 0 \leq i < j \text{ или } 0 = j < i, \\ (j - i - 1) \bmod n, & 0 < j < i. \end{cases}$$

Величина $n^2 - 3n + 2 + \rho(i, j)$ есть точное значение (i, j) -ехр Γ в первых трёх случаях и при $0 < j < i$ есть верхняя оценка (i, j) -ехр Γ . Оценочная матрица для матэкса имеет вид

$$\mathfrak{M}(\Gamma) = \begin{pmatrix} n^2 - 2n + 2 & n^2 - 3n + 3 & n^2 - 3n + 4 & \dots & n^2 - 2n & n^2 - 2n + 1 \\ n^2 - 2n + 1 & n^2 - 3n + 2 & n^2 - 3n + 3 & \dots & n^2 - 2n - 1 & n^2 - 2n \\ n^2 - 2n & n^2 - 2n & n^2 - 3n + 2 & \dots & n^2 - 2n - 2 & n^2 - 2n - 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n^2 - 3n + 4 & n^2 - 3n + 4 & n^2 - 3n + 5 & \dots & n^2 - 3n + 2 & n^2 - 3n + 3 \\ n^2 - 3n + 3 & n^2 - 3n + 3 & n^2 - 3n + 4 & \dots & n^2 - 2n & n^2 - 3n + 2 \end{pmatrix}.$$

В орграфе Γ наряду с расстояниями между вершинами и между множествами вершин можно рассматривать метрические характеристики, связанные с локальными экспонентами. Определим некоторые из них.

Пусть $I, J \subseteq \mathbb{N}_n$, $\emptyset \neq I = \{i_1, \dots, i_k\}$, $\emptyset \neq J = \{j_1, \dots, j_r\}$. Обозначим $I \times J$ -ехр $M = \gamma_{I,J}$. Таким образом, $\gamma_{I,J} = \max_{(i,j) \in I \times J} (i, j)$ -ехр M .

Назовём k, r -экспорадиусом орграфа Γ величину

$$\text{exrd}_{k,r} \Gamma = \min_{(I,J): |I|=k, |J|=r} \gamma_{I,J}.$$

При $|I| = k$, $|J| = r$ множество $I \times J$ назовём k, r -экспоцентром графа Γ , если $\gamma_{I,J} = \text{exrd}_{k,r} \Gamma$.

В примитивном орграфе Γ при любых фиксированных k, r существует k, r -экспоцентр, в общем случае неединственный. Для локально примитивного орграфа Γ k, r -экспоцентр существует, если Γ имеет конечный k, r -экспорадиус.

5. К задаче построения s -боксов

Важным элементом некоторых криптографических алгоритмов являются нелинейные отображения $V_k \rightarrow V_r$, называемые s -боксами размера

$k \times r$ и используемые при построении раундовых подстановок блочных шифров (DES — s -боксы размера 6×4 , AES и «Кузнечик» — s -боксы размера 8×8 , ГОСТ 28147-89 — s -боксы размера 4×4 и др.). Для использования в качестве s -боксов необходимо, чтобы преобразования имели ряд заданных свойств. К необходимым свойствам преобразования относятся, в частности, биективность (при $k = r$), совершенность (т. е. существенная зависимость каждой координатной булевой функции от всех входных переменных), возможность относительно несложной программной и/или аппаратной реализации и ряд других. При небольших размерах s -боксов ($r \leq 8$) реализация может быть выполнена с помощью таблиц. Однако чем больше r , тем более ресурсоёмкой является табличная реализация, как по размеру памяти, так и по времени реализации. Вместе с тем, имеются достаточные основания полагать, что алгоритмическая реализация s -боксов потребует памяти относительно небольшого размера и будет сравнима по времени. Поэтому актуальной является разработка способов алгоритмической реализации s -боксов и исследование характеристик этих способов.

Один из возможных путей построения совершенных s -боксов размера $k \times r$, в том числе при относительно больших k и r , основан на возведении в степень определённого преобразования g пространства булевых векторов, у которого некоторые локальные экспоненты перемешивающей матрицы относительно невелики.

Опишем данный подход к построению отображений $V_k \rightarrow V_r$ с помощью преобразования g множества V_n , где $n > \max\{k, r\}$. Введём следующие обозначения: $X = \{x_1, \dots, x_n\}$, $\{g_1(X), \dots, g_n(X)\}$ — система координатных функций преобразования g , $G^t = \{g_1^t(X), \dots, g_n^t(X)\}$ — система координатных функций преобразования g^t , $t = 1, 2, \dots$, Γ — перемешивающий орграф преобразования g , M — матрица смежности вершин орграфа Γ , G_J^t — неповторная упорядоченная выборка размера r из множества G^t , сохраняющая порядок следования координатных функций и такая, что $g_j^t(X) \in G_J^t$ тогда и только тогда, когда $j \in J$, X_I — неповторная упорядоченная выборка размера k из множества X , сохраняющая порядок следования переменных и такая, что $x_i \in X_I$ тогда и только тогда, когда $i \in I$.

Выборке X_I соответствует множество $\{\bar{\alpha}\}$ всевозможных фиксаций переменных из $X \setminus X_I$, следовательно, выборке G_J^t при любой фиксации $\bar{\alpha}$ соответствует система координатных функций, реализующих отображение $V_k \rightarrow V_r$, $t = 1, 2, \dots$ (обозначим через $G_J^t(I, \bar{\alpha})$ такую систему функций и реализуемое ей отображение).

С помощью введённых метрических характеристик локально примитивного орграфа определим, при каких выборках I, J и при каком наименьшем натуральном t отображение $G_J^t(I, \bar{\alpha})$ может быть совершенным (когда каждая координатная функция отображения $G_J^t(I, \bar{\alpha})$ зависит от всех переменных набора X_I). Для быстроты реализации важно, чтобы некоторые локальные экспоненты перемешивающей матрицы были относительно невелики.

Отображение $G_J^t(I, \bar{\alpha})$ имеет наилучшие перемешивающие свойства, если орграф Γ является $I \times J$ -примитивным и при фиксированных I, J наименьшее t с таким свойством равно $I \times J$ -exp Γ . Минимизация значения t выполняется с помощью выбора множеств I и J порядка k и r соответственно из множества всех допустимых вариантов. А именно, если k, r -экспорадиус орграфа Γ конечный, $\text{exrd}_{k,r} \Gamma = \theta$, то наилучший выбор множеств I и J выполняется тогда, когда множество $I \times J$ есть k, r -экспоцентр графа Γ . Для упрощения записи формул положим $I = \{1, \dots, k\}$, $J = \{1, \dots, r\}$, что не ограничивает общности рассуждений. Тогда искомое отображение с наименьшим локальным экспонентом можно взять из множества $\{G_J^\theta(I, \bar{\alpha})\}$, где $\bar{\alpha}$ пробегает все фиксации переменных из $X \setminus X_I$, т. е. $\bar{\alpha} = (a_{k+1}, \dots, a_n)$, $x_{k+1} = a_{k+1}, \dots, x_n = a_n$.

В общем случае условия существования в множестве $\{G_J^\theta(I, \bar{\alpha})\}$ совершенного отображения $V_k \rightarrow V_r$ не определены. Вместе с тем, имеются примеры реализации описанного подхода к построению совершенных отображений [3]. Кроме того, предварительные оценки позволили выдвинуть следующую гипотезу: для случайной подстановки g множества V_n при $\max\{k, r\} < n/2$ и при $n \rightarrow \infty$ вероятность успешного поиска в множестве $\{G_J^\theta(I, \bar{\alpha})\}$ совершенного отображения $V_k \rightarrow V_r$ стремится к 1.

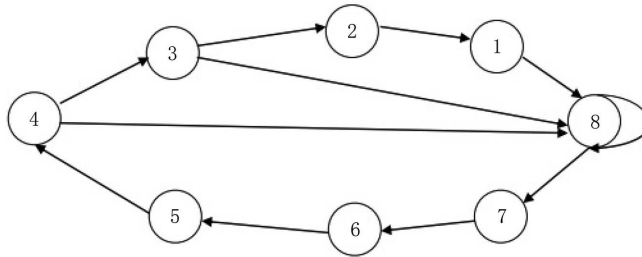


Рис. 1. Перемешивающий орграф Γ

Пример 5. Пусть g — преобразование регистра левого сдвига с функцией обратной связи $f(x_1, \dots, x_8) = x_1 \oplus x_3x_4 \oplus x_8$, а длина регистра равна 8. Построим отображения $V_4 \rightarrow V_4$ вида $s_\theta(\bar{\alpha})$.

Перемешивающий 8-вершинный оргграф Γ (рис. 1) преобразования g примитивен, так как он сильно связный и имеет петлю.

Составим матэкс $\mathfrak{M}(\Gamma)$ орграфа Γ , где (i, j) -ехр Γ равен длине кратчайшего пути из i в j , проходящего через вершину с петлёй:

$$\mathfrak{M}(\Gamma) = \begin{pmatrix} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 \\ 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 1 \end{pmatrix}.$$

По матэксу $\mathfrak{M}(\Gamma)$ определяем, что $\text{ехр } \Gamma = 11$ и 4,4-экспорадиус равен 4.

Вьпишем системы координатных функций для преобразований g, g^2, g^3, g^4 (табл. 2).

Т а б л и ц а 2

t	g_1^t	g_2^t	g_3^t	g_4^t	g_5^t	g_6^t	g_7^t	g_8^t
1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	f_1
2	x_3	x_4	x_5	x_6	x_7	x_8	f_1	f_2
3	x_4	x_5	x_6	x_7	x_8	f_1	f_2	f_3
4	x_5	x_6	x_7	x_8	f_1	f_2	f_3	f_4

Здесь

$$\begin{aligned} f_1(x_1, \dots, x_8) &= x_1 \oplus x_3x_4 \oplus x_8, \\ f_2(x_1, \dots, x_8) &= x_2 \oplus x_4x_5 \oplus f_1(x_1, \dots, x_8), \\ f_3(x_1, \dots, x_8) &= x_3 \oplus x_5x_6 \oplus f_2(x_1, \dots, x_8), \\ f_4(x_1, \dots, x_8) &= x_4 \oplus x_6x_7 \oplus f_3(x_1, \dots, x_8). \end{aligned}$$

В Γ имеется один 4,4-экспоцентр $\{1, 3, 4, 8\} \times \{5, 6, 7, 8\}$, которому соответствует класс отображений $V_4 \rightarrow V_4$ (при различных фиксациях переменных x_2, x_5, x_6, x_7 функций f_1, f_2, f_3, f_4). Например, при фиксации $x_6 = x_7 = 0$ и $x_2 = x_5 = 1$ имеем совершенное отображение $V_4 \rightarrow V_4$, заданное следующей системой координатных функций:

$$\begin{aligned} &\{x_1 \oplus x_3x_4 \oplus x_8, x_1 \oplus x_3x_4 \oplus x_8 \oplus x_4 \oplus 1, \\ &x_1 \oplus x_3x_4 \oplus x_8 \oplus x_3 \oplus x_4 \oplus 1, x_1 \oplus x_3x_4 \oplus x_8 \oplus x_3 \oplus 1\}. \end{aligned}$$

Заметим, что данное отображение не является примером «хорошего» s -блока, так как оно не биективно:

$$f_1(x_1, \dots, x_8) \oplus f_2(x_1, \dots, x_8) \oplus f_3(x_1, \dots, x_8) \oplus f_4(x_1, \dots, x_8) = 1.$$

В рамках описанного подхода проблему построения s -блоков размера $k \times r$ можно представить как описание при заданных $k, r, n > \max\{k, r\}$ преобразований g множества V_n , с использованием степени которых можно построить отображения $V_k \rightarrow V_r$ с заданным набором свойств.

ЛИТЕРАТУРА

1. **Кяжин С. Н., Фомичев В. М.** Локальная примитивность графов и неотрицательных матриц // Прикл. дискрет. математика. 2014. № 3. С. 68–80.
2. **Фомичев В. М.** О характеристиках локально примитивных орграфов и матриц // Прикл. дискрет. математика. Прил. 2017. № 10. С. 96–99.
3. **Фомичев В. М., Задорожный Д. И., Коренева А. М., Лолич Д. М., Юзбашев А. В.** Об алгоритмической реализации s -блоков. Докл. XIX Науч.-практ. междунар. конф. «РусКрипто-2017» (Московская область, 21–24 марта 2017 г.). http://www.ruscrypto.ru/resource/summary/rc2017/02_fomitchev_zadorozhny_koreneva_lolich_yuzbashev.pdf
4. **Фомичев В. М., Кяжин С. Н.** Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24, № 1. С. 97–119.
5. **Фомичев В. М., Мельников Д. А.** Криптографические методы защиты информации. Ч. 1. Математические аспекты: учебник для академического бакалавриата (под ред. В. М. Фомичева). М.: Изд-во ЮРАЙТ, 2016. 209 с.
6. **Berger T. P., Francq J., Minier M., Thomas G.** Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput // IEEE Tran. Comput. 2016. Vol. 65, No. 7. P. 2074–2089.
7. **Berger T. P., Minier M., Thomas G.** Extended generalized Feistel networks using matrix representation // Selected Areas in Cryptography. Rev. Selected Pap. 20th Int. Conf. SAC (Burnaby, Canada, Aug. 14–16, 2013). Heidelberg: Springer-Verl., 2014. (Lect. Notes Comput. Sci.; Vol. 8282).
8. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. No. 14. P. 483–499.
9. **Huang Y., Liu B.** Generalized r -exponents of primitive digraphs // Taiwan. J. Math. 2011. Vol. 15, No. 5. P. 1999–2012.
10. **Liu B.** Generalized exponents of Boolean matrices // Lin. Algebra Appl. 2003. No. 373. P. 169–182.
11. **Miao Z., Zhang K.** The local exponent sets of primitive digraphs // Lin. Algebra Appl. 2000. No. 307. P. 15–33.

12. **Shen J., Neufeld S.** Local exponents of primitive digraphs // *Lin. Algebra Appl.* 1998. No. 268. P. 117–129.
13. **Suzaki T., Minematsu K.** Improving the generalized Feistel // *Fast Software Encryption Rev. Selected Pap. 17th Int. Workshop FSE* (Seoul, Korea, Feb. 7–10, 2010). Heidelberg: Springer-Verl., 2010. P. 19–39. (*Lect. Notes Comput. Sci.*; Vol. 6147).

Фомичёв Владимир Михайлович

Статья поступила

3 июля 2017 г.

Исправленный вариант —

11 декабря 2017 г.

SEMIGROUP AND METRIC CHARACTERISTICS OF LOCALLY PRIMITIVE MATRICES AND GRAPHS

V. M. Fomichev^{1,2}

¹Financial University under the Government of the Russian Federation,
49 Leningradsky Ave., 125993 Moscow, Russia,

²National Research Nuclear University MEPhI,
31 Kashirskoe Highway, 115409 Moscow, Russia,

³Institute of Informatics Problems of FRC CSC RAS,
44-2 Vavilov St., 119333 Moscow, Russia

E-mail: fomichev@nm.ru

Abstract. The notion of local primitivity for a quadratic 0, 1-matrix of size $n \times n$ is extended to any part of the matrix which need not be a rectangular submatrix. A similar generalization is carried out for any set B of pairs of initial and final vertices of the paths in an n -vertex digraph, $B \subseteq \{(i, j) : 1 \leq i, j \leq n\}$. We establish the relationship between the local B -exponent of a matrix (digraph) and its characteristics such as the cyclic depth and period, the number of nonprimitive matrices, and the number of nonidempotent matrices in the multiplicative semigroup of all quadratic 0, 1-matrices of order n , etc. We obtain a criterion of B -primitivity and an upper bound for the B -exponent. We also introduce some new metric characteristics for a locally primitive digraph Γ : the k, r -exporadius, the k, r -expocenter, where $1 \leq k, r \leq n$, and the matex which is defined as the matrix of order n of all local exponents in the digraph Γ . An example of computation of the matex is given for the n -vertex Wielandt digraph. Using the introduced characteristics, we propose an idea for algorithmically constructing realizable s -boxes (elements of round functions of block ciphers) with a relatively wide range of sizes. Tab. 2, illustr. 1, bibliogr. 13.

Keywords: mixing matrix, primitive matrix, locally primitive matrix, exponent of a matrix, cyclic matrix semigroup.

REFERENCES

1. S. N. Kyazhin and V. M. Fomichev, Local primitiveness of graphs and nonnegative matrices, *Prikl. Diskretn. Mat.*, No. 3, 68–80, 2014 [Russian].
2. V. M. Fomichev, On characteristics of local primitive matrices and digraphs, *Prikl. Diskretn. Mat., Prilozh.*, No. 10, 96–99, 2017 [Russian].

3. **V. M. Fomichev, D. I. Zadorozhnyi, A. M. Koreneva, D. M. Lolich,** and **A. V. Yuzbashev**, On algorithmic implementation of s -boxes, in *Proc. XIX Sci. Pract. Conf. "RusCrypto", Moscow, Russia, Mar. 21–24, 2017*. Available at http://www.ruscrypto.ru/resource/summary/rc2017/02_fomichev_zadorozhny_koreneva_lolich_yuzbashev.pdf (accessed Dec. 29, 2017) [Russian].
4. **V. M. Fomichev** and **S. N. Kyazhin**, Local primitivity of matrices and graphs, *Diskretn. Anal. Issled. Oper.*, **24**, No. 1, 97–119, 2017 [Russian]. Translated in *J. Appl. Ind. Math.*, **11**, No. 1, 26–39, 2017.
5. **V. M. Fomichev** and **D. A. Melnikov**, *Kriptograficheskie metody zashchity informatsii. Chast' 1: Matematicheskie aspekty* (Cryptographic methods of information security. Part 1: Mathematical aspects), YURAIT, Moscow, 2016 [Russian].
6. **T. P. Berger, J. Francq, M. Minier,** and **G. Thomas**, Extended Generalized Feistel Networks using matrix representation to propose a new lightweight block cipher: Lilliput, *IEEE Trans. Comput.*, **65**, No. 7, 2074–2089, 2016.
7. **T. P. Berger, M. Minier,** and **G. Thomas**, Extended Generalized Feistel Networks using matrix representation, in *Selected Areas in Cryptography* (Revis. Sel. Pap. 20th Int. Conf. SAC, Burnaby, Canada, Aug. 14–16, 2013), Springer, Heidelberg, 2014 (Lect. Notes Comput. Sci., Vol. 8282).
8. **R. A. Brualdi** and **B. Liu**, Generalized exponents of primitive directed graphs, *J. Graph Theory*, **14**, 483–499, 1990.
9. **Y. Huang** and **B. Liu**, Generalized r -exponents of primitive digraphs, *Taiwan. J. Math.*, **15**, No. 5, 1999–2012, 2011.
10. **B. Liu**, Generalized exponents of Boolean matrices, *Linear Algebra Appl.*, **373**, 169–182, 2003.
11. **Z. Miao** and **K. Zhang**, The local exponent sets of primitive digraphs, *Linear Algebra Appl.*, **307**, 15–33, 2000.
12. **J. Shen** and **S. Neufeld**, Local exponents of primitive digraphs, *Linear Algebra Appl.*, **268**, 117–129, 1998.
13. **T. Suzaki** and **K. Minematsu**, Improving the generalized Feistel, in *Fast Software Encryption* (Revis. Sel. Pap. 17th Int. Workshop FSE, Seoul, Korea, Feb. 7–10, 2010), Springer, Heidelberg, 2010 (Lect. Notes Comput. Sci., Vol. 6147).

Vladimir M. Fomichev

Received

3 July 2017

Revised

11 December 2017