

ПРИМИТИВНОСТЬ И ЛОКАЛЬНАЯ ПРИМИТИВНОСТЬ ОРГРАФОВ И НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

В. М. Фомичёв^{1,2,3,a,}, Я. Э. Авезова^{2,b},
А. М. Коренева^{2,c}, С. Н. Кязжин^{2,d}*

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

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

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

E-mail: ^afomichev@nm.ru, ^bavezovayana@gmail.com,
^calisa.koreneva@gmail.com, ^ds.kyazhin@kaf42.ru

Аннотация. Дан обзор основных результатов исследования примитивности и локальной примитивности орграфов и матриц начиная с зарождения этого направления в 1912 г. по настоящее время. Представлены универсальные и частные критерии примитивности и локальной примитивности, универсальные и частные оценки экспонентов и локальных экспонентов орграфов и матриц. Описаны криптографические приложения данного математического аппарата для оценки перемешивающих свойств преобразований блочных шифров и генераторов гаммы. Сформулированы перспективные направления исследований в области примитивности и локальной примитивности орграфов и матриц. Библиогр. 47.

Ключевые слова: примитивный орграф, примитивная матрица, локальная примитивность, примитивное множество, экспонент орграфа, экспонент матрицы, локальный экспонент орграфа.

Основные обозначения и определения

\mathbb{N} — множество натуральных чисел, $n \in \mathbb{N}$;

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$;

$\mathbb{N}_n = \{1, \dots, n\}$;

V_n — множество двоичных n -мерных векторов;

Z_n — кольцо вычетов по модулю n , $n > 1$;

^{*)}Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 16-01-00226).

- $\gcd(l_1, \dots, l_m)$ — наибольший общий делитель натуральных чисел l_1, \dots, l_m , $m \in \mathbb{N}$;
 $\text{lcm}(l_1, \dots, l_m)$ — наименьшее общее кратное натуральных чисел l_1, \dots, l_m , $m \in \mathbb{N}$;
 $F(l_1, \dots, l_m)$ — число Фробениуса для аргументов $l_1, \dots, l_m \in \mathbb{N}$, где $\gcd(l_1, \dots, l_m) = 1$, $m \in \mathbb{N}$;
 $\langle a_1, \dots, a_p \rangle$ — полугруппа, порождённая множеством элементов $\{a_1, \dots, a_p\}$, $p \in \mathbb{N}$;
 $M_n^{0,1}$ — множество 0,1-матриц порядка n ;
 Γ — ориентированный n -вершинный граф;
 $\Gamma(g)$ — перемешивающий граф преобразования g множества V_n ;
 $\exp \Gamma$ ($\exp M$) — экспонент орграфа Γ (матрицы M);
 $\text{diam } \Gamma$ — диаметр орграфа Γ ;
 (i, j) — дуга в орграфе Γ , инцидентная вершинам i и j ;
 $[i, j]$ — путь в орграфе Γ из вершины i в вершину j ;
 $\langle i, j \rangle$ — кратчайший путь в орграфе Γ из вершины i в вершину j ;
 $\text{len } w$ ($\text{len } c$) — длина пути w (контура c), равная числу дуг пути (контура);
 $\rho_{i,j} = \text{len } \langle i, j \rangle$ — расстояние в орграфе Γ от вершины i до вершины j ;
 \tilde{U} — множество вершин орграфа U ;
ксс — компонента сильной связности;
 \Leftrightarrow — «тогда и только тогда, когда».

Введение

Неотрицательные матрицы, т. е. матрицы, все элементы которых суть неотрицательные действительные числа, являются активно разрабатываемым объектом в комбинаторном анализе (см. библиографию). Свойство неотрицательности матрицы M записывается так: $M \geq 0$. Матрицу M , все элементы которой положительны, называют *положительной* и записывают $M > 0$.

Для квадратной неотрицательной матрицы M естественно возникает вопрос: имеются ли положительные матрицы в ряду $M, M^2, \dots, M^t, \dots$? Иными словами, содержит ли циклическая полугруппа $\langle M \rangle$ положительные матрицы? Если содержит, то матрица M называется *примитивной*, и наименьшее натуральное γ , при котором $M^\gamma > 0$, называется *экспонентом* матрицы M и обозначается через $\exp M$. Если полугруппа $\langle M \rangle$ не содержит положительных матриц, то матрица M называется *непримитивной*, и полагаем $\exp M = \infty$.

Заметим, что мультипликативная полугруппа всех неотрицательных матриц гомоморфно отображается на полугруппу всех 0,1-матриц (т. е. матриц, все элементы которых суть 0 или 1) с помощью замены каждого положительного элемента единицей. Данный эпиморфизм согласован со свойством примитивности, т. е. прообразом любой примитивной 0,1-матрицы является класс, состоящий только из примитивных матриц, и прообразом любой непримитивной 0,1-матрицы является класс, состоящий только из непримитивных матриц. При исследовании примитивности это свойство позволяет ограничиться рассмотрением мультипликативных моноидов $M_n^{0,1}$, $n \in \mathbb{N}$, где умножение в $M_n^{0,1}$ выполняется как обычное умножение целочисленных матриц с последующей заменой положительных элементов единицами.

Множество матриц смежности вершин n -вершинных ориентированных графов с петлями совпадает с $M_n^{0,1}$, поэтому понятия примитивности и экспонента распространены на орграфы, где умножение орграфов определено как умножение бинарных отношений. Связь между графами и неотрицательными матрицами устанавливает общеизвестная теорема теории графов (назовём её основной теоремой): если M — матрица смежности вершин графа Γ и $M^t = (m_{i,j}^{(t)})$, то число путей длины t из i в j в графе Γ равно $m_{i,j}^{(t)}$, $i, j \in \{1, \dots, n\}$. Поэтому примитивность орграфа и величина экспонента определяются свойствами путей в графе, в частности, $M > 0$ тогда и только тогда, когда орграф Γ полный. Вообще, всякий результат о примитивности и об экспонентах допускает равносильную интерпретацию как на матричном, так и на графовом языках.

Свойство примитивности матрицы M по-разному обобщается на множество матриц $\widehat{M} = \{M_1, \dots, M_p\}$, $p \in \mathbb{N}$: множество \widehat{M} называется *примитивным* (*непримитивным*), если мультипликативная полугруппа $\langle \widehat{M} \rangle$ содержит (не содержит) положительную матрицу. Длина кратчайшего слова в алфавите \widehat{M} , которому соответствует положительное произведение матриц, называется *экспонентом множества матриц* \widehat{M} и обозначается через $\text{exr } \widehat{M}$.

При другом обобщении множество \widehat{M} называется *множественно примитивным*, если при некотором $k \in \mathbb{N}$ весь k -й слой полугруппы $\langle \widehat{M} \rangle$ (т. е. множество матриц, соответствующих всем словам длины k в алфавите \widehat{M}) состоит только из положительных матриц. Наименьшее k с таким свойством называется *множественным экспонентом* множества \widehat{M} . Отметим, что множественно примитивное множество \widehat{M} состоит только из примитивных матриц, в то время как примитивное множество \widehat{M} может содержать непримитивные матрицы.

Важным обобщением свойства примитивности матрицы является так называемая локальная примитивность матрицы M . Это связано с положительностью определённого фрагмента B в каждой матрице из ряда $\{M^t\}$ для всех $t \geq \gamma$, где $\gamma \in \mathbb{N}$, $\emptyset \neq B \subseteq \mathbb{N}_n^2$. Фрагментом B может быть любое непустое подмножество элементов матрицы M , например, подматрица, полученная из M вычеркиванием некоторых строк и столбцов. Наименьшее γ с таким свойством называется *локальным B -экспонентом* матрицы M и обозначается через $B\text{-exp } M$.

В данной статье представлен систематический обзор основных теоретических и прикладных результатов по исследованию примитивности матриц (орграфов) и обобщений этого свойства; теоретические основы матрично-графового подхода изложены в учебнике [22, ч. 1, гл. 11]. При изложении материала авторами использован либо матричный, либо графовый способ, либо оба способа, в зависимости от удобства изложения. Статья состоит из введения и пяти разделов. В разд. 1 изложены основные результаты исследования примитивности орграфов и матриц, приведены универсальные и частные оценки экспонентов примитивных орграфов. Разд. 2 посвящён примитивности множеств орграфов и матриц и некоторым обобщениям этого свойства. В разд. 3 изложены результаты исследования локальной примитивности орграфов и матриц, приведены универсальные и частные оценки локальных экспонентов локально примитивных орграфов. В разд. 4 даны некоторые результаты применения представленного математического аппарата к оценке перемешивающих свойств преобразований, реализуемых блочными шифрами и генераторами гаммы. Для перемешивающих орграфов указанных преобразований приведены условия примитивности (локальной примитивности) и оценки экспонентов (локальных экспонентов). В разд. 5 сформулированы перспективные направления исследований, связанных со свойством примитивности орграфов и матриц.

1. Универсальные и частные оценки экспонентов матриц и орграфов

Далее считаем, что M есть матрица смежности вершин орграфа Γ .

Постановка задачи о распознавании примитивности неотрицательной матрицы (орграфа) и об определении экспонента была дана Фробениусом (F. G. Frobenius) [33] в 1912 г. Работы с основополагающими результатами опубликованы в середине XX в. Виландтом (H. Wielandt), Перкинсом (P. Perkins), творческим тандемом Далмэджа и Мендельсона (A. L. Dulmage, N. S. Mendelsohn) и др. Термин «экспонент» был введён

в [30]. Развитие этого направления связано с выявлением условий примитивности, а также с получением универсальных оценок экспонентов и оценок экспонентов для частных классов матриц и орграфов.

Из правила умножения матриц и из основной теоремы следуют свойства:

- 1) примитивная матрица M не содержит нулевых строк и столбцов, поэтому если $M^\gamma > 0$, то $M^t > 0$ при любом $t > \gamma$;
- 2) примитивность является наследственным свойством, иначе говоря если M — примитивная матрица, то матрица M^t также примитивная при любом $t \in \mathbb{N}$;
- 3) примитивный орграф Γ является сильно связным;
- 4) экспонент орграфа Γ не меньше его диаметра;
- 5) случайная равновероятная матрица $M \in M_n^{0,1}$ при $n \rightarrow \infty$ с вероятностью, стремящейся к единице, является примитивной и $\exp M = 2$ [14, с. 243].

Универсальная оценка (без доказательства) экспонента n -вершинного орграфа Γ дана Виландтом [47] в 1950 г.:

$$\exp \Gamma \leq n^2 - 2n + 2. \quad (1)$$

Доказательство оценки (1) представлено в [34, 40].

Критерий примитивности орграфа Γ , доказанный в 1961 г. Перкинсом [40], определяется множеством его контуров. В Γ множество контуров $\{C_1, \dots, C_m\}$ длин l_1, \dots, l_m соответственно, где $m \geq 1$, называется *примитивным*, если $\gcd(l_1, \dots, l_m) = 1$. При $m = 1$ примитивное множество контуров вырождается в единственную петлю. Критерий примитивности орграфа можно сформулировать так: сильно связный орграф Γ примитивен тогда и только тогда, когда он содержит примитивное множество контуров.

В [31] выделены «лакуны», т. е. натуральные числа, меньшие $n^2 - 2n + 2$, не являющиеся экспонентами какого-либо n -вершинного орграфа. Таковы, например, числа из интервалов $(n^2 - 3n + 4, (n - 1)^2)$ и $(n^2 - 4n + 6, n^2 - 3n + 2)$. При чётном n «лакуной» является интервал $(n^2 - 4n + 6, (n - 1)^2)$, объединяющий оба предыдущих. В [36] данные результаты усилены: для любых $n, t \in \mathbb{N}$ не существует n -вершинного орграфа с экспонентом таким, что

$$n^2 - tn + (t + 1)^2/4 < \exp \Gamma < n^2 - (t - 1)n + t - 2.$$

При $n > 1$ описаны n -вершинные орграфы [17, 31] (названные в [17] в честь Виландта), на которых достигается оценка (1). Эти орграфы

изоморфны и имеют $n + 1$ дуг, образующих контуры длины n и $n - 1$. Для других примитивных орграфов $\exp \Gamma \leq n^2 - 3n + 4$ при нечётном $n > 3$ и $\exp \Gamma \leq n^2 - 4n + 6$ при чётном $n > 3$ в соответствии с «лакунами».

В [31] дана более точная оценка с помощью известной длины l контура в Γ , $l < n$:

$$\exp \Gamma \leq n + l(n - 2). \quad (2)$$

Если примитивный орграф Γ является минимальным сильно связным [24] (т. е. удаление любой дуги нарушает сильную связность), то верна оценка

$$\exp \Gamma \leq n^2 - 4n + 6,$$

а при известной длине l контура в Γ , $l < n$, —

$$\exp \Gamma \leq n + l(n - 3).$$

Получена универсальная оценка экспонента орграфа [39] через его диаметр d :

$$\exp \Gamma \leq d^2 + 1.$$

С использованием множества $L = \{l_1, \dots, l_m\}$ длин всех простых контуров примитивного орграфа Γ дана универсальная оценка экспонента [31]:

$$\exp \Gamma \leq F(l_1, \dots, l_m) + r(\Gamma) + 1, \quad (3)$$

где $F(l_1, \dots, l_m)$ — число Фробениуса для аргументов l_1, \dots, l_m (т. е. наибольшее натуральное число, не принадлежащее аддитивной полугруппе $\langle l_1, \dots, l_m \rangle$); $r(\Gamma) = \max_{1 \leq u, v \leq n} r_{u,v}$, где $r_{u,v}$ — длина кратчайшего пути из вершины u в вершину v , проходящего через некоторую вершину контура длины l_i , $i = 1, \dots, m$.

Укажем варианты улучшения в ряде случаев оценки (3) при использовании:

а) длин не всех простых контуров, а лишь примитивного подмножества — в этом случае может уменьшиться величина $r(\Gamma)$;

б) длин контуров из непримитивного множества \widehat{C} и длин некоторого множества путей, проходящих через вершины каждого контура из множества \widehat{C} .

В примитивном орграфе Γ обозначим через $K(\Gamma)$ булеан множества всех простых контуров, через $P(\Gamma)$ — класс всех примитивных множеств простых контуров, через $L(\widehat{C})$ — множество длин контуров из множества \widehat{C} , $r(\widehat{C}) = \max_{1 \leq u, v \leq n} r_{u,v}$, где $r_{u,v}$ — длина кратчайшего пути в Γ из вершины u в вершину v , проходящего через некоторую вершину каждого

контур из \widehat{C} . Множество $K(\Gamma)$ образует решётку относительно теоретико-множественного включения, $P(\Gamma)$ есть её верхняя подполурешётка. Тогда оценка (3) может быть улучшена:

$$\exp \Gamma \leq \min_{\widehat{C} \in P(\Gamma)} (F(L(\widehat{C})) + r(\widehat{C}) + 1). \quad (4)$$

При поиске минимума необходимо учесть следующее свойство: если $\widehat{C} \subset \widehat{C}'$, то $r(\widehat{C}) \leq r(\widehat{C}')$, значит, если $F(L(\widehat{C})) = F(L(\widehat{C}'))$, то оценка (4) при \widehat{C} ниже, чем при \widehat{C}' .

Технические трудности вычисления оценки (4) в общем случае состоят в определении числа Фробениуса $F(L(\widehat{C}))$ и величины $r(\widehat{C})$. При $m > 2$ для вычисления чисел Фробениуса не существует простых формул, вместе с тем, проблема в целом решена, а соответствующие алгоритмы изложены в [20, 42]. Величина $r(\widehat{C})$ неявно оценена в теоремах 1 и 2.

Теорема 1 [22, ч. 1]. Если примитивный n -вершинный орграф Γ содержит примитивное множество контуров длин l_1, \dots, l_m , то

$$\exp \Gamma \leq n(m + 1) + F(l_1, \dots, l_m) - l_1 - \dots - l_m. \quad (5)$$

Оценка (5) улучшена с учётом структурных свойств. Пусть $\widehat{C} = \{C_1, \dots, C_m\}$ — примитивное множество контуров. Обозначим через $\Gamma(\widehat{C}) = C_1 \cup \dots \cup C_m$ часть орграфа Γ .

Лемма 1. Сильно связный орграф $\Gamma(\widehat{C})$ содержит контур Z , обходящий все контуры множества \widehat{C} и проходящий через каждую дугу столько раз, сколько контуров множества \widehat{C} содержат эту дугу.

Указанный контур Z (в общем случае определённый неоднозначно) назовём квазиэйлеровым \widehat{C} -контуром, его длина равна $\text{len } Z = l_1 + \dots + l_m$ в силу леммы 1.

С учётом леммы 1 оценка (5) уточнена [19, с. 80].

Теорема 2. Если орграф Γ содержит примитивное множество \widehat{C} контуров длин l_1, \dots, l_m и орграф $\Gamma(\widehat{C})$, имеющий компоненты связности $\widehat{C}_1, \dots, \widehat{C}_r$, где $l_1 \leq \dots \leq l_m$, $1 \leq r \leq m$, содержит множество независимых контуров $\{Z_1, \dots, Z_r\}$, где Z_j — квазиэйлеров \widehat{C}_j -контур длины λ_j , $j = 1, \dots, r$, и $\lambda_1 \geq \dots \geq \lambda_r$, то

$$\exp \Gamma \leq n(r + 1) + F(l_1, \dots, l_m) - \sum_{j=1}^r (l_j + (j - 1)\lambda_j). \quad (6)$$

Если в условиях теоремы 2 орграф $\Gamma(\widehat{C})$ связный, то

$$\exp \Gamma \leq 2n - l_1 + F(l_1, \dots, l_m). \quad (7)$$

Приведём оценки экспонентов для некоторых частных классов орграфов. Из (2) (как и из (7)) следует, что для сильно связного орграфа Γ с петлёй

$$\exp \Gamma \leq 2n - 2. \quad (8)$$

Оценка (8) уточнена [16, с. 121–122] с учётом (3). Введём следующие обозначения: Π — множество вершин с петлёй в орграфе Γ , $d_{i,p,j}$ — длина кратчайшего пути из i в j , проходящего через вершину p , $i, j, p \in \mathbb{N}_n$. В Γ имеются пути из i в j длины t для любого $t \geq \min_{p \in \Pi} d_{i,p,j}$. Следовательно,

$$\exp \Gamma \leq \max_{i,j \in \{1, \dots, n\}} \min_{p \in \Pi} d_{i,p,j}.$$

Пусть $n > 2$ и Γ содержит контуры C и C' длины l и λ , причём $\gcd(l, \lambda) = 1$, $l > \lambda$ и h — число общих вершин контуров. Тогда при $h = 0$ (контуры независимые) из (6) следует, что

$$\exp \Gamma \leq l\lambda - 2l - 3\lambda + 3n,$$

и при $h > 0$ оценка (6) улучшена [17, с. 104] следующим образом:

$$\exp \Gamma \leq l\lambda - l - 3\lambda + h + 2n.$$

Получены также оценки экспонентов для орграфов с тремя простыми контурами длины l, λ, μ и с определёнными дополнительными дугами [18], где $\gcd(l, \lambda, \mu) = 1$.

Орграф без петель называют *турниром*, если каждая пара различных вершин соединена ровно одной дугой. Для примитивного турнира Γ доказано [14, с. 398], что

$$\text{diam } \Gamma \leq \exp \Gamma \leq \text{diam } \Gamma + 3.$$

Матрица M порядка n называется *частично разложимой*, если она содержит нулевую подматрицу размера $r \times s$, где $r, s > 0$ и $r + s = n$. Матрица *вполне неразложима*, если она не является частично разложимой. Вполне неразложимая матрица M примитивна [14, с. 300] и

$$\exp M \leq n - 1.$$

Обозначим через p_i число дуг, входящих в вершину i , а через q_i — число дуг, исходящих из вершины i (полустепень захода и полустепень исхода вершины i соответственно), $i = 1, \dots, n$. Граф называется *псевдосимметрическим*, если $p_i = q_i$ (*дихотомическим*, если $p_i = q_i = 2$),

$i = 1, \dots, n$. В [7] получены верхние оценки экспонентов примитивных псевдосимметрических и дихотомических графов, при этом орграфы классифицированы по длине обхвата (кратчайшего контура). Класс сильно связанных псевдосимметрических графов с n вершинами, каждая из которых имеет не менее k (в точности k) входящих и исходящих дуг, с обхватом не менее p (в точности p) обозначим через $H(n, k, p)$ ($G(n, k, p)$). Класс примитивных графов из $G(n, k, p)$ с обхватом в точности p обозначается через $P(n, k, p)$. Справедлива следующая цепочка включений:

$$P(n, k, p) \subset G(n, k, p) \subset H(n, k, p).$$

В [7, § 3, ч. 3] описаны структурные свойства графов из множества $G(n, 2, (n-1)/2)$. При нечётном $n > 12$ верно $G(n, 2, (n-1)/2) = P(n, 2, (n-1)/2)$ и для любого $\Gamma \in P(n, 2, (n-1)/2)$

$$\exp \Gamma \leq \frac{(n-1)^2}{4} + 5.$$

Верхние оценки экспонентов дихотомических графов получены в [7, § 4, ч. 3]. Для любого орграфа $\Gamma \in P(n, 2, p)$, где $3 \leq p \leq \lceil n/2 \rceil$, доказано, что

$$\exp \Gamma \leq \frac{(p+1)n}{2p-1} + p(n-2) + 5.$$

В [7, § 5, ч. 3] получены верхние оценки экспонентов графов из классов $P(n, k, p)$ при $p = 1, 2$. В частности, для любого $\Gamma \in P(n, k, 2)$, где $k > 2$, справедливо неравенство

$$\exp \Gamma \leq \begin{cases} \frac{1}{2}(29\frac{n-1}{k+1} - 5), & k > 6\frac{n-1}{n+1} - 1, \\ n + \frac{1}{2}(\frac{11n-6}{k+1} - 3), & k \leq 6\frac{n-1}{n+1} - 1. \end{cases}$$

Для любого $\Gamma \in P(n, k, 1)$, где $k > 2$, выполнено

$$\exp \Gamma \leq 3 \left(\frac{n-1}{k+1} + \frac{n-2}{k} \right) - 2.$$

2. Примитивность и субпримитивность множеств матриц и орграфов

Пусть $\widehat{M} = \{M_1, \dots, M_p\} \subseteq M_n^{0,1}$, $\langle \widehat{M} \rangle$ — мультипликативная подгруппа, порождённая словами в алфавите \widehat{M} . Слову $(M_{w_1}, \dots, M_{w_s}) \in \langle \widehat{M} \rangle$, где $w = w_1 \dots w_s$ — слово в алфавите \mathbb{N}_p , соответствует произведение матриц $M(w) = M_{w_1} \dots M_{w_s}$. Слово $(M_{w_1}, \dots, M_{w_s})$ назовём *положительным* (*примитивным*), если матрица $M(w)$ положительная (примитивная).

Множество \widehat{M} называется *множественно примитивным*, если при некотором $k \in \mathbb{N}$ положительны все слова длины k в алфавите \widehat{M} . Наименьшее такое k называется *множественным экспонентом* \widehat{M} . Множественно примитивное множество состоит только из примитивных матриц (орграфов), поэтому если положительны все слова длины k , то положительны все слова длины l при любом $l > k$.

Множественный экспонент любого множественно примитивного множества не превышает $2^n - 2$ [14], и эта оценка достижима. Множество вполне неразложимых матриц порядка n является множественно примитивным [7], и множественный экспонент не превышает $n - 1$.

Матрица M порядка n называется *r -неразложимой*, $0 \leq r < n$, если она не содержит нулевой подматрицы размера $p \times q$, где $p + q = n - r + 1$, $0 < p, q \leq n - r$. Наибольшее из чисел r , при которых матрица M является r -неразложимой, называется *индексом неразложимости* матрицы M .

Если индекс неразложимости матрицы M_i не меньше r , где $r > 0$, $i = 1, \dots, p$, то множество \widehat{M} множественно примитивное с множественным экспонентом k [13]:

$$k \leq \begin{cases} (n-1)/r, & \text{если } r \text{ делит } n-1, \\ \lceil (n-1)/r \rceil, & \text{в ином случае.} \end{cases}$$

Множество \widehat{M} называется *примитивным*, если полугруппа $\langle \widehat{M} \rangle$ содержит положительное слово; наименьшая длина положительного слова из $\langle \widehat{M} \rangle$ называется *экспонентом множества* \widehat{M} (обозначается через $\exp \widehat{M}$). Если такого слова не существует, то полагаем $\exp \widehat{M} = \infty$.

На множестве $M_n^{0,1}$ задан частичный порядок:

$$\begin{aligned} M' \leq M \text{ для } M = (m_{ij}), M' = (m'_{ij}) \\ \Leftrightarrow m'_{ij} \leq m_{ij} \text{ для любой пары } (i, j) \in \mathbb{N}_n^2. \end{aligned}$$

На булеане множества $M_n^{0,1}$ задан квазипорядок, а именно:

$$\begin{aligned} \widehat{M}' \preceq \widehat{M} \text{ для множеств } \widehat{M}, \widehat{M}' \\ \Leftrightarrow \text{для любой матрицы } M' \in \widehat{M}' \text{ имеется} \\ \text{матрица } M \in \widehat{M} \text{ такая, что } M' \leq M. \end{aligned}$$

Если $\widehat{M}' \preceq \widehat{M}$, то $\exp \widehat{M} \leq \exp \widehat{M}'$.

Обозначим через $\widehat{M} \setminus M$ подмножество \widehat{M} , которое получается из \widehat{M} удалением матрицы M . Слово $(M_{w_1}, \dots, M_{w_s})$ в алфавите $\widehat{M} \setminus M$ назовём

покрывающим для M , если $M \leq M(w)$. Матрицу M , для которой существует покрывающее слово, назовём *избыточной матрицей* в множестве \widehat{M} . Множество \widehat{M} называется *минимальным*, если оно не содержит избыточной матрицы. Матрица M называется *максимальной матрицей* множества \widehat{M} , если для матрицы $M' \in \widehat{M}$ из соотношения $M \leq M'$ следует $M = M'$. Множество матриц \widehat{M} называется *сокращённым*, если оно состоит только из максимальных матриц. Аналогично определяются понятия максимального орграфа и сокращённого множества орграфов. Любое множество матриц может быть приведено к сокращённому удалением всех не максимальных матриц.

Множеству \widehat{M} биективно соответствует множество орграфов $\widehat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$, где M_r — матрица смежности вершин орграфа Γ_r , а также помеченный мультиграф $\Gamma^{(p)} = \Gamma_1 \cup \dots \cup \Gamma_p$, в котором дуга орграфа Γ_r помечена символом r , $r = 1, \dots, p$. В мультиграфе $\Gamma^{(p)}$ любой путь длины s помечен словом $w = w_1 \dots w_s$, составленным из меток дуг пути. Множество $\widehat{\Gamma}$ *примитивное*, если найдётся слово w в алфавите \mathbb{N}_p такое, что для любых $i, j \in \mathbb{N}_n$ в орграфе $\Gamma^{(p)}$ имеется путь длины s из i в j с меткой w . Наименьшая длина s такого слова равна $\exp \widehat{\Gamma}$.

Справедливо такое обобщение основной теоремы [22, ч. 1]: в мультиграфе $\Gamma^{(p)}$ число путей длины s из вершины i в вершину j с меткой (w_1, \dots, w_s) равно $m_{ij}(w)$, где $M(w) = (m_{ij}(w))$. Из обобщения основной теоремы следует, что множество орграфов $\widehat{\Gamma}$ примитивно тогда и только тогда, когда множество матриц \widehat{M} примитивно, и $\exp \widehat{\Gamma} = \exp \widehat{M}$.

Из данных определений и правила умножения матриц следуют нижеперечисленные свойства.

1. Множество \widehat{M} примитивно тогда и только тогда, когда полугруппа $\langle \widehat{M} \rangle$ содержит примитивное слово $(M_{w_1}, \dots, M_{w_s})$, при этом

$$\exp \widehat{M} \leq s \cdot \exp M(w),$$

где s — длина примитивного слова, $M(w) = M_{w_1} \dots M_{w_s}$ [2].

2. Если множество \widehat{M} примитивно, то матрица $M = M_1 + \dots + M_p$ также примитивна и $\exp M \leq \exp \widehat{M} \leq \min\{\exp M_1, \dots, \exp M_p\}$ [2].

3. Существуют примитивные множества, не содержащие примитивных матриц.

4. Матрица M избыточна в примитивном множестве \widehat{M} тогда и только тогда, когда подмножество $\widehat{M} \setminus M$ примитивно [3].

5. Минимальное множество матриц является сокращённым [3].

6. Если множество матриц \widehat{M} сокращённое, то оно образует антицепь

в решётке $\langle M_n^{0,1}, \leq \rangle$ и $p \leq C_m^{\lceil m/2 \rceil}$, где $m = n^2$; при $p = 2$ существует $2^{2m-1} + 2^{m-1} - 3^m$ сокращённых множеств матриц [3].

7. Если каждая матрица множества \widehat{M} не содержит нулевых строк и столбцов и $M(w) > 0$, то $M(u) > 0$ для любого продолжения u слова w .

8. Если множество \widehat{M} примитивно, то мультиграф $\Gamma^{(p)}$ сильно связный.

9. Экспонент орграфа Γ_r , $r = 1, \dots, p$, не меньше диаметра мультиграфа $\Gamma^{(p)}$.

Критерий примитивности множества матриц \widehat{M} без нулевых строк и столбцов сформулирован на матричном языке и доказан Ю. В. Протасовым и А. С. Войновым [41], различные варианты его доказательства даны в [4, 5, 28, 41]. Суть критерия такова: полугруппа $\langle \widehat{M} \rangle$ не содержит положительных слов тогда и только тогда, когда существует разбиение множества \mathbb{N}_n на подмножества $\Omega_1, \dots, \Omega_r$, $r > 1$, на которых все матрицы из \widehat{M} действуют как перестановки. Оценка экспонента множества \widehat{M} дана А. С. Войновым в [46]:

$$\exp \widehat{M} \leq \frac{n^3 + n^2}{2} - 2n + 1.$$

Улучшение этой оценки возможно при учёте зависимости от порядка множества \widehat{M} .

Доказан критерий примитивности орграфа $\Gamma_{w_1} \dots \Gamma_{w_s}$ для произвольного слова $w = w_1 \dots w_s$ в алфавите \mathbb{N}_p [3].

Путь имеет метку w^t , если он есть конкатенация t путей с метками w ; путь с меткой w^0 пуст. Сильно связный мультиграф $\Gamma^{(p)}$ назовём w -сильно связным, если для любых $i, j \in \mathbb{N}_n$ существует путь с меткой $w^{t_{ij}}$ из i в j при некотором $t_{ij} \in \mathbb{N}$.

Теорема 3. Орграф $\Gamma(w) = \Gamma_{w_1} \dots \Gamma_{w_s}$, где $w = w_1 \dots w_s$, примитивен тогда и только тогда, когда $\Gamma^{(p)}$ является w -сильно связным и содержит контуры с метками w^{t_1}, \dots, w^{t_m} , где $\gcd(t_1, \dots, t_m) = 1$.

Распознать примитивность множества \widehat{M} можно с помощью применения критерия примитивности орграфа $\Gamma(w)$ для различных слов w . Число проверяемых слов конечно в силу конечности множества $M_n^{0,1}$.

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

Получены условия примитивности и оценки экспонентов для некоторых множеств гамильтоновых орграфов [3]. Пусть $\widehat{\Gamma} = \{\Gamma_0, \dots, \Gamma_{n-1}\}$ —

множество орграфов, где оргграф Γ_i имеет гамильтонов контур $(0, \dots, n-1)$, $i = 0, \dots, n-1$. Если

а) оргграф Γ_i имеет дугу $(i, (i+l) \bmod n)$, $n \geq l > 1$, $i = 0, \dots, n-1$, то множество $\widehat{\Gamma}$ примитивно тогда и только тогда, когда $\gcd(n, l-1) = 1$, при этом

$$n-1 \leq \exp \widehat{\Gamma} \leq 2n-2;$$

б) оргграф Γ_i имеет дуги $(i, (i+l) \bmod n)$ и $(i, (i+\lambda) \bmod n)$, $n \geq \lambda > l > 1$, то множество $\widehat{\Gamma}$ примитивно тогда и только тогда, когда $\gcd(n, l-1, \lambda-1) = 1$ [1]; если при этом $\gcd(n, l-1) = 1$, то

$$\exp \widehat{\Gamma} \leq n-1 + \max\{b, n-b+1\},$$

где $b = (\lambda-1)(l-1)^{\phi(n)-1} \bmod n$, $\phi(n)$ — функция Эйлера.

Другое обобщение примитивности множеств, введённое в 2010 г. [15], называется субпримитивностью. Множество матриц \widehat{M} называется *субпримитивным*, если $M_\Sigma(w) > 0$ для некоторого слова $w = w_1 \dots w_s$ в алфавите \mathbb{N}_p , где

$$M_\Sigma(w) = M(w_1) + M(w_1 w_2) + \dots + M(w_1 \dots w_s).$$

Субэкспонентом множества матриц \widehat{M} (обозначается через $\text{sbxp } \widehat{M}$) называется наименьшая длина s слова w , при котором $M_\Sigma(w) > 0$. Если такого слова не существует, то полагаем $\text{sbxp } \widehat{M} = \infty$. Для любого множества матриц \widehat{M} выполнена оценка

$$\text{diam } \Gamma^{(p)} \leq \text{sbxp } \widehat{M} \leq \exp \widehat{M}.$$

Если множество \widehat{M} состоит из единственной матрицы M , то

$$\text{sbxp } \widehat{M} = \text{diam } \Gamma.$$

Получен критерий субпримитивности [15, с. 205]: множество \widehat{M} субпримитивно тогда и только тогда, когда мультиграф $\Gamma^{(p)}$ сильно связный. Дана универсальная оценка субэкспонента множества матриц [16]: если множество \widehat{M} субпримитивно, $n \geq 4$, то

$$\text{sbxp } \widehat{M} \leq \frac{(n^2-2)(n-1)}{2}.$$

3. Локальная примитивность матриц и графов

В 1990-е гг. положено начало исследованию локальных экспонентов примитивных орграфов [29]. *Локальным экспонентом вершины i* орграфа Γ (обозначаем через $\exp(\Gamma, i)$) названо наименьшее натуральное γ такое, что для любого $t \geq \gamma$ в Γ имеется путь длины t из i в любую вершину. Показано, что $\exp(\Gamma, i) \leq n^2 - 3n + i + 2$.

Положим, что $\exp(\Gamma, 1) \leq \exp(\Gamma, 2) \leq \dots \leq \exp(\Gamma, n)$ (это верно при определённой нумерации n вершин графа) и обозначим через $N_{n,k}$ множество всех k -элементных подмножеств множества \mathbb{N}_n вершин орграфа, $1 \leq k \leq n$. *Локальным экспонентом множества вершин I* (обозначаем через $\exp(\Gamma, I)$) названо наименьшее натуральное γ такое, что для любого $t \geq \gamma$ в Γ существует путь длины t из некоторой вершины множества I в любую вершину, т. е. $\exp(\Gamma, I) \leq \min_{i \in I} \exp(\Gamma, i)$. Величины

$$f(\Gamma, k) = \min_{I \in N_{n,k}} \exp(\Gamma, I), \quad F(\Gamma, k) = \max_{I \in N_{n,k}} \exp(\Gamma, I)$$

названы k -м нижним и k -м верхним мультиэкспонентом примитивного орграфа Γ соответственно. Получены оценки этих величин для $k = 2, \dots, n-2$:

$$f(\Gamma, k) \leq n^2 - (k+2)n + k + 2,$$

$$F(\Gamma, k) \leq n^2 - (k+1)n + k + 1.$$

В [37] представлены оценки локального экспонента вершин, k -го нижнего и верхнего мультиэкспонентов для различных классов матриц и орграфов. Введены определения i -примитивного, k -нижнепримитивного и k -верхнепримитивного орграфа, обобщающие свойство примитивности орграфа.

В [35] обобщены понятия, введённые в [29]: r -экспонентом множества вершин I (обозначается через $\exp_r(\Gamma, I)$) при $r \leq n$ называется наименьшее натуральное γ такое, что существует множество вершин $J \in N_{n,r}$, для которого при любом $t \geq \gamma$ в Γ существует путь длины t хотя бы из одной вершины из множества I в любую вершину из множества J . При допустимых k, r числа

$$f_r(\Gamma, k) = \min_{I \in N_{n,k}} \exp_r(\Gamma, I), \quad F_r(\Gamma, k) = \max_{I \in N_{n,k}} \exp_r(\Gamma, I)$$

называются k -м нижним и k -м верхним r -мультиэкспонентом орграфа Γ соответственно. Для примитивного орграфа Γ при $2 \leq k < r \leq n$

показано, что

$$f_r(\Gamma, k) \leq nr - (k+1)n + (k-1)r + 2,$$

$$F_r(\Gamma, k) \leq nr - n - r + 1.$$

В множестве P_n всех n -вершинных примитивных орграфов описаны множество $E_n(1)$ [44] и множества $E_n(i)$, $i = 2, \dots, n$, где $E_n(i) = \{\exp(\Gamma, i) \mid \Gamma \in P_n\}$ [38].

В 2013 г. В. М. Фомичёв ввёл понятия локальной примитивности и локального экспонента матриц и орграфов, распространённые на широкий класс непримитивных орграфов и определившие существенное расширение области приложений. Приведём соответствующие определения и основные результаты [7, 8, 21].

Пусть $I = \{i_1, \dots, i_k\}$, $J = \{j_1, \dots, j_r\}$, $\emptyset \neq I, J \subseteq \mathbb{N}_n$, $M(I \times J)$ — матрица размера $k \times r$, полученная из M удалением строк с номерами $i \notin I$ и столбцов с номерами $j \notin J$, $M(J^2) = M(I \times J)$ при $I = J$. Матрица M называется $I \times J$ -примитивной (локально примитивной), если $M^t(I \times J) > 0$ при всех $t \geq \gamma$, где $\gamma \in \mathbb{N}$. Наименьшее такое число γ обозначается через $I \times J$ -exp M или, кратко, $\gamma_{I \times J}$ (в случае $I = \{i\}$, $J = \{j\}$ обозначается через $i \times j$ -exp M или, кратко, $\gamma_{i \times j}$) и называется локальным $I \times J$ -экспонентом матрицы M .

Особенность свойства локальной примитивности состоит в том, что из соотношения $M^t(I \times J) > 0$ при некотором t в общем случае не следует, что $M^\tau(I \times J) > 0$ при всех $\tau > t$. Получен критерий локальной примитивности матрицы: если полугруппу $\langle M \rangle$ определяет соотношение $M^d = M^{d+p}$, где d — циклическая глубина, p — период матрицы M , то матрица M является $I \times J$ -примитивной тогда и только тогда, когда $M^t(I \times J) > 0$ при $t = d, d+1, \dots, d+p-1$, в случае локальной примитивности $I \times J$ -exp $M \leq d$.

Следующие достаточные условия локальной примитивности матрицы [10, с. 70] несложно проверить: если $M(I^2)$ не содержит нулевых строк или $M(J^2)$ не содержит нулевых столбцов и γ — наименьшее натуральное число, при котором $M^\gamma(I \times J) > 0$, то матрица M является $I \times J$ -примитивной и $I \times J$ -exp $M = \gamma$.

Орграф Γ является $I \times J$ -примитивным, если найдётся $\gamma \in \mathbb{N}$ такое, что при любом $t \geq \gamma$ для каждой пары $(i, j) \in I \times J$ в Γ имеется путь длины t из i в j ; наименьшее такое γ равно $I \times J$ -exp Γ . Орграф Γ является $I \times J$ -примитивным тогда и только тогда, когда матрица M является $I \times J$ -примитивной, и $I \times J$ -exp $M = I \times J$ -exp Γ .

Из данных определений вытекают следующие свойства:

1) оргграф Γ является $I \times J$ -примитивным тогда и только тогда, когда Γ $i \times j$ -примитивен для любой пары $(i, j) \in I \times J$, при этом $\gamma_{I \times J} =$

$$\max_{(i,j) \in I \times J} \gamma_{i \times j};$$

2) если оргграф Γ является $I \times J$ -примитивным, то для любой пары $(i, j) \in I \times J$ существует путь из вершины i в вершину j , проходящий через некоторую компоненту сильной связности (ксс) оргграфа Γ , называемую i, j -связывающей ксс.

Получен универсальный критерий локальной примитивности оргграфа и оценки локальных экспонентов, как универсальные, так и частные. Результаты получены для двух случаев: $I \cap J \neq \emptyset$ [10] и $I \cap J = \emptyset$ [21].

Введём в оргграфе Γ следующие обозначения: X — непустое подмножество вершин; Γ_X — ксс оргграфа Γ , содержащая X ;

$$\rho(I, J) = \min_{(i,j) \in I \times J} \rho_{i,j}, \quad \rho(I, J) = 0 \text{ при } I \cap J \neq \emptyset;$$

$$\theta(I, J) = \max_{i \in I} \rho(i, J), \quad \theta(I, J) = 0 \text{ при } I \subseteq J;$$

$$\tau(I, J) = \max_{j \in J} \rho(I, j), \quad \tau(I, J) = 0 \text{ при } J \subseteq I.$$

Теорема 4. При $I \cap J \neq \emptyset$ оргграф Γ является $I \times J$ -примитивным тогда и только тогда, когда в Γ имеется примитивная ксс $\Gamma_{I \cap J}$, i, j -связывающая для любой пары $(i, j) \in I \times J$, при этом

$$\begin{aligned} -\theta(I, \tilde{\Gamma}_{I \cap J}) - \tau(\tilde{\Gamma}_{I \cap J}, J) &\leq \exp \Gamma_{I \cap J} - \gamma_{I \times J} \\ &\leq \theta(\tilde{\Gamma}_{I \cap J}, I \cap J) + \tau(I \cap J, \tilde{\Gamma}_{I \cap J}). \end{aligned}$$

Ксс U , а также любой содержащийся в U контур, назовём *смежными с путём w* , если w проходит через некоторые вершины U . Множество контуров назовём *смежным с путём w* , если каждый контур множества смежен с путём w . Обозначим через $\hat{C}(w) = \{C_1^w, \dots, C_m^w\}$ множество всех контуров, смежных с путём w . Пусть длины этих контуров равны l_1^w, \dots, l_m^w соответственно. Индексом пути w (обозначается $d(w)$) назовём $\gcd(l_1^w, \dots, l_m^w)$.

Пусть вершины i и j не принадлежат общей ксс и j достижима из i . Обозначим через $P(i, j)$ множество всех простых путей из i в j , а через $P^{(d)}(i, j)$ — класс путей из $P(i, j)$ индекса d . Выполнено разбиение множества $P(i, j)$:

$$P(i, j) = P^{(d_1)}(i, j) \cup \dots \cup P^{(d_k)}(i, j). \quad (9)$$

Спектром множества путей W называется множество чисел $\text{spc } W = \{\text{len } w \mid w \in W\}$. Обозначим $\text{spc}_d W = \{\text{len } w \bmod d \mid w \in W\}$, $\overline{\text{spc}}_d W = \mathbb{Z}_d \setminus \text{spc}_d W$, и в соответствии с (9) имеем

$$H(P(i, j)) = \overline{\text{spc}}_{d_1} P^{(d_1)}(i, j) \times \cdots \times \overline{\text{spc}}_{d_k} P^{(d_k)}(i, j).$$

Множество целых чисел Y , содержащее полную систему вычетов по модулю d , называется d -полным. Для d -полного множества Y через $\xi_d(Y)$ обозначим такое наименьшее натуральное число a , что для любого из чисел $a, a+1, \dots, a+d-1$ в Y имеется число $b \leq a$, сравнимое с a по модулю d .

Доказано, что оргграф Γ $i \times j$ -примитивен тогда и только тогда, когда система сравнений $\{x \equiv b_\theta \pmod{d_\theta}, \theta = 1, \dots, k\}$ при любом наборе $(b_1, \dots, b_k) \in H(P(i, j))$ не имеет решений по модулю $\delta = \text{lcm}(d_1, \dots, d_k)$.

Обозначим через $W^{(d)}(i, j)$ множество всех путей индекса d из вершины i в вершину j . Для $i \times j$ -примитивного оргграфа верна оценка $\gamma_{i \times j} \leq \xi_\delta(Y)$, где

$$Y = \bigcup_{d \in \{d_1, \dots, d_k\}} \bigcup_{\tau=0}^{\delta/d-1} (\tau d + \text{spc } W^{(d)}(i, j)). \quad (10)$$

В частности, оргграф Γ $i \times j$ -примитивный, если при некотором $d \in \{d_1, \dots, d_k\}$ множество $\text{spc } P^{(d)}(i, j)$ является d -полным. В этом случае $\gamma_{i \times j} \leq \xi_d(Y)$, где

$$Y = \text{spc } W^{(d)}(i, j). \quad (11)$$

Величина полученных оценок в ряде случаев характеризуется следующим утверждением: если в Γ множество контуров длины l_1, \dots, l_m индекса d смежно с каждым путём из $P^{(d)}(i, j)$, то при $n \rightarrow \infty$

$$i \times j\text{-exp } \Gamma \leq \mathcal{O}(\max(mn, d \cdot F(l_1/d, \dots, l_m/d))).$$

В [21] оценки (10) и (11) более детально выражены через характеристики множества $P(i, j)$ и длины контуров оргграфа. В [9] получены оценки локальных экспонентов для частных классов оргграфов.

4. Прикладные направления исследований

Одной из важных задач криптографического анализа является определение множества существенных переменных функций, в частности, координатных функций преобразований векторного пространства.

Для преобразования $g: V_n \rightarrow V_n$ (заданного системой координатных функций $\{f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)\}$) через $\Gamma(g)$ обозначим перемешивающий орграф с множеством вершин \mathbb{N}_n , где (i, j) — дуга тогда и только тогда, когда x_i — существенная переменная функции f_j , $i, j \in \{1, \dots, n\}$, $n > 1$. Матрицу $M(g)$ смежности вершин графа $\Gamma(g)$ называют *перемешивающей матрицей преобразования* g .

При анализе произведения $g_1 \dots g_t$ преобразований векторного пространства для решения задачи применяется оценочный матрично-графовый подход (МГП). Суть МГП состоит в построении перемешивающих матриц $M(g_1), \dots, M(g_t)$ (перемешивающих орграфов $\Gamma(g_1), \dots, \Gamma(g_t)$) преобразований g_1, \dots, g_t и определении множества ненулевых элементов в произведении матриц $M(g_1) \dots M(g_t)$ (множества путей в произведении орграфов $\Gamma(g_1) \dots \Gamma(g_t)$). Корректность такого подхода основана на неравенстве из [22, ч. 1, с. 183]:

$$M(g_1 \dots g_t) \leq M(g_1) \dots M(g_t).$$

Реализация МГП существенно проще с точки зрения сложности вычислений по сравнению с точным решением задачи для преобразования $g_1 \dots g_t$.

4.1. Экспоненты перемешивающих графов регистровых преобразований. Регистровые преобразования активно используются при построении систем защиты информации, так как обладают рядом позитивных криптографических свойств и весьма удобно реализуются как аппаратным способом, так и программно на ЭВМ.

Обозначим через $R(n, r, t)$ класс преобразований множества V_{nr} , называемых *преобразованиями регистров сдвига длины n над множеством V_r с t обратными связями*. Заметим, что преобразования из класса $R(2, r, 1)$ реализуются блочными шифрами Фейстеля (например, при $r = 32$ DES-алгоритм и ГОСТ 28147-89). Преобразование $\varphi \in R(2, r, 1)$ при фиксированном ключе имеет вид

$$\varphi(z_0, z_1) = (z_1, z_0 \oplus \psi(z_1)),$$

где $z_0, z_1 \in V_r$, $\psi: V_r \rightarrow V_r$ — отличная от константы функция усложнения и \oplus есть XOR-суммирование векторов пространства V_r .

При $n > 2$ и $1 \leq t < n$ преобразования из $R(n, r, t)$ можно рассматривать как обобщения шифров Фейстеля. Примерами являются алгоритмы CAST-256, RC6, MARS и др. В [6] исследовано преобразование $\varphi \in R(n, r, 1)$ вида

$$\varphi(z_0, \dots, z_{n-1}) = (z_1, \dots, z_{n-1}, f(z_0, \dots, z_{n-1})), \quad (12)$$

где $z_0, \dots, z_{n-1} \in V_r$, $f: V_{nr} \rightarrow V_r$ — функция обратной связи регистра:

$$f(z_0, \dots, z_{n-1}) = z_0 \oplus \psi(z_1, \dots, z_{n-1}). \quad (13)$$

Известно, что φ — подстановка тогда и только тогда, когда f биективна по переменной z_0 [15, с. 119].

Применим МГП к оценке перемешивающих свойств регистровых преобразований (12). Введём необходимые обозначения и определения.

Для преобразования φ вершины перемешивающего орграфа $\Gamma(\varphi)$ обозначим числами $u + ri$, координатные булевы функции — через φ_{u+ri} , $u = 0, \dots, r-1$, $i = 0, \dots, n-1$. Через $E(\varphi_{u+ri})$ обозначим множество номеров существенных переменных координатной функции φ_{u+ri} . По определению перемешивающего орграфа пара $(v + ri, u + rj)$ образует дугу в $\Gamma(\varphi)$ тогда и только тогда, когда $(v + ri) \in E(\varphi_{u+rj})$, $v, u \in \{0, \dots, r-1\}$, $i, j \in \{0, \dots, n-1\}$.

Двоичные r -мерные векторы рассмотрим как блоки информации, составляющие nr -мерные векторы состояний регистра сдвига. В связи с этим для класса регистровых преобразований $\varphi \in R(n, r, t)$ определены блоковые перемешивающие n -вершинные орграфы, обозначаемые через $\Gamma_B(\varphi)$. В орграфе $\Gamma_B(\varphi)$ имеется дуга (i, j) тогда и только тогда, когда некоторый бит j -го выходного блока преобразования φ существенно зависит от некоторых битов i -го входного блока преобразования φ , $i, j = 0, \dots, n-1$. Исследование блоковых перемешивающих орграфов удобно в силу относительно небольшого числа вершин по сравнению с перемешивающими орграфами. Вместе с тем, точность получаемых результатов ниже. Для любого преобразования $\varphi \in R(n, r, t)$ выполнена оценка $\exp \Gamma_B(\varphi) \leq \exp \Gamma(\varphi)$.

В [25, 26, 45] исследованы блоковые n -вершинные перемешивающие орграфы для регистров из классов $R(n, r, 1)$, $R(n, r, n/2)$, $R(n, r, n-1)$, соответствующих обобщённым сетям Фейстеля 1-го, 2-го и 3-го типов. Для блокового орграфа преобразования $\varphi \in R(n, r, 1)$ верна оценка

$$\exp \Gamma_B(\varphi) \leq (n-1)^2 + 1,$$

если φ реализует циклический сдвиг блоков, и

$$\exp \Gamma_B(\varphi) \leq \left\lceil \frac{n(n+2)}{2} \right\rceil - 2,$$

если φ реализует некоторую перестановку блоков. При чётном n для $\varphi \in R(n, r, n/2)$ получена оценка $\exp \Gamma_B(\varphi) \leq n$. Данная оценка понижена

до $2 \log_2 n$ при определённой перестановке блоков. Для $\varphi \in R(n, r, n-1)$ выполнена оценка $\exp \Gamma_B(\varphi) \leq n$. С использованием результатов исследования блоковых перемешивающих графов оценены перемешивающие свойства блочных алгоритмов TWINE (2012 г.) и Lilliput (2016 г.), рекомендуемых разработчиками для защиты информации в условиях ограниченных ресурсов пользователя.

Приведём основные результаты [6] исследования примитивности перемешивающих nr -вершинных орграфов $\Gamma(\varphi)$ подстановок φ из класса $R(n, r, 1)$, заданных в соответствии с (12) и (13). Для орграфа $\Gamma(\varphi)$ определим оргграф $\Gamma(\psi)$ с числом вершин r : пара (v, u) образует дугу в $\Gamma(\psi)$ тогда и только тогда, когда функция $\varphi_{u+r(n-1)}$ зависит существенно хотя бы от одной из переменных множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$, $v, u \in \{0, \dots, r-1\}$. Оргграф $\Gamma(\varphi)$ сильно связный, если и только если оргграф $\Gamma(\psi)$ сильно связный [6, с. 78].

Теорема 5 (достаточное условие примитивности $\Gamma(\varphi)$). Пусть координатная функция $\varphi_{u+r(n-1)}$ подстановки φ зависит существенно от переменных с номерами $u + rd_j$, $u = 0, \dots, r-1$, где $j = 0, \dots, q$, $0 < q$, $0 = d_0 < \dots < d_q < n$. Тогда сильно связный оргграф $\Gamma(\varphi)$ примитивен, если $\gcd L = 1$, где $L = \{n - d_0, \dots, n - d_q\}$. В этом случае

$$\exp \Gamma(\varphi) \leq n^2 r + nr - 2n. \quad (14)$$

В различных условиях эта оценка уточнена. Если переменная x_u существенная для φ_u , где $u \in \{(n-1)r, (n-1)r+1, \dots, nr-1\}$, то $\exp \Gamma(\varphi) \leq 2nr - 2$.

Если l_1 — длина простого контура в орграфе $\Gamma(\varphi)$, то

$$\exp \Gamma(\varphi) \leq nr + \min\{n, l_1\}(nr - 2). \quad (15)$$

Оценка (15) улучшает оценку (14) при $l_1 < n$.

Если $\varphi_{u+r(n-1)}$ зависит существенно от x_{v+rk} и $x_{v+r(k-1)}$, $k \in \{2, \dots, n-1\}$, и l_2 — длина простого контура в $\Gamma(\varphi)$, проходящего через дугу $(v + (k-1)r, u + (n-1)r)$, то оргграф $\Gamma(\varphi)$ примитивный и

$$\exp \Gamma(\varphi) \leq l_2^2 - 2l_2 + 2nr - 1. \quad (16)$$

Оценка (16) улучшает оценку (14) при $l_2 < \sqrt{n^2 r - n(r-2)}$.

Если в орграфе $\Gamma(\varphi)$ имеется простой контур длины l_3 , проходящий через дугу $(v + kr, u + (n-1)r)$, $v, u = 0, \dots, r-1$, и $\gcd(l_3, n) = 1$, то

$$\exp \Gamma(\varphi) \leq n(l_3 + 2r) - k - l_3 - 2 \min\{l_3, n\}. \quad (17)$$

Оценка (17) улучшает оценку (14) при $l_3 < r(n-1)$.

При некоторых функциях обратной связи величина $\exp \Gamma(\varphi)$ близка к $2nr$.

4.2. Экспоненты перемешивающих графов преобразований модифицированных аддитивных генераторов. Ряд криптографических алгоритмов (Fish, Pike, Mush) построены на основе аддитивных генераторов по модулю 2^r , $r > 1$, известных также как «запаздывающие генераторы Фибоначчи» [23, 27, 43]. Такие алгоритмы имеют эффективную реализацию, вместе с тем, они плохо перемешивают входные данные. В связи с этим особый интерес представляет изучение перемешивающих свойств модификаций аддитивных генераторов по модулю 2^r с помощью преобразования g множества V_r , применяемого к значениям функции обратной связи и обеспечивающего полное перемешивание входных данных.

Обозначим через $\text{МАГ}(n, r, t)$ класс преобразований регистров сдвига длины n над множеством V_r с t обратными связями, построенных на основе модифицированных аддитивных генераторов (МАГ), $n, r, t \in \mathbb{N}$, по определению $\text{МАГ}(n, r, t) \subset R(n, r, t)$ при любом преобразовании g . В [8] исследованы преобразования $\varphi^g \in \text{МАГ}(n, r, 1)$, соответствующие модифицирующему преобразованию g , при итерациях которых достигается полное перемешивание входных данных. Пусть b — биекция, определяющая двоичный r -мерный вектор для числа $\tilde{z} \in Z_{2^r}$: если $\tilde{z} = 2^{r-1}x_0 + \dots + 2x_{r-2} + x_{r-1}$, то $b(\tilde{z}) = (x_0, \dots, x_{r-1}) \in V_r$. Тогда при модификации g преобразование φ^g имеет вид

$$\varphi^g(z_0, \dots, z_{n-1}) = \left(z_1, \dots, z_{n-1}, g\left(b\left(\left(\sum_{k \in D} \tilde{z}_k\right) \bmod 2^r\right)\right) \right),$$

где $z_0, \dots, z_{n-1} \in V_r$, $D = \{d_0, \dots, d_q\} \subseteq \{0, \dots, n-1\}$ — непустое множество точек съёма (номера суммируемых чисел из набора $(\tilde{z}_0, \dots, \tilde{z}_{n-1})$), $0 < q$, $0 = d_0 < \dots < d_q < n$. Как и ранее, $L = \{n - d_0, \dots, n - d_q\}$.

Теорема 6 (критерий примитивности $\Gamma(\varphi^g)$). *При $q \geq 1$ сильно связный орграф $\Gamma(\varphi^g)$ является примитивным тогда и только тогда, когда $\gcd L = 1$.*

Обозначим через $\Delta(D) = \max\{n - d_q, d_q - d_{q-1}, \dots, d_1 - d_0\}$ число, характеризующее наибольший разброс соседних точек съёма на регистре, через $F(L)$ — число Фробениуса, а через $\rho(0, r-1)$ — длину кратчайшего пути из вершины 0 в вершину $r-1$ в r -вершинном перемешивающем орграфе $\Gamma(g)$.

Теорема 7. Если оргграф $\Gamma(\varphi^g)$ примитивный, то

$$\exp \Gamma(\varphi^g) \leq \Delta(D) + (n - d_q)\rho(0, r - 1) + F(L) + n.$$

Следствие 2. Если $d_q = n - 1$ и в $\Gamma(g)$ есть дуга $(0, r - 1)$, то $\exp \Gamma(\varphi^g) \leq \Delta(D) + n$.

Полученные оценки показывают, что при определённых значениях параметров регистровых преобразований, построенных на основе МАГ, полное перемешивание знаков начального состояния может быть достигнуто за число итераций, существенно меньшее числа вершин перемешивающего оргграфа. Конструкции на основе МАГ представляются перспективными для построения криптографических алгоритмов.

4.3. Локальные экспоненты перемешивающих графов преобразований генераторов гаммы. При оценке множества существенных ключевых переменных для выходных функций генераторов гаммы исследуются перемешивающие графы преобразований внутренних состояний генераторов. Такие оргграфы нередко не являются примитивными, но обладают свойствами локальной примитивности.

Введём следующие обозначения: h — преобразование множества состояний генератора, h_t^s — t -я координатная функция преобразования h^s , $t = 1, 2, \dots$, $\Gamma(h)$ — перемешивающий оргграф преобразования h , $E(f)$ — множество номеров существенных переменных функции f .

Пусть генератор построен на основе регистров правого сдвига: управляющего длины m с функцией обратной связи $f_1(x_1, \dots, x_m)$ и генерирующего длины n с функцией обратной связи $f_2(x_{m+1}, \dots, x_{m+n})$, $m, n > 1$.

Пусть h — преобразование множества V_{m+n} состояний генератора, заданное следующей системой булевых координатных функций:

$$\begin{aligned} &\{h_1(x_1, \dots, x_{m+n}), \dots, h_{m+n}(x_1, \dots, x_{m+n})\}, \\ &h_1 = f_1(x_1, \dots, x_m), \\ &E(f_1) = \{b_1, \dots, b_\nu\}, \quad 1 \leq b_1 < \dots < b_\nu = m, \\ &h_k = x_{k-1}, \quad k = 2, \dots, m, m+2, \dots, m+n, \\ &h_{m+1} = x_m \oplus f_2(x_{m+1}, \dots, x_{m+n}), \\ &E(f_2) = \{c_1, \dots, c_\mu\}, \quad m+1 \leq c_1 < \dots < c_\mu = m+n. \end{aligned}$$

Пусть $\gcd(b_1, \dots, b_\nu) = d_1$, $\gcd(c_1 - m, \dots, c_\mu - m) = d_2$.

При начальном состоянии (x_1, \dots, x_{m+n}) генератора t -й знак гаммы равен $\gamma_t = h_{m+n}^t(x_1, \dots, x_{m+n})$. Обозначим $I = \{1, \dots, m\}$. Исследована $\mathbb{N}_{m+n} \times \{m+n\}$ -примитивность и $I \times \{m+n\}$ -примитивность графа $\Gamma(h)$.

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

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

где $\rho_2 = \max_{l \in \mathbb{N}_\mu} \{c_l - c_{l-1}\}$, $c_0 = m$ [21].

Утверждение 2. Орграф $\Gamma(h)$ является $I \times \{m+n\}$ -примитивным тогда и только тогда, когда $\gcd(d_1, d_2) = 1$. В случае $I \times \{m+n\}$ -примитивности верна оценка

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

где $\rho_1 = \max_{l \in \mathbb{N}_\nu} \{b_l - b_{l-1}\}$, $b_0 = 1$ [21].

Одним из способов усложнения зависимости знаков выходной последовательности от знаков начального заполнения является неравномерное движение информации в генераторе. Например, генератор «1–2 шагов» [15] построен на основе управляющего и генерирующего двоичных регистров сдвига. Преобразование h множества состояний генератора нелинейно в силу неравномерности движения генерирующего регистра. В зависимости от знака управляющей последовательности (выходного знака управляющего регистра) генерирующий регистр сдвигается каждый такт на 1 или 2 шага.

Пусть управляющий и генерирующий регистры правого сдвига имеют длины $m, n > 2$, их функции обратной связи суть $f_1(x_1, \dots, x_m)$, $f_2(x_{m+1}, \dots, x_{m+n})$ соответственно, движение генерирующего регистра на 1–2 шага задано с помощью управляющей функции $u(x_1, \dots, x_m)$. Подстановки, реализуемые управляющим и генерирующим регистрами, обозначим через $\phi(x_1, \dots, x_m)$ и $\psi(x_{m+1}, \dots, x_{m+n})$ соответственно. Тогда

$$h^t(x_1, \dots, x_{m+n}) = (\phi^t(x_1, \dots, x_m), \psi^{\sigma(t, x_1, \dots, x_m)}(x_{m+1}, \dots, x_{m+n})).$$

Здесь $\sigma(t, x_1, \dots, x_m)$ — «глубина продвижки» генерирующего регистра за t тактов работы генератора, определяемая формулой

$$\sigma(t, x_1, \dots, x_m) = \sum_{l=1}^t ((u(\phi^l(x_1, \dots, x_m)) \oplus 1) + 2u(\phi^l(x_1, \dots, x_m))),$$

$$t = 1, 2, \dots$$

При начальном состоянии (x_1, \dots, x_{m+n}) генератора t -й знак гаммы равен $\gamma_t = h_{m+n}^t(x_1, \dots, x_{m+n})$.

Пусть $E(f_2) = \{c_1, \dots, c_\mu\}$, $m+1 \leq c_1 < \dots < c_\mu = m+n$.

Утверждение 3. Орграф $\Gamma(h)$ является $\mathbb{N}_{m+n} \times \{m+n\}$ -примитивным, при этом

$$\mathbb{N}_{m+n} \times \{m+n\}\text{-exp } \Gamma(h) \leq \lceil n/2 \rceil + \max_{i \in \mathbb{N}_{m+n}} \rho_{i,m+1} + \lambda(\lambda-1),$$

где $\lambda = \lceil (c_1 - m)/2 \rceil$ [12].

Также исследованы локальные экспоненты других генераторов: с перемежающимся шагом [12] и генератора типа A5/1 [11]. В обоих случаях получены точные значения локальных экспонентов перемешивающих орграфов преобразований.

5. Перспективные направления исследований

Перспективными направлениями представляются следующие.

1. Исследование примитивности и локальной примитивности специальных классов матриц и графов, в том числе перемешивающих орграфов для множеств

- всех нелинейных преобразований векторных пространств;
- нелинейных регистров сдвига с несколькими обратными связями над конечными кольцами и полями;
- нелинейных регистров сдвига с одной и несколькими обратными связями над векторными пространствами.

2. Построение криптографических преобразований, имеющих перемешивающий граф с заданным ограничением экспонента или локального экспонента.

3. Улучшение универсальной оценки экспонентов орграфов с использованием длин непримитивного множества контуров и длин множества путей, проходящих через вершины данного множества контуров.

ЛИТЕРАТУРА

1. Авезова Я. Э. О примитивности некоторых множеств перемешивающих орграфов регистровых преобразований // Прикл. дискрет. математика. Прил. 2017. № 10. С. 60–62.
2. Авезова Я. Э., Фомичёв В. М. Комбинаторные свойства систем разноразмерных 0,1-матриц // Прикл. дискрет. математика. 2014. № 2 (24). С. 5–11.

3. **Авезова Я. Э., Фомичёв В. М.** Условия примитивности и оценки экспонентов множеств ориентированных графов // Прикл. дискрет. математика. 2017. № 35. С. 89–101.
4. **Альпин Ю. А., Альпина В. С.** Комбинаторные свойства неприводимых полугрупп неотрицательных матриц // Зап. научн. сем. ПОМИ. 2012. № 405. С. 13–23.
5. **Войнов А. С.** Многомерные уравнения самоподобия и приложения: дисс. ... докт. физ.-мат. наук: 01.01.01. Москва, 2016. 75 с.
6. **Дорохова А. М., Фомичёв В. М.** Уточненные оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикл. дискрет. математика. 2014. № 1. С. 77–83.
7. **Князев А. В.** Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: дисс. ... докт. физ.-мат. наук: 01.01.09. Москва, 2002. 203 с.
8. **Коренева А. М., Фомичёв В. М.** Перемешивающие свойства модифицированных аддитивных генераторов // Дискрет. анализ и исслед. операций. 2017. Т. 24, № 2. С. 32–52.
9. **Кяжин С. Н.** О применении условий локальной примитивности и оценок локальных экспонентов орграфов // Прикл. дискрет. математика. 2016. № 4. С. 81–98.
10. **Кяжин С. Н., Фомичёв В. М.** Локальная примитивность графов и неотрицательных матриц // Прикл. дискрет. математика. 2014. № 3. С. 68–80.
11. **Кяжин С. Н., Фомичёв В. М.** О локальных экспонентах перемешивающих графов функций, реализуемых алгоритмами типа A5/1 // Прикл. дискрет. математика. Прил. 2015. № 8. С. 11–13.
12. **Кяжин С. Н., Фомичёв В. М.** Перемешивающие свойства двухкаскадных генераторов // Прикл. дискрет. математика. Прил. 2016. № 9. С. 60–62.
13. **Сачков В. Н.** Вероятностные преобразователи и правильные мультиграфы // Тр. по дискрет. математике. 1997. Т. 1. С. 227–250.
14. **Сачков В. Н., Тараканов В. Е.** Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
15. **Фомичёв В. М.** Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
16. **Фомичёв В. М.** Свойства путей в графах и мультиграфах // Прикл. дискрет. математика. 2010. № 1. С. 118–124.
17. **Фомичёв В. М.** Оценки экспонентов примитивных графов // Прикл. дискрет. математика. 2011. № 2. С. 101–112.
18. **Фомичёв В. М.** Оценка экспонента некоторых графов с помощью чисел Фробениуса для трёх аргументов // Прикл. дискрет. математика. 2014. № 2. С. 88–96.

19. **Фомичёв В. М.** Новая универсальная оценка экспонентов графов // Прикл. дискрет. математика. 2016. № 3. С. 78–84.
20. **Фомичёв В. М.** О вычислительной сложности оригинальной и расширенной диофантовой проблемы Фробениуса // Дискрет. анализ и исслед. операций. 2017. Т. 24, № 3. С. 104–124.
21. **Фомичёв В. М., Кяжин С. Н.** Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24, № 1. С. 97–119.
22. **Фомичёв В. М., Мельников Д. А.** Криптографические методы защиты информации. М.: Изд-во ЮРАЙТ, 2016. 454 с.
23. **Anderson R.** On Fibonacci keystream generators // Fast Software Encryption. Proc. 2nd Int. Workshop (Leuven Belgium, Dec. 14–16, 1994). Heidelberg: Springer, 1995. P. 346–352. (Lect. Notes Comput. Sci.; Vol. 1008).
24. **Barghi A.** Exponents of primitive digraphs // <https://math.dartmouth.edu/~pw/M100W11/amir.pdf>.
25. **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 Trans. Comput. 2016. Vol. 65, No. 7. P. 2074–2089.
26. **Berger T. P., Minier M., Thomas G.** Extended generalized Feistel networks using matrix representation // Selected Areas in Cryptography. Rev. Sel. Pap. 20th Int. Conf. (Burnaby, Canada, Aug. 14–16, 2013). Heidelberg: Springer, 2014. P. 289–305. (Lect. Notes Comput. Sci.; Vol. 8282).
27. **Blöcher U., Dichtl M.** Fish: a fast software stream cipher // Fast Software Encryption. Proc. Camb. Security Workshop (Cambridge, UK, Dec. 9–11, 1993). Heidelberg: Springer, 1994. P. 41–44. (Lect. Notes Comput. Sci.; Vol. 809).
28. **Blondel V. D., Jungers R. M., Olshevsky A.** On primitivity of sets of matrices // Automatica. 2015. Vol. 61. P. 80–88.
29. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. No. 14. P. 483–499.
30. **Dulmage A. L., Mendelsohn N. S.** The exponent of a primitive matrix // Can. Math. Bull. 1962. No. 5. P. 241–244.
31. **Dulmage A. L., Mendelsohn N. S.** Gaps in the exponent set of primitive matrices // Ill. J. Math. 1964. No. 8. P. 642–656.
32. **Dulmage A. L., Mendelsohn N. S.** Graphs and matrices // Graph Theory Theor. Phys. 1967. P. 167–229.
33. **Frobenius G.** Über Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss. 1912. P. 456–477.
34. **Holladay J. C., Varga R. S.** On powers of non-negative matrices // Proc. Amer. Math. Soc. 1958. Vol. 9. P. 631.
35. **Huang Y., Liu B.** Generalized r -exponents of primitive digraphs // Taiwan. J. Math. 2011. Vol. 15, No. 5. P. 1999–2012.

36. **Lewin M., Vitek Y.** A system of gaps in the exponent set of primitive matrices // *Ill. J. Math.* 1981. Vol. 25, No. 1. P. 87–98.
37. **Liu B.** Generalized exponents of Boolean matrices // *Linear Algebra Appl.* 2003. Vol. 373. P. 169–182.
38. **Miao Z., Zhang K.** The local exponent sets of primitive digraphs // *Linear Algebra Appl.* 2000. Vol. 307. P. 15–33.
39. **Neufeld S. W.** A diameter bound on the exponent of a primitive directed graph // *Linear Algebra Appl.* 1996. Vol. 245. P. 27–47.
40. **Perkins P.** A theorem on regular graphs // *Pac. J. Math.* 1961. Vol. 2. P. 1529–1533.
41. **Protasov V. Yu., Voynov A. S.** Sets of nonnegative matrices without positive products // *Linear Algebra Appl.* 2012. Vol. 437, No. 3. P. 749–765.
42. **Ramírez Alfonsín J. L.** The Diophantine Frobenius problem // Oxford: Clarendon. Press, 2005. (Oxf. Lect. Ser. Math. Appl.; Vol. 30).
43. **Schneier B.** Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, Inc., New York, 1996.
44. **Shen J., Neufeld S.** Local exponents of primitive digraphs // *Linear Algebra Appl.* 1998. Vol. 268. P. 117–129.
45. **Suzaki T., Minematsu K.** Improving the generalized Feistel // *Fast Software Encryption. Rev. Sel. Pap. 17th Int. Workshop (Seoul, Korea, Feb. 7–10, 2010).* Heidelberg: Springer, 2010. 2010. P. 19–39. (Lect. Notes Comput. Sci.; Vol. 6147).
46. **Voynov A. S.** Shortest positive products of nonnegative matrices // *Linear Algebra Appl.* 2013. Vol. 439, No. 6. P. 1627–1634.
47. **Wielandt H.** Unzerlegbare nicht negative Matrizen // *Math. Z.* 1950. Bd. 52. S. 642–648.

Фомичёв Владимир Михайлович
Авезова Яна Эдуардовна
Коренева Алиса Михайловна
Кяжин Сергей Николаевич

Статья поступила
16 октября 2017 г.
Исправленный вариант —
23 марта 2018 г.

PRIMITIVITY AND LOCAL PRIMITIVITY OF DIGRAPHS AND NONNEGATIVE MATRICES

V. M. Fomichev^{1,2,3,a}, Ya. E. Avezova^{2,b},
A. M. Koreneva^{2,c}, and S. N. Kyazhin^{2,d}

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 Vavilova St., 119333 Moscow, Russia

E-mail: ^afomichev@nm.ru, ^bavezovayana@gmail.com,
^calisa.koreneva@gmail.com, ^ds.kyazhin@kaf42.ru

Abstract. The article surveys the main results on the primitivity and local primitivity of digraphs and matrices from the inception of this research area in 1912 by now. We review the universal and special criteria for primitivity and local primitivity as well as universal and special bounds on the exponents and local exponents of digraphs and matrices. We describe some cryptographic applications of this mathematical apparatus for analyzing the mixing properties of block ciphers and keystream generators. The new promising research directions are formulated in the study of primitivity and local primitivity of digraphs and matrices. Bibliogr. 47.

Keywords: primitive digraph, primitive matrix, local primitivity, primitive set, exponent, local exponent.

REFERENCES

1. Ya. E. Avezova, On primitivity of some sets of shift registers mixing digraphs, *Prikl. Diskretn. Mat., Prilozh.*, No. 10, 60–62, 2017 [Russian].
2. Ya. E. Avezova and V. M. Fomichev, Combinatorial properties of rectangular 0,1-matrix systems, *Prikl. Diskretn. Mat.*, No. 2, 5–11, 2014 [Russian].
3. Ya. E. Avezova and V. M. Fomichev, Conditions of primitivity and exponent bounds for sets of digraphs, *Prikl. Diskretn. Mat.*, No. 35, 89–101, 2017 [Russian].
4. Yu. A. Al'pin and V. S. Al'pina, Combinatorial properties of irreducible semigroups of nonnegative matrices, *Zap. Nauchn. Semin. POMI*, **405**, 13–23, 2012 [Russian]. Translated in *J. Math. Sci.*, **191**, No. 1, 4–9, 2013.

5. **A. S. Voynov**, Multidimensional equations of self-similarity and applications, *Dr. Sci. Diss.*, Mosk. Gos. Univ., Moscow, 2016 [Russian].
6. **A. M. Dorokhova** and **V. M. Fomichev**, Improvement of exponent estimates for mixing graphs of bijective shift registers over a set of binary vectors, *Prikl. Diskretn. Mat.*, No. 1, 77–83, 2014 [Russian].
7. **A. V. Knyazev**, Estimations for extreme values of principal metric characteristics of pseudosymmetrical graphs, *Dr. Sci. Diss.*, VTs RAN, Moscow, 2016 [Russian].
8. **A. M. Koreneva** and **V. M. Fomichev**, Mixing properties of modified additive generators, *Diskretn. Anal. Issled. Oper.*, **24**, No. 2, 32–52, 2017 [Russian]. Translated in *J. Appl. Ind. Math.*, **11**, No. 2, 215–226, 2017.
9. **S. N. Kyazhin**, On adaptation of digraph local primitiveness conditions and local exponent estimations, *Prikl. Diskretn. Mat.*, No. 4, 81–98, 2016 [Russian].
10. **S. N. Kyazhin** and **V. M. Fomichev**, Local primitiveness of graphs and nonnegative matrices, *Prikl. Diskretn. Mat.*, No. 3, 68–80, 2014 [Russian].
11. **S. N. Kyazhin** and **V. M. Fomichev**, On local exponents of the mixing graphs for the functions realized by A5/1 type algorithms, *Prikl. Diskretn. Mat., Prilozh.*, No. 8, 11–13, 2015 [Russian].
12. **S. N. Kyazhin** and **V. M. Fomichev**, Mixing properties of 2-cascade generators, *Prikl. Diskretn. Mat., Prilozh.*, No. 9, 60–62, 2016 [Russian].
13. **V. N. Sachkov**, Probabilistic converters and regular multigraphs. I, *Tr. Diskretn. Mat.*, **1**, 227–250, 1997 [Russian].
14. **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).
15. **V. M. Fomichev**, *Methods of discrete mathematics in cryptology*, Dialog-MIFI, Moscow, 2010 [Russian].
16. **V. M. Fomichev**, Properties of paths in graphs and multigraphs, *Prikl. Diskretn. Mat.*, No. 1, 118–124, 2010 [Russian].
17. **V. M. Fomichev**, The estimates for exponents of primitive graphs, *Prikl. Diskretn. Mat.*, No. 2, 101–112, 2011 [Russian].
18. **V. M. Fomichev**, Estimates for exponent of some graphs by means of Frobenius's numbers of three arguments, *Prikl. Diskretn. Mat.*, No. 2, 88–96, 2014 [Russian].
19. **V. M. Fomichev**, The new universal estimation for exponents of graphs, *Prikl. Diskretn. Mat.*, No. 3, 78–84, 2016 [Russian].
20. **V. M. Fomichev**, Computational complexity of the original and extended Diophantine Frobenius problem, *Diskretn. Anal. Issled. Oper.*, **24**, No. 3, 104–124, 2017 [Russian]. Translated in *J. Appl. Ind. Math.*, **11**, No. 3, 334–346, 2017.

21. 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.
22. V. M. Fomichev and D. A. Melnikov, *Cryptographic methods of information security*, in 2 pts, YURAYT, Moscow, 2016 [Russian].
23. R. Anderson, On Fibonacci keystream generators, in *Fast Software Encryption* (Proc. 2nd Int. Workshop FSE, Leuven, Belgium, Dec. 14–16, 1994), pp. 346–352, Springer, Heidelberg, 1995 (Lect. Notes Comput. Sci., Vol. 1008).
24. A. Barghi, Exponents of primitive digraphs. Available at <http://math.dartmouth.edu/~pw/M100W11/amir.pdf> (accessed Apr. 15, 2018).
25. 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.
26. 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), pp. 289–305, Springer, Heidelberg, 2014 (Lect. Notes Comput. Sci., Vol. 8282).
27. U. Blöcher and M. Dichtl, Fish: A fast software stream cipher, in *Fast Software Encryption* (Proc. Camb. Secur. Workshop, Cambridge, UK, Dec. 9–11, 1993), pp. 41–44, Springer-Verl., Heidelberg, 1994 (Lect. Notes Comput. Sci., Vol. 809).
28. V. D. Blondel, R. M. Jungers, and A. Olshevsky, On primitivity of sets of matrices, *Automatica*, **61**, 80–88, 2015.
29. R. A. Brualdi and B. Liu, Generalized exponents of primitive directed graphs, *J. Graph Theory*, **14**, 483–499, 1990.
30. A. L. Dulmage and N. S. Mendelsohn, The exponent of a primitive matrix, *Can. Math. Bull.*, **5**, 241–244, 1962.
31. A. L. Dulmage and N. S. Mendelsohn, Gaps in the exponent set of primitive matrices, *Ill. J. Math.*, **8**, 642–656, 1964.
32. A. L. Dulmage and N. S. Mendelsohn, Graphs and matrices, in *Graph Theory and Theoretical Physics*, pp. 167–229, Acad. Press, London, 1967.
33. G. Frobenius, Über Matrizen aus nicht negativen Elementen, *Berl. Ber.*, 456–477, 1912 [German].
34. J. C. Holladay and R. S. Varga, On powers of non-negative matrices, *Proc. Am. Math. Soc.*, **9**, 631, 1958.
35. Y. Huang and B. Liu, Generalized r -exponents of primitive digraphs, *Taiwan. J. Math.*, **15**, No. 5, 1999–2012, 2011.
36. M. Lewin and Y. Vitek, A system of gaps in the exponent set of primitive matrices, *Ill. J. Math.*, **25**, No. 1, 87–98, 1981.
37. B. Liu, Generalized exponents of Boolean matrices, *Linear Algebra Appl.*, **373**, 169–182, 2003.

-
38. **Z. Miao** and **K. Zhang**, The local exponent sets of primitive digraphs, *Linear Algebra Appl.*, **307**, 15–33, 2000.
39. **S. W. Neufeld**, A diameter bound on the exponent of a primitive directed graph, *Linear Algebra Appl.*, **245**, 27–47, 1996.
40. **P. Perkins**, A theorem on regular graphs, *Pac. J. Math.*, **2**, 1529–1533, 1961.
41. **V. Yu. Protasov** and **A. S. Voynov**, Sets of nonnegative matrices without positive products, *Linear Algebra Appl.*, **437**, No. 3, 749–765, 2012.
42. **J. L. Ramírez Alfonsín**, *The Diophantine Frobenius Problem*, Clarendon Press, Oxford, 2005 (Oxf. Lect. Ser. Math. Appl., Vol. 30).
43. **B. Schneier**, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, New York, 1996. Translated under the title *Prikladnaya kriptografiya: Protokoly, algoritmy, iskhodnye teksty na yazyke Si*, Triumph, Moscow, 2002.
44. **J. Shen** and **S. W. Neufeld**, Local exponents of primitive digraphs, *Linear Algebra Appl.*, **268**, 117–129, 1998.
45. **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), pp. 19–39, Springer, Heidelberg, 2010 (Lect. Notes Comput. Sci., Vol. 6147).
46. **A. S. Voynov**, Shortest positive products of nonnegative matrices, *Linear Algebra Appl.*, **439**, No. 6, 1627–1634, 2013.
47. **H. Wielandt**, Unzerlegbare, nicht negative Matrizen, *Math. Z.*, **52**, 642–648, 1950 [German].

Vladimir M. Fomichev
Yana E. Avezova
Alisa M. Koreneva
Sergey N. Kyazhin

Received
16 October 2017
Revised
23 March 2018