

ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 33 № 2 2026

Новосибирск
Издательство Института математики

ЛОКАЛЬНАЯ НЕЛИНЕЙНОСТЬ СТЕПЕНЕЙ ПРЕОБРАЗОВАНИЯ

В. М. Фомичёв^{1, 2}

¹ Российский университет дружбы народов им. Патриса Лумумбы,
ул. Миклухо-Маклая, 6, 117198 Москва, Россия

² Институт проблем информатики ФИЦ «Информатика и управление»,
ул. Вавилова, 44, корп. 2, 119333 Москва, Россия
E-mail: fomichev.2016@yandex.ru

Аннотация. В соответствии с шенноновской концепцией о перемешивающих свойствах преобразований информации развивается ранее предложенный автором матрично-графовый подход к оценке характеристик нелинейности произведения преобразований векторного пространства. Подход позволяет оценить локальные нелинейные свойства произведения преобразований с помощью троичных матриц и помеченных орграфов, однозначно соответствующих преобразованиям. Для троичных матриц и для помеченных орграфов с использованием длин путей определены свойство локальной 2-примитивности, оценки локальных 2-экспонентов и, в частности, точные значения. Получены критерии локальной 2-примитивности. Результаты для матриц и помеченных орграфов применяются для оценки характеристик произведения преобразований векторного пространства. Рассмотрены примеры. Библиогр. 18.

Ключевые слова: троичная матрица, локально примитивная матрица, 2-примитивная матрица, 2-экспонент матрицы, 2-примитивный помеченный орграф.

Введение

Преобразование данных в симметричных криптографических системах защиты информации часто строится на основе произведения функций векторных пространств, имеющих приемлемую сложность программной и/или аппаратной реализации. Задачи криптографического анализа произведения функций, как правило, сложны в силу аналитической сложности связей между элементами входных и выходных данных. Вместе с тем показал продуктивность матрично-графовый подход (МГП) к оценке некоторых характеристик произведения функций, в частности,

к оценке множеств существенных и нелинейных переменных координатных функций степеней преобразований векторных пространств [1–3].

МГП основывается на комбинаторных свойствах мультипликативных полугрупп неотрицательных матриц и ориентированных графов. Первая постановка задачи в этой области относится к 1912 г. (Фробениус [4]): была поставлена задача распознавания наличия положительной матрицы в циклической полугруппе, порождённой заданной неотрицательной матрицей. При наличии порождающая матрица была названа примитивной, а её наименьшая степень, у которой все элементы положительные, спустя полвека названа экспонентом примитивной матрицы [5]. Задача Фробениуса к середине XX — началу XXI вв. инициировала несколько связанных с МГП основополагающих результатов в области неотрицательных матриц и графов [6–18]. Таковыми являются критерии конечности экспонентов и их количественные оценки. Ряд зарубежных результатов касались локальных характеристик, однако, лишь для класса примитивных матриц и графов.

При дальнейшем развитии теоретических основ МГП обнаружилась связь с подходом Шеннона к перемешивающим свойствам криптографических преобразований, что существенно расширило область приложений МГП в криптографии и стимулировало обобщение понятий примитивности и распространение экспонента на несильно связные орграфы. Продвижение в изучении экспонентов матриц и графов, в частности, раскрывающие детализацию подхода Шеннона к перемешивающим свойствам криптографических преобразований, достигнуто в основном после 2014 г. Результаты представлены в статьях и отражены в учебной литературе.

Для множества существенных и нелинейных переменных произведения преобразований основные результаты даны в [1, 2]. Исследование локальных характеристик матриц и орграфов, связанных с произведением преобразований, представлено в [3] и относится к множеству существенных переменных. Данная работа дополняет понятийную базу оценки локальных характеристик нелинейности преобразований векторных пространств с помощью оценки локальных свойств троичных матриц и помеченных орграфов. Получены новые конструктивные критерии локальной примитивности и 2-примитивности орграфов.

Разработанный подход в части локальных характеристик нелинейности произведения преобразований применим вкупе с вычислительными экспериментами для анализа криптографических систем, построенных по итеративному принципу, например, симметричных блочных шифров и алгоритмов контроля целостности данных.

1. Основы матрично-графового подхода

Положительное свойство систем защиты, построенных по итеративному принципу, — существенная нелинейная зависимость от большого числа булевых входных переменных всех координатных функций произведения криптографических преобразований двоичных векторных пространств. Для произведения преобразований это свойство интерпретируется с помощью МГП как положительность большого числа элементов соответствующих перемешивающих матриц или наличие определённых путей в соответствующих перемешивающих орграфах. Применение МГП к степеням преобразований помогает в решении следующих задач:

- при определении существенных переменных — в распознавании примитивности или локальной примитивности двоичных матриц и ориентированных графов, а также вычислении их экспонентов или локальных экспонентов;
- при определении нелинейных переменных — в распознавании 2-примитивности или локальной 2-примитивности троичных матриц и помеченных орграфов, а также вычислении их 2-экспонентов или локальных 2-экспонентов.

Данные ниже определения дополняют введённую ранее терминологию [1–3] для изучения локально примитивных двоичных матриц и орграфов и локально 2-примитивных троичных матриц и помеченных орграфов.

2. Локальная 2-примитивность троичных матриц

В статье используются следующие обозначения:

- $\mathbb{N}$ — множество натуральных чисел;
- $n, m, d \in \mathbb{N}$; $L \subseteq \mathbb{N}$;
- $L^{[n]} = \{l \in L \mid l \leq n\}$;
- $L^{[m]} = \{l \in L \mid m < l\}$;
- $L^{(m,n)} = L^{[m]} \cap L^{[n]} = \{l \in L \mid m < l \leq n\}$;
- $n + L = \{n + l \mid l \in L\}$;
- $nL = \{nl \mid l \in L\}$;
- $\mathbb{Z}$ — множество целых чисел;
- $\mathbb{Z}_m$ — кольцо вычетов по модулю m ;
- $m \mid n$ — число m делит n без остатка;
- $n \equiv_d m$ — число n сравнимо с m по модулю d ;
- $\{L \equiv_d\} = \{l \bmod d \mid l \in L\}$ — множество целых неотрицательных вычетов;
- $G = \{0, 1, 2\}$ — коммутативная полугруппа по умножению, при этом $0g = 0$ для всех $g \in G$ и $gh = \max\{g, h\}$ для ненулевых $g, h \in G$;
- $M_n^{[G]}$ — множество квадратных троичных матриц порядка n над G .

Отметим следующие свойства множества $M_n^{[G]}$:

1) $M_n^{[G]}$ — мультипликативный моноид: если $A, M \in M_n^{[G]}$, $A = (a_{ij})$, $M = (m_{ij})$, то $(AM)_{ij} = \max_{1 \leq p \leq n} a_{ip} m_{pj}$, при этом умножение выполняется в G ;

2) моноид $M_n^{[G]}$ частично упорядочен: $A \leq M$ тогда и только тогда, когда $a_{ij} \leq m_{ij}$, $1 \leq i, j \leq n$.

Приведём известное определение $2_{(i,j)}$ -примитивной матрицы. Пусть $M \in M_n^{[G]}$ и $M^t = (m_{ij}^{(t)})$, $t \geq 1$. Матрицу M называют $2_{(i,j)}$ -примитивной, $1 \leq i, j \leq n$, если существует $\gamma \in \mathbb{N}$ такое, что $m_{ij}^{(t)} = 2$ при любом $t \geq \gamma$; наименьшее такое γ называется $2_{(i,j)}$ -экспонентом матрицы M и обозначается через $\gamma_{2(i,j)}$. Если матрица M не $2_{(i,j)}$ -примитивная, то полагаем $\gamma_{2(i,j)} = \infty$.

Матрица M 2-примитивная, если она $2_{(i,j)}$ -примитивная для любых $i, j \in \overline{1, n}$, что символически записываем в виде $M^\gamma = (2)$. Для 2-экспонента матрицы M , обозначаемого через γ_2 , выполнено свойство

$$\gamma_2 = \exp^{[2]} M = \max_{1 \leq i, j \leq n} \gamma_{2(i,j)}.$$

Обобщим 2-примитивность, требуя $2_{(i,j)}$ -примитивность лишь для собственного подмножества всех пар (i, j) , $1 \leq i, j \leq n$. Пусть $B = (b_{ij})$ — ненулевая двоичная матрица (маска) порядка n , $B * M = (b_{ij} m_{ij})$, умножение $b_{ij} m_{ij}$ выполнено в G , т. е.

$$b_{ij} m_{ij} = \begin{cases} 0, & \text{если } b_{ij} = 0, \\ m_{ij}, & \text{если } b_{ij} = 1. \end{cases}$$

Матрицу $M \in M_n^{[G]}$ назовём

а) 2_B -полной, если из равенства $b_{ij} = 1$ следует $m_{ij} = 2$, $1 \leq i, j \leq n$, символически запишем это свойство так: $M = (2_B)$;

б) 2_B -примитивной, если из равенства $b_{ij} = 1$ следует, что M $2_{(i,j)}$ -примитивная; 2_B -экспонент матрицы M , обозначаемый через $\exp^{[2_B]} M$ (или кратко через γ_{2_B}), равен

$$\gamma_{2_B} = \max_{(i,j): b_{ij}=1} \gamma_{2(i,j)}.$$

Из определений вытекают следующие свойства 2_B -примитивной матрицы $M \in M_n^{[G]}$:

1) M 2_B -примитивная тогда и только тогда, когда она $2_{(i,j)}$ -примитивная при всех (i, j) таких, что $b_{ij} = 1$;

2) если M 2-примитивная, то она 2_B -примитивная при любой маске B и $\exp^{[2]} M \geq \exp^{[2_B]} M$;

3) *антимонотонность по матрицам*: если $A \leq M$ и матрица A 2_B -примитивная, то M тоже 2_B -примитивная и $\exp^{[2_B]} A \geq \exp^{[2_B]} M$;

4) *монотонность по маскам*: если $\emptyset \neq E \subseteq B$, то 2_B -примитивная матрица M будет 2_E -примитивной и $\exp^{[2_E]} M \leq \exp^{[2_B]} M$;

5) *ненаследственность*: из равенства $M^t = (2_B)$, $t \in \mathbb{N}$, вообще говоря, не следует, что $M^{t+1} = (2_B)$ (при этом заметим, что равенство $M^t = (2)$ влечёт $M^{t+1} = (2)$ для любого $t \in \mathbb{N}$).

В связи со свойством 5 дадим достаточные условия 2_B -полноты всех матриц $M^t, M^{t+1}, \dots$. Обозначим i -ю строку и j -й столбец матрицы A через $A_{i\rightarrow}$ и $A_{j\downarrow}$ соответственно, а их скалярное произведение — через $(A_{i\rightarrow}, A_{j\downarrow})$.

Теорема 1. Если для любых $1 \leq i, j \leq n$ при $b_{ij} = 1$ имеет место $\max\{(m_{i\rightarrow}, b_{j\downarrow}), (b_{i\rightarrow}, m_{j\downarrow})\} > 0$, то из равенства $M^t = (2_B)$, $t \geq 1$, следует, что $M^{t+1} = (2_B)$ и $\gamma_{2_B} = \min\{t \mid M^t = (2_B)\}$.

ДОКАЗАТЕЛЬСТВО. Из равенств $M^{t+1} = MM^t = M^tM$ получаем

$$m_{ij}^{(t+1)} = \max_{1 \leq r \leq n} m_{ir} m_{rj}^{(t)}, \quad m_{ij}^{(t+1)} = \max_{1 \leq s \leq n} m_{is}^{(t)} m_{sj}.$$

Если $(m_{i\rightarrow}, b_{j\downarrow}) > 0$, то $m_{ir} = b_{r,j} > 0$ при некотором $r \in \overline{1, n}$, значит, $m_{ir} m_{rj}^{(t)} = 2m_{ir} = 2$ в силу 2_B -полноты матрицы M^t .

Если $(b_{i\rightarrow}, m_{j\downarrow}) > 0$, то $b_{is} = m_{sj} > 0$ при некотором $s \in \overline{1, n}$, значит, $m_{is}^{(t)} m_{sj} = 2m_{sj} = 2$ в силу 2_B -полноты матрицы M^t .

По условию при $b_{ij} = 1$ выполняется хотя бы одно из неравенств $(m_{i\rightarrow}, b_{j\downarrow}) > 0$, $(b_{i\rightarrow}, m_{j\downarrow}) > 0$. Значит, в обоих случаях $m_{ij}^{(t+1)} = 2$, т. е. $M^{t+1} = (2_B)$. Теорема 1 доказана.

3. Свойства наборов натуральных чисел

Пусть $L = \{l_1, \dots, l_m\} \subset \mathbb{N}$ — бесповторная выборка. Обозначим через $\langle L \rangle$ порождённую множеством L аддитивную полугруппу, состоящую из множества всех линейных комбинаций (л. к.) чисел множества L ; здесь и далее коэффициенты л. к. суть неотрицательные целые; $\langle \emptyset \rangle = \emptyset$.

При $\text{НОД } L = 1$ числом Фробениуса $F(L)$ называют наибольшее целое число $l \notin \langle L \rangle$; $F(1) = -1$; если $l > F(L)$, то $l \in \langle L \rangle$.

Известна формула $F(L)$ для двух аргументов: $F(l_1, l_2) = l_1 l_2 - l_1 - l_2$. При $m > 2$ общей полиномиальной формулы для $F(L)$ не существует [2].

Если $\text{НОД } L = d_L \geq 1$, то $\frac{L}{d_L} = \{\frac{l_1}{d_L}, \dots, \frac{l_m}{d_L}\}$ и $\text{НОД } \frac{L}{d_L} = 1$. Обобщая число Фробениуса, положим $\Phi(L) = d_L F(\frac{L}{d_L})$, т. е. $\Phi(L)$ — наибольшее кратное d_L целое, не принадлежащее $\langle L \rangle$.

Из определений вытекают следующие свойства:

1) $\Phi(L) = F(L)$ при $d_L = 1$;

- 2) если $L \neq \emptyset$, то число $\Phi(L)$ существует;
- 3) $\Phi(l) = -l$ при $l \in \mathbb{N}$, а при $m = 2$ верно $\Phi(l_1, l_2) = \frac{l_1 l_2}{d_L} - l_1 - l_2$;
- 4) если $l > \Phi(L)$ и l кратно d_L , то $l \in \langle L \rangle$;
- 5) если $L \supseteq L'$, то $\Phi(L) \leq \Phi(L')$.

Элемент $l \in \langle L \cup H \rangle$, где $\emptyset \neq H = \{h_1, \dots, h_r\} \subset \mathbb{N}$, $r > 0$, представляется (вообще говоря, неоднозначно) как л. к. вида

$$l = \alpha_1 l_1 + \dots + \alpha_m l_m + \beta_1 h_1 + \dots + \beta_r h_r,$$

где коэффициенты $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_r$ целые неотрицательные. Набор коэффициентов $(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_r)$ назовём *представлением числа l в базе $\{L, H\}$* . Множество представлений числа l в базе $\{L, H\}$ обозначим через $\Pi_{\{L, H\}}(l)$.

Назовём *H -весом числа l в базе $\{L, H\}$* (обозначим $p_H(l)$) наибольшее число ненулевых коэффициентов в наборе $(\beta_1, \dots, \beta_r)$ среди всех представлений из $\Pi_{\{L, H\}}(l)$, откуда $0 \leq p_H(l) \leq r$ для любого $l \in \langle L \cup H \rangle$.

Пусть $\langle L \cup [H]^+ \rangle = \{l \in \langle L \cup H \rangle \mid p_H(l) > 0\}$. Имеет место покрытие

$$\langle L \cup [H]^+ \rangle = \bigcup_{s=1}^r (h_s + \langle L \cup H \rangle). \quad (1)$$

Лемма 1. $\langle L \cup [H]^+ \rangle \supseteq (\min_{1 \leq s \leq r} h_s + \Phi(L \cup H) + d_{L \cup H} \mathbb{N})$.

ДОКАЗАТЕЛЬСТВО следует из (1) и свойства полугруппы $\langle L \cup H \rangle$, так как все числа множества $h_s + \Phi(L \cup H) + d_{L \cup H} \mathbb{N}$ кратны $d_{L \cup H}$, $1 \leq s \leq r$. Лемма 1 доказана.

Пример 1. Пусть $L = \{15, 45\}$, $H = \{9, 21, 27\}$. Тогда $d_{L \cup H} = 3$, $\Phi(L \cup H) = 12$ и $\langle L \cup H \rangle = \langle 9, 15, 21, 27, 45 \rangle = \{0, 9, 15, 21\} \cup (21 + 3\mathbb{N}) = \{0, 9\} \cup (12 + 3\mathbb{N})$.

Имеется единственное представление числа 24: $\Pi_{\{L, H\}}(24) = \{9 + 15\}$, $p_H(24) = 1$. Имеются 5 представлений числа 54:

$\Pi_{\{L, H\}}(54) = \{6 \cdot 9, 3 \cdot 9 + 27, 2 \cdot 9 + 15 + 21, 9 + 3 \cdot 15, 2 \cdot 27\}$, $p_H(54) = 2$. В соответствии с (1) имеем покрытие

$$\langle L \cup [H]^+ \rangle = (9 + \langle L \cup H \rangle) \cup (21 + \langle L \cup H \rangle) \cup (27 + \langle L \cup H \rangle).$$

Пусть $d, l \in \mathbb{N}$ и $\varphi \in \{-d\} \cup d\mathbb{N}$, т. е. φ кратно d . Бесповторную выборку $S(\varphi, d, l) = (l + B) \cup (l + \varphi + d\mathbb{N}) \subseteq \mathbb{N}$ назовём (φ, d, l) -выборкой, если $B \subseteq \{d, \dots, \varphi - d\} \subseteq d\mathbb{N}$ при $\varphi > d$ и $B = \emptyset$ при $\varphi \in \{-d, d\}$. Заметим, что $l + \varphi \notin S(\varphi, d, l)$ при $\varphi > d$ и $b \equiv_d l$ для любого $b \in S(\varphi, d, l)$.

Множество выборок $\{S(\varphi_i, d_i, l_i)\}_{i=1}^k$ назовём *полным*, если имеет место включение $\bigcup_{i=1}^k S(\varphi_i, d_i, l_i) \supseteq \mathbb{N}^{[q]}$ при некотором $q \in \mathbb{N}$. Например, полными будут выборка $S(\varphi, 1, l)$ при любых φ и l (тогда $q = l + \varphi$),

а также множество выборок $\{S(\varphi, d, l)\}_{l=1}^d$ при $\varphi > 0$ и при любом d (тогда $q = d + \varphi$).

Положим $S = \bigcup_{i=1}^k S(\varphi_i, d_i, l_i)$, $h = \max_{1 \leq i \leq k} \{\varphi_i + l_i\}$.

Теорема 2. Положим $D = \text{НОК}\{d_1, \dots, d_k\}$. Множество выборок $\{S(\varphi_i, d_i, l_i)\}_{i=1}^k$ полное тогда и только тогда, когда полна система вычетов $\{S^{(h, h+D]} \equiv_D\}$, при этом

$$\max \mathbb{N} \setminus S = \max \bigcap_{i=1}^k (\mathbb{N}^{\lceil \varphi_i + l_i \rceil} \setminus S(\varphi_i, d_i, l_i)^{\lceil \varphi_i + l_i \rceil}).$$

Вычисление $\max \mathbb{N} \setminus S$ по множеству выборок $\{S(\varphi_i, d_i, l_i)\}_{i=1}^k$ требует менее $k \lceil \log_2 k \rceil + \lceil \log_2 h \rceil \sum_{i=1}^k \varphi_i$ сравнений целых неотрицательных чисел.

ДОКАЗАТЕЛЬСТВО. В силу того, что $d_i \mid D$, $i = 1, \dots, k$, выполнено $S(\varphi_i, d_i, l_i) \supseteq l_i + \varphi_i + D\mathbb{N}$. Следовательно, $S \supseteq h + D\mathbb{N}$. Отсюда равны множества вычетов $\{S^{(h+(s-1)D, h+sD]} \equiv_D\} = \{S^{(h, h+D]} \equiv_D\}$, $s \in \mathbb{N}$. Значит, полнота данного множества выборок равносильна полноте системы вычетов $\{S^{(h, h+D]} \equiv_D\}$.

В силу свойств операций объединения и пересечения множеств имеем

$$\mathbb{N} \setminus S = \mathbb{N} \setminus \bigcup_{i=1}^k S(\varphi_i, d_i, l_i) = \bigcap_{i=1}^k (\mathbb{N} \setminus S(\varphi_i, d_i, l_i)).$$

Заметим, что $\mathbb{N} \setminus S(\varphi_i, d_i, l_i) = \mathbb{N}^{\lceil \varphi_i + l_i \rceil} \setminus S(\varphi_i, d_i, l_i)^{\lceil \varphi_i + l_i \rceil}$, так как если целое $l > \varphi_i + l_i$ и $d_i \mid l - l_i$, то $l \in S(\varphi_i, d_i, l_i)$ по определению выборки. В силу полноты множества вычетов $\{S^{(h, h+D]} \equiv_D\}$ для любого целого $l > h$ в множестве $\{S(\varphi_i, d_i, l_i)\}_{i=1}^k$ найдётся содержащая число l выборка.

Множество $S^{(h, h+D]}$ состоит из чисел l , где $h < l \leq h + D$, содержащихся хотя бы в одной выборке множества $\{S(\varphi_i, d_i, l_i)\}_{i=1}^k$. Следовательно,

$$S^{(h, h+D]} = \bigcup_{i=1}^k \{\varphi_i + l_i + td_i \in (h, h + D] \mid t \in \mathbb{N}\}.$$

Оценим сложность вычисления числа $\gamma = \max \bigcap_{i=1}^k (\mathbb{N} \setminus S(\varphi_i, d_i, l_i))$, упорядочив выборки по правилу $\varphi_t + l_t \geq \varphi_{t+1} + l_{t+1}$, $t = 1, \dots, k - 1$.

Пусть $L_0 = \mathbb{N}^{\lceil \varphi_1 + l_1 \rceil}$ — упорядоченный массив чисел.

Найдём γ за k шагов. На шаге i все числа $l \in S(\varphi_i, d_i, l_i)^{\lceil \varphi_i + l_i \rceil}$ удаляем из массива L_{i-1} . Полагаем $L_i = L_{i-1} \setminus S(\varphi_i, d_i, l_i)^{\lceil \varphi_i + l_i \rceil}$, $i = 1, \dots, k$. Наибольшее число массива L_k равно γ .

Для оценки вычислительной сложности алгоритма заметим, что

- $\varphi_1 + l_1 = h$;
- $|S(\varphi_i, d_i, l_i)^{\lceil \varphi_i + l_i \rceil}| < \varphi_i$ в силу определения (φ, d, l) -выборки;
- так как $|L_i| < h$, $i = 1, \dots, k$, для поиска любого числа в упорядоченном массиве L_i требуется менее $\lceil \log_2 h \rceil$ сравнений чисел.

Предварительное упорядочение выборок требует не более $k \lceil \log_2 k \rceil$ сравнений. Тогда сложность алгоритма меньше $k \lceil \log_2 k \rceil + \lceil \log_2 h \rceil \sum_{i=1}^k \varphi_i$.

Теорема 2 доказана.

4. Усложнение простых путей орграфа

Пусть Γ_n — класс орграфов с множеством вершин $\overline{1, n}$.

Введём следующие обозначения для орграфа $\Gamma \in \Gamma_n$:

- $P(i, j)$ — множество всех простых путей из i в j , $1 \leq i, j \leq n$;
- l_w (или l_C) — длина пути w (или контура C), равная числу дуг, составляющих путь (или контур);
- $L(W) = \{l_w \mid w \in W\}$, где W — множество путей;
- $w \parallel w'$ — конкатенация (присоединение) путей w и w' , где конечная вершина пути w совпадает с начальной вершиной пути w' .

Контур, проходящий через вершину пути w , назовём *w-инцидентным*. Контур C назовём *w-достижимым*, если он *w-инцидентный* или существует путь из w в некоторую вершину контура C . Путь w назовём *достижимым* из контура C , если этот контур *w-инцидентный* или существует путь из C в некоторую вершину пути w . При выполнении обоих условий путь и контур называются *взаимно достижимыми*.

В сильно связном орграфе любые путь и контур взаимно достижимы.

Пусть $P(i, j) \neq \emptyset$. Введём следующие обозначения:

- $\tilde{\Gamma}_n^{(i, j)}$ — класс орграфов из Γ_n , в которых для любого пути $w \in P(i, j)$ каждый *w-достижимый* контур *w-инцидентный*;
- $\widehat{C}_w$ — множество всех *w-инцидентных* контуров, $w \in P(i, j)$;
- $C^{[k]}(v)$ — пройденный k -кратно из начальной вершины v контур C , $k \geq 0$;

Индексом (*$\widehat{C}_w$ -индексом*) пути w назовём число $d_w = \text{НОД}(L(\widehat{C}_w))$, $d_w = 0$, если $\widehat{C}_w = \emptyset$. Подмножество $\widehat{C}_w'$ множества $\widehat{C}_w$ назовём *d_w -минимальным*, если $d(\widehat{C}_w') = d_w$ и из включения $\widehat{C}_w'' \subset \widehat{C}_w'$ следует, что $d(\widehat{C}_w'') > d_w$.

Без ограничения общности далее считаем, что множество $\widehat{C}_w$ d_w -минимально и $\widehat{C}_w = \{C_1, \dots, C_m\}$, где $d_w \geq 1$ и $m \geq 1$.

На множестве путей орграфа Γ определим бинарное отношение «усложнения», которое обозначим через $\lesssim$. Если $w = (v_0, \dots, v_t)$ — некоторый

путь и v_r — вершина w -инцидентного контура C , $0 \leq r \leq t$, то $C^{[k]}(v_r)$ -усложнением пути w назовём его усложнение с помощью k -кратного обхода контура C , $k \geq 0$:

$$w(C^{[k]}(v_r)) = \begin{cases} C^{[k]}(v_0) \parallel w, & \text{если } r = 0, \\ (v_0, \dots, v_r) \parallel C^{[k]}(v_r) \parallel (v_r, \dots, v_t), & \text{если } 0 < r < t, \\ w \parallel C^{[k]}(v_t), & \text{если } r = t. \end{cases}$$

Путь $C^{[0]}(v_r)$ пустой. В соответствии с определением конкатенации путей

$$l_{w \parallel w'} = l_w + l_{w'}, \quad l_{w(C^{[k]}(v_r))} = l_w + kl_C.$$

Усложнение пути w с помощью контуров из $\widehat{C}_w$ назовём $\widehat{C}_w$ -усложнением. Если контур C_s обходится k_s -кратно, $s = 1, \dots, m$, то $C^{[k]}(v_r)$ -усложнение пути w имеет длину $l_w + \sum_{s=1}^m k_s l_s$. Множество вариантов кратности обхода контуров счётное, и w имеет счётное множество усложнений, если $\widehat{C}_w \neq \emptyset$. Если $\widehat{C}_w$ -усложнение пути w усложнить некоторым контуром, не инцидентным пути w , то получим усложнение, отличное от $\widehat{C}_w$ -усложнений. Такие усложнения пути w назовём w -свободными.

Введём следующие обозначения:

- $P^{(0)}$ — класс простых путей $w \in P(i, j)$ индекса $d_w = 0$;
- $P^{(+)}$ — класс простых путей $w \in P(i, j)$ индекса $d_w > 0$;
- U_w — класс всех усложнений простого пути w положительного индекса, как w -свободных, так и $\widehat{C}_w$ -усложнений;
- $\widehat{U}_w$ — класс всех $\widehat{C}_w$ -усложнений простого пути w положительного индекса; при $\widehat{C}_w = \emptyset$ имеем $\widehat{U}_w = \{w\}$, $L(\widehat{U}_w) = \{l_w\}$;
- $\widehat{U} = \bigcup_{w \in P^{(+)}} \widehat{U}_w$;
- $U = \bigcup_{w \in P^{(+)}} U_w$;
- $\Phi_w = \Phi(L(\widehat{C}_w))$;
- $\Phi^{(i,j)} = \max_{w \in P^{(+)}} \Phi_w$;
- $h^{(i,j)} = \max_{w \in P^{(+)}} (l_w + \Phi_w)$;
- $D = \text{НОК}\{d_w \mid w \in P^{(+)}\}$.

Теорема 3 (о длинах усложнений пути). В орграфе $\Gamma \in \Gamma_n$ множество $L(\widehat{U}_w)$ длин всех $\widehat{C}_w$ -усложнений пути $w \in P^{(+)}$ есть (Φ_w, d_w, l_w) -выборка:

$$L(\widehat{U}_w) = l_w + \langle l_1, \dots, l_m \rangle \supseteq l_w + \Phi_w + d_w \mathbb{N}.$$

ДОКАЗАТЕЛЬСТВО. Если при $\widehat{C}_w$ -усложнении простого пути w контур C_s обходится k_s -кратно, $s = 1, \dots, m$, то длина усложнения равна

$l_w + k_1 l_1 + \dots + k_m l_m$. Тогда $L(\widehat{U}_w) = l_w + \langle l_1, \dots, l_m \rangle$, так как допустима любая кратность обхода контуров из $\widehat{C}_w$.

По свойству числа Φ полугруппа $\langle l_1, \dots, l_m \rangle$ содержит все числа, кратные d_w и превышающие Φ_w . Значит, $L(\widehat{U}_w) \supseteq l_w + \Phi_w + d_w \mathbb{N}$. Теорема 3 доказана.

Следствие 1. Для любого $l \in L(\widehat{U}_w)$ имеет место сравнение $l \equiv_{d_w} l_w$.

ДОКАЗАТЕЛЬСТВО. Число Φ_w и любое число из $\langle l_1, \dots, l_m \rangle$ кратно d_w , так как $d_w \mid l_s$, $s = 1, \dots, m$. Тогда $l \equiv_{d_w} l_w$ в силу теоремы 3. Следствие 1 доказано.

5. О локальной примитивности орграфа

В силу имеющейся биекции $M_n \leftrightarrow \Gamma_n$, где M_n — множество двоичных матриц порядка n , локальные примитивности матриц и орграфов равносильны. Используем более удобную графовую модель.

С помощью множества длин путей получим для орграфа $\Gamma \in \Gamma_n$ критерий (i, j) -примитивности и оценку (i, j) -экспонента. Покажем, что для орграфов $\Gamma \in \widetilde{\Gamma}_n^{(i,j)}$ данная оценка совпадает с точным значением.

Напомним, что Γ называется (i, j) -примитивным, $1 \leq i, j \leq n$, если найдётся число $\gamma \in \mathbb{N}$ такое, что для любого $t \geq \gamma$ в Γ имеется путь длины t из i в j (или дуга (i, j) в Γ^t); наименьшее такое γ называют (i, j) -экспонентом орграфа Γ (обозначается $\exp^{(i,j)} \Gamma$ или кратко $\gamma_{(i,j)}$).

По определению в (i, j) -примитивном орграфе имеются простой путь $w \in P^{(+)}$ и некоторый w -инцидентный контур. Иначе все простые пути имеют индекс 0 и число их усложнений конечно в силу тривиальности усложнений, что противоречит (i, j) -примитивности орграфа.

Теорема 4 (критерий (i, j) -примитивности орграфа). Граф $\Gamma \in \Gamma_n$ (i, j) -примитивный тогда и только тогда, когда множество $\mathbb{N} \setminus L(U)$ конечно и $\gamma_{(i,j)} \leq 1 + \varepsilon_{(i,j)}$, где

$$\varepsilon_{(i,j)} = \max_{w \in P^{(+)}} \bigcap (\mathbb{N}^{\lceil l_w + \Phi_w \rceil} \setminus L(\widehat{U}_w)^{\lceil l_w + \Phi_w \rceil}) \setminus L(P^{(0)}).$$

Если $\Gamma \in \widetilde{\Gamma}_n^{(i,j)}$, то Γ (i, j) -примитивный тогда и только тогда, когда полна система вычетов $\{L(\widehat{U})^{(h^{(i,j)}, h^{(i,j)} + D)} \equiv_D\}$ и $\gamma_{(i,j)} = 1 + \varepsilon_{(i,j)}$.

Вычисление $\varepsilon_{(i,j)}$ требует менее

$$|P^{(+)}| \lceil \log_2 |P^{(+)}| \rceil + \left(\sum_{w \in P^{(+)}} \Phi_w + |P^{(0)}| \right) \lceil \log_2 h^{(i,j)} \rceil$$

сравнений целых чисел, не больших $\max\{n, \Phi^{(i,j)}\}$.

ДОКАЗАТЕЛЬСТВО. В соответствии с определением оргграф $\Gamma \in \Gamma_n$ (i, j) -примитивный с (i, j) -экспонентом $\gamma_{(i,j)}$ тогда и только тогда, когда $L(U) \supseteq \mathbb{N}^{\lfloor \gamma_{(i,j)} - 1 \rfloor}$ и $(\gamma_{(i,j)} - 1) \notin L(U)$. Значит, $L(U)$ содержит все числа, не меньшие $\gamma_{(i,j)}$, и $\gamma_{(i,j)} = 1 + \max \mathbb{N} \setminus L(U)$.

Так как $\widehat{U}_w \subseteq U_w$, $w \in P^{(+)}$, то $L(\widehat{U}_w) \subseteq L(U_w)$, отсюда $\Phi(L(\widehat{U}_w)) \geq \Phi(L(U_w))$ в силу свойства 5 чисел Φ . Следовательно, $\max_{w \in P^{(+)}} \Phi(L(\widehat{U}_w)) \geq$

$\max_{w \in P^{(+)}} \Phi(L(U_w))$, значит, $\max \mathbb{N} \setminus L(\widehat{U}) \geq \max \mathbb{N} \setminus L(U) = \gamma_{(i,j)} - 1$.

По теореме 3 множество $L(\widehat{U}_w)$ представляет собой (Φ_w, d_w, l_w) -выборку. Объединение этих выборок для всех путей $w \in P^{(+)}$ есть $L(\widehat{U})$. По теореме 2 $L(\widehat{U}) = \bigcup_{w \in P^{(+)}} L(\widehat{U}_w)$ полное тогда и только тогда, когда

полна система вычетов $\{L(\widehat{U})^{(h^{(i,j)}, h^{(i,j)} + D)} \equiv_D\}$.

В соответствии с теоремой 2 и с учётом путей нулевого индекса

$$\max \mathbb{N} \setminus L(\widehat{U}) = \max_{w \in P^{(+)}} \bigcap (\mathbb{N}^{\lceil l_w + \Phi_w \rceil} \setminus L(\widehat{U}_w)^{\lceil l_w + \Phi_w \rceil}) \setminus L(P^{(0)}) = \varepsilon_{(i,j)}.$$

Если $\Gamma \in \widetilde{\Gamma}_n^{(i,j)}$, то $L(U) = L(\widehat{U})$ и $1 + \varepsilon_{(i,j)}$ есть точное значение.

Количество сравнений целых чисел для вычисления $\varepsilon_{(i,j)}$ ограничено упорядочиванием множества $P^{(+)}$ и поиском чисел из $\mathbb{N} \setminus L(\widehat{U})$ в упорядоченном массиве мощности, меньшей $\Phi^{(i,j)}$. Сравнимые числа не превышают n (количества разных длин простых путей), и числа усложнений длины не выше $l_w + \Phi_w$, которое не больше Φ_w для всех путей $w \in P^{(+)}$. Теорема 4 доказана.

Замечание 1. Множество $\{L(\widehat{U})^{(h^{(i,j)}, h^{(i,j)} + D)} \equiv_D\}$ состоит из длин l всех $\widehat{C}_w$ -усложнений путей $w \in P^{(+)}$, где $h^{(i,j)} < l \leq h^{(i,j)} + D$. Следовательно,

$$\{L(\widehat{U})^{(h^{(i,j)}, h^{(i,j)} + D)} \equiv_D\} = \bigcup_{w \in P^{(+)}} \{l_w + \Phi_w + sd_w \in (h^{(i,j)}, h^{(i,j)} + D) \mid s \in \mathbb{N}\}.$$

6. Об усложнениях путей помеченного оргграфа

Введём следующие обозначения:

- $\Gamma_{n,G}$ — множество оргграфов с множествами вершин $\overline{1, n}$ и меток дуг G ;
- $\widetilde{\Gamma}_{n,G}^{(i,j)}$ — множество оргграфов из $\widetilde{\Gamma}_n^{(i,j)}$ с множеством меток дуг G ;
- $\theta: M_n^{[G]} \leftrightarrow \Gamma_n^{[G]}$ — биекция, при которой матрице $M = (m_{ij})$ порядка n над G соответствует оргграф $\Gamma = \theta(M)$ с матрицей меток M .

В $\Gamma_{n,G}$ дуга (i, j) с меткой m_{ij} задана тройкой (i, m_{ij}, j) . Пути $w = (y_0, \dots, y_t)$ длины t соответствует слово $(m_1, \dots, m_t)$, где m_s — метка дуги (y_{s-1}, y_s) , $s = 1, \dots, t$. Произведение $m = m_1 \dots m_t$ (умножение в G) назовём *меткой* пути w :

$$m = \begin{cases} \max_{1 \leq s \leq t} m_s, & \text{если } m_s > 0 \text{ при } s \in \{1, \dots, t\}, \\ 0, & \text{если } m_s = 0 \text{ для некоторого } s \in \{1, \dots, t\}. \end{cases}$$

Путь (контур) с меткой $g \in \{1, 2\}$ назовём *g-путём* (*g-контуром*).

Если в орграфе Γ имеются пути $w_1, \dots, w_r$ из i в j длины t с метками $m_1, \dots, m_r$ соответственно, то метка дуги (i, j) в орграфе Γ^t есть произведение $m_1 \dots m_r$.

Пусть оргграф $\Gamma' \in \Gamma_{n,G}$ имеет матрицу меток (μ_{ij}) . Обозначим через V_{ij} множество вершин v таких, что (i, v) — дуга в Γ и (v, j) — дуга в Γ' . Тогда в орграфе $\Gamma\Gamma'$ при $V_{ij} = \emptyset$ метка дуги (i, j) есть 0, а при $V_{ij} \neq \emptyset$ имеется дуга (i, b_{ij}, j) с меткой $b_{ij} = \max_{v \in V_{ij}} m_{iv} \mu_{vj}$. Отсюда следует

Теорема 5 (о метках дуг). Пусть оргграф $\Gamma \in \Gamma_{n,G}$ имеет матрицу меток $M = (m_{ij})$. Тогда метка $m_{ij}^{(t)}$ дуги (i, j) в орграфе Γ^t равна наибольшей среди меток всех путей длины $t \geq 1$ из вершины i в вершину j оргграфа Γ :

$$m_{ij}^{(t)} = \begin{cases} 0, & \text{если } j \text{ недостижима из } i \text{ за } t \text{ шагов в } \Gamma, \\ 1, & \text{если каждый путь из } i \text{ в } j \text{ длины } t \text{ в } \Gamma \text{ есть 1-путь,} \\ 2, & \text{если имеется 2-путь из } i \text{ в } j \text{ длины } t \text{ в } \Gamma. \end{cases}$$

Для $w \in P^{(+)}$ выполнено разбиение $\widehat{C}_w = \widehat{C}_w^1 \cup \widehat{C}_w^2$ (пустые блоки допустимы), где $\widehat{C}_w^g$ — множество всех w -инцидентных g -контуров, $g \in \{1, 2\}$.

Назовём $\widehat{C}_w^{[g]}$ -*усложнением* пути w его $\widehat{C}_w$ -усложнение с меткой g .

В орграфе $\Gamma \in \widetilde{\Gamma}_{n,G}^{(i,j)}$ опишем длины всех $\widehat{C}_w^{[g]}$ -усложнений простого пути w с учётом меток путей и контуров. Пусть при $g \in \{1, 2\}$

- $P^{(g,0)}$ — множество простых g -путей из i в j с нулевым индексом;
- $P^{(g,+)}$ — множество простых g -путей из i в j с положительным индексом;
- $\widehat{U}_w^{(g)}$ — множество всех $\widehat{C}_w^{[g]}$ -усложнений пути w ;
- $\widehat{U}^{(g)} = \bigcup_{w \in P^{(+)}} \widehat{U}_w^{(g)}$;
- $\lambda_w = \min L(\widehat{C}_w^2)$ для пути $w \in P^{(1,+)}$;
- $\delta_w = l_w + \Phi_w + \lambda_w$ для пути $w \in P^{(1,+)}$;
- $\delta^{(i,j)} = \max_{w \in P^{(+)}} \delta_w$.

Теорема 6 (о длинах $\widehat{C}_w^{[g]}$ -усложнений). Если $w \in P^{(+)}$, то

$$L(\widehat{U}_w^{(1)}) = \begin{cases} l_w + \langle L(\widehat{C}_w^1) \rangle, & \text{если } w \in P^{(1,+)}, \\ \emptyset, & \text{если } w \in P^{(2,+)}, \end{cases}$$

$$L(\widehat{U}_w^{(2)}) = \begin{cases} \emptyset, & \text{если } w \in P^{(1,+)}, \widehat{C}_w^2 = \emptyset, \\ l_w + (L(\widehat{C}_w^1) \cup [L(\widehat{C}_w^2)]^+), & \text{если } w \in P^{(1,+)}, \widehat{C}_w^2 \neq \emptyset, \\ l_w + \langle L(\widehat{C}_w) \rangle, & \text{если } w \in P^{(2,+)}. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. В силу теоремы 5 усложнение h -контуром g -пути w есть gh -путь. Тогда 1-усложнение возможно лишь 1-контурами для 1-пути w , и сумма длин усложняющих контуров есть число полугруппы $\langle L(\widehat{C}_w^1) \rangle$.

Для 2-пути любые контуры дают 2-усложнения, для 1-пути w лишь набор контуров, содержащий 2-контур, даёт 2-усложнение, тогда сумма длин усложняющих контуров есть число множества $L(\widehat{C}_w^1) \cup [L(\widehat{C}_w^2)]^+$. Формулы для $L(\widehat{U}_w^{(g)})$ доказаны, $g \in \{1, 2\}$. Теорема 6 доказана.

Следствие 2. Для путей $w \in P^{(+)}$ верны включения

$$L(\widehat{U}_w^{(2)}) \supseteq \begin{cases} \delta_w + d_w \mathbb{N}, & \text{если } w \in P^{(1,+)}, \widehat{C}_w^2 \neq \emptyset, \\ l_w + \Phi_w + d_w \mathbb{N}, & \text{если } w \in P^{(2,+)}, \widehat{C}_w \neq \emptyset. \end{cases}$$

ДОКАЗАТЕЛЬСТВО вытекает из теоремы 6 и леммы 1. Следствие 2 доказано.

7. О локальной 2-примитивности помеченного орграфа

Пусть $\Gamma \in \Gamma_{n,G}$ и $M = (m_{ij})$ — матрица меток. Обозначим через Γ_B орграф с матрицей меток $B * M$, где B — двоичная маска порядка n для орграфа Γ . Орграфы Γ и Γ_B назовём 2_B -полными, если $B * M = (2_B)$. Орграф Γ называется $2_{(i,j)}$ -примитивным, $1 \leq i, j \leq n$, если существует число $\gamma \in \mathbb{N}$ такое, что для любого $t \geq \gamma$ в Γ имеется 2-путь длины t из i в j (или в Γ^t имеется дуга (i, j) с меткой 2); наименьшее такое γ обозначим $\exp^{[2_{(i,j)}]} \Gamma$ (кратко $\gamma_{2_{(i,j)}}$) и назовём $2_{(i,j)}$ -экспонентом орграфа Γ . Орграф Γ называется 2_B -примитивным, если из равенства $b_{ij} = 1$ следует $2_{(i,j)}$ -примитивность. Величину $\exp^{[2_B]} \Gamma$, кратко γ_{2_B} , назовём 2_B -экспонентом: $\gamma_{2_B} = \max_{(i,j): b_{ij}=1} \gamma_{2_{(i,j)}}$.

Свойства 2_B -примитивного n -вершинного орграфа Γ :

- 1) если $\Gamma = \theta(M)$, то $\exp^{[2_B]} \Gamma = \exp^{[2_B]} M$;
- 2) если орграф $2_{(i,j)}$ -примитивный, то $P^{(1,+)} \cup P^{(2,+)} \neq \emptyset$;
- 3) если орграф 2-примитивный, то при любой маске B он 2_B -примитивный и $\exp^{[2]} \Gamma \geq \exp^{[2_B]} \Gamma$;

4) 2_B -примитивный оргграф при некоторой маске B не обязательно связный или сильно связный;

5) *монотонность по маскам*: если $A \leq B$, то 2_B -примитивный оргграф Γ является 2_A -примитивным и $\exp^{[2_A]} \Gamma \leq \exp^{[2_B]} \Gamma$.

Множество $L(U^{(2)})$ длин 2-усложнений простых путей из i в j вполне определяет $2_{(i,j)}$ -примитивность помеченного оргграфа и его $2_{(i,j)}$ -экспонент.

Пусть

$$\begin{aligned} \bullet \Lambda^{(1)} &= \bigcap_{w \in P^{(1,+)}} (\mathbb{N}^{[\delta_w]} \setminus L(U_w^{(2)}))^{[\delta_w]}; \\ \bullet \Lambda^{(2)} &= \bigcap_{w \in P^{(2,+)}} (\mathbb{N}^{[l_w + \Phi_w]} \setminus L(U_w^{(2)}))^{[l_w + \Phi_w]}. \end{aligned}$$

Теорема 7 (критерий $2_{(i,j)}$ -примитивности). Пусть для $\Gamma \in \Gamma_{n,G}$ имеем $P^{(+)} \neq \emptyset$. Оргграф Γ $2_{(i,j)}$ -примитивный тогда и только тогда, когда система вычетов $\{L(U^{(2)})^{(\sigma^{(i,j)}, \sigma^{(i,j)} + D)} \equiv_D\}$ полна, где

$$\sigma^{(i,j)} = \begin{cases} \delta^{(i,j)}, & \text{если } P^{(2,+)} = \emptyset, \\ h^{(i,j)} & \text{иначе.} \end{cases}$$

При этом для $2_{(i,j)}$ -экспонента верна оценка

$$\gamma_{2_{(i,j)}} \leq 1 + \begin{cases} \max \Lambda^{(1)} \setminus L(P^{(0)}), & \text{если } P^{(2,+)} = \emptyset, \\ \max \Lambda^{(2)} \setminus L(P^{(0)}), & \text{если } P^{(1,+)} = \emptyset, \\ \max(\Lambda^{(1)} \cap \Lambda^{(2)}) \setminus L(P^{(0)}) & \text{иначе.} \end{cases} \quad (2)$$

В частности, если $\Gamma \in \tilde{\Gamma}_{n,G}^{(i,j)}$, то в (2) имеет место равенство.

Вычисление оценок требует менее

$$|P^{(+)}| \lceil \log_2 |P^{(+)}| \rceil + \left(\sum_{w \in P^{(+)}} \Phi_w + |P^{(0)}| \right) \lceil \log_2 \sigma^{(i,j)} \rceil$$

сравнений целых чисел, не больших $\max\{n, \Phi^{(i,j)}\}$.

Доказательство. Если оргграф Γ $2_{(i,j)}$ -примитивный с $2_{(i,j)}$ -экспонентом, равным $\gamma_{2_{(i,j)}}$, то $L(U^{(2)})$ не содержит $\gamma_{2_{(i,j)}} - 1$ и содержит все целые числа, не меньшие $\gamma_{2_{(i,j)}}$. Значит, $L(U^{(2)})$ содержит все числа, не меньшие $\gamma_{2_{(i,j)}}$, и $\gamma_{2_{(i,j)}} = 1 + \max \mathbb{N} \setminus L(U^{(2)})$.

Пусть $\Gamma \in \tilde{\Gamma}_{n,G}^{(i,j)}$. В соответствии с теоремой 3 возможны 3 случая.

1) $P^{(2,+)} = \emptyset$. Тогда $L(U_w)$ есть $(\Phi_w + \lambda_w, d_w, l_w)$ -выборка. Полнота объединения $L(U^{(2)})$ выборок для путей $w \in P^{(1,+)}$ по теореме 2 равносильна полноте системы $\{L(U^{(2)})^{(\delta^{(i,j)}, \delta^{(i,j)} + D)} \equiv_D\}$, откуда с учётом путей нулевого индекса $\gamma_{2_{(i,j)}} - 1 = \max \Lambda^{(1)} \setminus L(P^{(0)})$.

2) $P^{(1,+)} = \emptyset$. Тогда $L(U_w)$ есть (Φ_w, d_w, l_w) -выборка. Полнота объединения $L(U^{(2)})$ выборов для путей $w \in P^{(2,+)}$ по теореме 2 равносильна полноте системы $\{L(U)^{(h^{(i,j)}, h^{(i,j)}+D)} \equiv_D\}$, откуда с учётом $P^{(0)}$ имеем

$$\gamma_{2(i,j)} - 1 = \max \Lambda^{(2)} \setminus L(P^{(0)}).$$

3) $P^{(1,+)} \neq \emptyset$ и $P^{(2,+)} \neq \emptyset$. Тогда $L(U_w)$ есть (Φ_w, d_w, l_w) -выборка. Полнота объединения $L(U^{(2)})$ выборов для путей $w \in P^{(+)}$ по теореме 3 равносильна полноте системы вычетов $\{L(U)^{(h^{(i,j)}, h^{(i,j)}+D)} \equiv_D\}$, откуда с учётом $P^{(0)}$

$$\gamma_{2(i,j)} - 1 = \max(\Lambda^{(1)} \cap \Lambda^{(2)}) \setminus L(P^{(0)}).$$

Если $\Gamma \in \Gamma_{n,G}$, то множество $L(U^{(2)})$ может быть шире, чем для $\Gamma \in \tilde{\Gamma}_{n,G}^{(i,j)}$, т. е. возможно снижение значения $\gamma_{2(i,j)}$ по сравнению с оценкой.

Алгоритм вычисления оценок $\gamma_{2(i,j)}$ состоит в упорядочивании множества $P^{(+)}$ (что требует не более $|P^{(+)}| \lceil \log_2 |P^{(+)}| \rceil$ сравнений чисел) и поиске чисел из $\mathbb{N} \setminus \widehat{L(U)}$ в упорядоченном массиве мощности, меньшей $\Phi^{(i,j)}$. Сравнимые числа не превышают n (количества разных длин простых путей), а числа усложнений длины не больше значения $l_w + \Phi_w$, ограниченного числом Φ_w для каждого пути $w \in P^{(+)}$. Во всех случаях в соответствии с теоремой 3 и с учётом путей из $P^{(0)}$ оценка сложности вычисления $\gamma_{2(i,j)}$ имеет нужный вид.

При оценке вычислительной сложности алгоритма учтено, что

- 1) $l_{w_1} + \Phi_{w_1} + \lambda_{w_1} = \delta^{(i,j)}$ в силу упорядоченности путей;
 - 2) $|L(U_{w_t}^{(2)})^{\lceil \delta^{(i,j)} \rceil}| < \Phi_{w_t}$;
 - 3) $|L^{(0)}| \leq |P^{(2,0)}|$, так как усложнения пути индекса 0 тривиальны;
 - 4) в силу неравенств $|L_t| \leq \sigma^{(i,j)}$, $t = 0, \dots, r$, для поиска числа в упорядоченном массиве L_t требуется не более $\lceil \log_2 \sigma^{(i,j)} \rceil$ сравнений чисел.
- Теорема 7 доказана.

Пример 2. Для 5-вершинного орграфа Γ , заданного списком помеченных дуг $(1,1,2)$, $(1,1,3)$, $(1,1,4)$, $(2,1,3)$, $(2,2,5)$, $(3,1,4)$, $(4,1,2)$, распознаем его $2_{(1,5)}$ -примитивность, при положительном результате найдём $\exp^{[2_{(1,5)}]} \Gamma$.

Орграф Γ принадлежит $\tilde{\Gamma}_{5,G}^{(1,5)}$ и содержит 1-контур $C = (2, 3, 4)$ длины $l = 3$, инцидентный простым 2-путям $(1, 2, 5)$, $(1, 4, 2, 5)$ и $(1, 3, 4, 2, 5)$, $P^{(1,+)} = \emptyset$.

Характеристики путей из 1 в 5: $d = D = 3$, $\Phi(L(C)) = \Phi(3) = -3$, $h^{(1,5)} = \max\{2 - 3, 3 - 3, 4 - 3\} = 1$, $L(U^{(2)}) = \{2, 3, 4\}$. По теореме 10

$$\{L(U^{(2)})^{(h^{(1,5)}, h^{(1,5)}+D)} \equiv_D\} = L(U^{(2)})^{(1,4)} = \{2, 3, 4\},$$

т. е. множество вычетов полное: $\{\{2, 3, 4\} \equiv_3\} = \{0, 1, 2\}$. Тогда по теореме 7 орграф $2_{(1,5)}$ -примитивный и $\gamma_{2_{(1,5)}} = 2$.

Пример 3. Для 8-вершинного орграфа Γ , заданного списком помеченных дуг $(1,1,2)$, $(1,1,3)$, $(2,1,3)$, $(3,1,4)$, $(3,1,5)$, $(4,1,2)$, $(5,2,6)$, $(6,1,7)$, $(6,2,8)$, $(7,1,3)$, распознаем $2_{(1,8)}$ -примитивность, и при наличии свойства найдём $\exp^{[2_{(1,8)}]} \Gamma$.

Орграф Γ принадлежит $\tilde{\Gamma}_{8,G}^{(1,8)}$ и содержит 1-контур $C_1 = (2, 3, 4)$ длины $l_1 = 3$ и 2-контур $C_2 = (3, 5, 6, 7)$ длины $l_2 = 4$. Тогда $\widehat{C} = \{C_1, C_2\}$ и через контуры проходят 2 простых пути из 1 в 8: 2-путь $(1, 3, 5, 6, 8)$ длины 4 и 2-путь $(1, 2, 3, 5, 6, 8)$ длины 5; C_1 и C_2 инцидентны обоим путям, $P^{(1,+)} = \emptyset$.

Характеристики путей из 1 в 8: $d_1 = d_2 = D = 1$, $\Phi(L(\widehat{C})) = \Phi(3, 4) = 5$, $h = \max\{4+5, 5+5\} = 10$, $L(U^{(2)}) = \{4, 5\}$. Множество вычетов полное:

$$L(U^{(2)})^{(h(1,8)+\delta(1,8), h(1,8)+\delta(1,8)+D)} = L(U^{(2)})^{(10,11)} = \{11\},$$

$\{\{11\} \equiv_1\} = \{0\}$. Значит, $2_{(1,8)}$ -примитивность выполнена, и $\gamma_{2_{(1,8)}} = 10$ по теореме 7.

8. О нелинейности преобразований векторного пространства

Сложные криптографические функции часто построены с помощью произведения функций, относительно несложно реализуемых аппаратно и/или программно. Например, в симметричных блочных шифрах шифрующая подстановка есть произведение нескольких однотипных раундовых функций. Для оценки некоторых характеристик нелинейности произведения функций применим МГП, использующий троичные матрицы и помеченные орграфы.

Следуя ранее введённой терминологии, дадим ряд понятий.

Булеву функцию назовём *вполне нелинейной* (в.н.ф.), если она зависит нелинейно от каждого переменного. Заметим, что класс в.н.ф. содержит не только все максимально нелинейные б.ф., но и ряд равновероятных б.ф., перспективных с точки зрения криптографических приложений.

Для преобразования $g: V_n \rightarrow V_n$ его координатные б.ф. обозначим через $g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)$, а координатные б.ф. степени g^t , $t \geq 1$, — через $g_1^t(x_1, \dots, x_n), \dots, g_n^t(x_1, \dots, x_n)$.

Преобразование g называется

а) *вполне нелинейным* (в.н.п.), если все его координатные б.ф. суть в.н.ф.;

б) *B-нелинейным*, если из равенства $b_{ij} = 1$ следует, что координатная б.ф. $g_j(x_1, \dots, x_n)$ зависит нелинейно от x_i ;

в) *2-перфективным*, если в циклической полугруппе $\langle g \rangle$ содержится в. н. п.; наименьшее $t \in \mathbb{N}$, при котором g^t — в. н. п., назовём *показателем 2-перфективности* преобразования g и обозначим через $\text{prf}^{[2]} g$;

г) *2_B-перфективным*, если в циклической полугруппе $\langle g \rangle$ содержится B -нелинейное преобразование; наименьшее $t \in \mathbb{N}$, при котором g^t B -нелинейно, назовём *показателем 2_B-перфективности* преобразования g , обозначим через $\text{prf}^{[2B]} g$.

Преобразованию g пространства V_n однозначно соответствуют

а) троичная матрица $M_\theta(g) = (m_{ij}^g)$ порядка n над G , называемая *матрицей нелинейности* преобразования g , где

$$m_{ij}^g = \begin{cases} 0, & \text{если } g_j \text{ зависит от } x_i \text{ фиктивно,} \\ 1, & \text{если } g_j \text{ зависит от } x_i \text{ линейно,} \\ 2, & \text{если } g_j \text{ зависит от } x_i \text{ нелинейно,} \end{cases}$$

$1 \leq i, j \leq n$; положим $M_{\theta,B}(g) = B * M_\theta(g)$;

б) помеченный орграф $\Gamma_\theta(g)$ с множеством вершин $\overline{1, n}$, называемый *графом нелинейности* преобразования g , где дуга (i, j) помечена числом m_{ij}^g , $1 \leq i, j \leq n$, нулевая метка кодирует отсутствие дуги в графе; через $\Gamma_{\theta,B}(g)$ обозначим B -часть орграфа $\Gamma_\theta(g)$.

Матрица $M_\theta(g)$ есть матрица меток орграфа $\Gamma_\theta(g)$.

Обозначим через $\widehat{G} = \{g^{(1)}, \dots, g^{(p)}\}$ множество преобразований пространства V_n , $p \geq 1$. Множество $\widehat{G}$ называется

а) *2-перфективным*, если полугруппа $\langle \widehat{G} \rangle$ содержит в. н. п.; наименьшая длина слова в алфавите $\widehat{G}$, задающего в. н. п., называется *показателем 2-перфективности* множества $\widehat{G}$, обозначается $\text{prf}^{[2]} \widehat{G}$;

б) *2_B-перфективным*, если полугруппа $\langle \widehat{G} \rangle$ содержит B -нелинейное преобразование; наименьшая длина слова в алфавите $\widehat{G}$, задающего B -нелинейное преобразование, называется *показателем 2_B-перфективности* множества $\widehat{G}$, обозначается $\text{prf}^{[2B]} \widehat{G}$.

Множеству $\widehat{G}$ преобразований соответствуют множество матриц нелинейности $\widehat{M}_\theta(\widehat{G}) = \{M_\theta(g^{(1)}), \dots, M_\theta(g^{(p)})\}$ и множество орграфов нелинейности $\widehat{\Gamma}_\theta(\widehat{G}) = \{\Gamma_\theta(g^{(1)}), \dots, \Gamma_\theta(g^{(p)})\}$.

Теорема 8 (основная теорема МГП [3]). Для произвольных преобразований $g^{(1)}, \dots, g^{(p)}$ пространства V_n имеем

$$M_\theta(g^{(1)}) \dots g^{(p)} \leq M_\theta(g^{(1)}) \dots M_\theta(g^{(p)}), \quad p \geq 1;$$

в частности, $M_\theta(g^t) \leq (M_\theta(g))^t$ для преобразования g при $t > 1$.

Отношение превосходства верно и для $M_{\theta,B}(g)$ при любой маске B .

Следствие 3. Для 2-перфективного множества $\widehat{G}$ имеем

$$\text{prf}^{[2]} \widehat{G} \geq \exp^{[2]} \widehat{M}_\theta(\widehat{G}).$$

В частности, $\text{prf}^{[2]} g \geq \exp^{[2]} M_\theta(g)$ для 2-перфективного преобразования g . Отсюда $\text{prf}^{[2_B]} \widehat{G} \geq \exp^{[2_B]} \widehat{M}_\theta(\widehat{G})$ для любой матрицы B , в частности,

$$\text{prf}^{[2_B]} g \geq \exp^{[2_B]} M_\theta(g).$$

Свойства 2_B -перфективных преобразований при любой маске B .

1) Свойства 2-перфективности и 2_B -перфективности не являются монотонными и наследственными: если преобразование g^t 2-перфективно (2_B -перфективно), $t \geq 1$, то не обязательно g^{t+k} или g^{kt} 2-перфективно (2_B -перфективно), $k \geq 1$.

2) Если порождённая небиективным 2_B -перфективным преобразованием g циклическая полугруппа $\langle g \rangle$ определена соотношением $g^d = g^{d+n}$, где d — циклическая глубина, а n — период преобразования g , то начиная со степени $t \geq d + n$ преобразования g^t повторяются, т. е. $g^{t-d} = g^t$. Это означает, что справедливы оценки

$$\exp^{[2_B]} M_\theta(g) \leq \text{prf}^{[2_B]} g < d + n.$$

3) Если подстановка g 2_B -перфективна, то

$$\exp^{[2_B]} M_\theta(g) \leq \text{prf}^{[2_B]} g < \text{ord } g.$$

Пример 4. При $B = \{(1, 2), (1, 4), (2, 3)\}$ оценим $\text{prf}^{[2_B]} g$ для подстановки g регистра левого сдвига длины 4 с обратной связью $f = x_1 \oplus x_3 x_4$. Составим матрицу нелинейности $M_\theta(g) = M$ и найдём $\exp^{[2_B]} M_\theta(g)$:

$$\begin{aligned} M &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix}, & M^2 &= \begin{pmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 2 \end{pmatrix}, \\ M^3 &= \begin{pmatrix} 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 \end{pmatrix}, & M^4 &= \begin{pmatrix} 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \\ M^5 &= \begin{pmatrix} 2 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, & M^6 &= \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}. \end{aligned}$$

Тогда в силу следствия 3 имеем

$$\text{prf}^{[2_B]} g \geq \exp^{[2_B]} M = 4.$$

Вычислим АНФ координатных функций для степеней подстановки g . Используя закон рекурсии регистра сдвига, найдём его выходные функции $f_i(x_1, x_2, x_3, x_4)$, где g^i задана координатными функциями $f_{i+1}(x_1, x_2, x_3, x_4)$, $f_{i+2}(x_1, x_2, x_3, x_4)$, $f_{i+3}(x_1, x_2, x_3, x_4)$, $f_{i+4}(x_1, x_2, x_3, x_4)$, $i \geq 1$:

$$\begin{aligned} f_i(x_1, x_2, x_3, x_4) &= x_i, \quad i = 1, 2, 3, 4, \\ f_5(x_1, x_2, x_3, x_4) &= x_1 \oplus x_3x_4, \\ f_6(x_1, x_2, x_3, x_4) &= x_2 \oplus x_1x_4 \oplus x_3x_4, \\ f_7(x_1, x_2, x_3, x_4) &= x_3 \oplus x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \oplus x_2x_3x_4, \\ f_8(x_1, x_2, x_3, x_4) &= x_4 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4. \end{aligned}$$

Отсюда подстановки g, g^2, g^3 не B -нелинейные. Подстановка g^4 B -нелинейная, так как имеются нелинейные зависимости: f_6 и f_8 от x_1 , f_7 от x_2 . Следовательно, подстановка g 2_B -перфективна, $\text{prf}^{[2_B]} g = 4$.

Финансирование работы

Исследование выполнено за счёт бюджетов организаций, указанных автором на первой странице статьи. Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Автор заявляет, что у него нет конфликта интересов.

Литература

1. **Fomichev V. M., Koreneva A. M.** Encryption performance and security of certain wide block ciphers // J. Comput. Virol. Hacking Tech. 2020. V. 16. P. 197–216.
2. **Фомичёв В. М., Авезова Я. А., Коренева А. М., Кяжин С. Н.** Примитивность и локальная примитивность орграфов и неотрицательных матриц // Дискрет. анализ и исслед. операций. 2018. Т. 25, № 3. С. 95–125.
3. **Фомичёв В. М.** Оценка характеристик нелинейности итеративных преобразований векторного пространства // Дискрет. анализ и исслед. операций. 2020. Т. 27, № 4. С. 131–151.
4. **Frobenius G.** Über Matrizen aus nicht negativen Elementen // Berl. Ber. 1912. S. 456–477. [German].
5. **Dulmage A. L., Mendelsohn N. S.** Gaps in the exponent set of primitive matrices // Ill. J. Math. 1964. V. 8, No. 4. P. 642–656.
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 Trans. Comput. 2016. V. 65, No. 7. P. 2074–2089.

7. **Berger T., Minier M., Thomas G.** Extended generalized Feistel networks using matrix representation // Selected areas in cryptography—SAC 2013. Proc. 20th Int. Conf. (Burnaby, Canada, Aug. 14–16, 2013). Heidelberg: Springer, 2014. P. 289–305. (Lect. Notes Comput. Sci.; V. 8282).
8. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. V. 14, No. 4. P. 483–499.
9. **Huang Y., Liu B.** Generalized r -exponents of primitive digraphs // Taiwan. J. Math. 2011. V. 15, No. 5. P. 1999–2012.
10. **Liu B.** Generalized exponents of Boolean matrices // Lin. Algebra Appl. 2003. V. 373. P. 169–182.
11. **Miao Z., Zhang K.** The local exponent sets of primitive digraphs // Lin. Algebra Appl. 2000. V. 307. P. 15–33.
12. **Shen J., Neufeld S.** Local exponents of primitive digraphs // Lin. Algebra Appl. 1998. V. 268. P. 117–129.
13. **Suzaki T., Minematsu K.** Improving the generalized Feistel // Fast software encryption. Proc. 17th Int. Workshop (Seoul, Korea, Feb. 7–10, 2010). Heidelberg: Springer, 2010. P. 19–39. (Lect. Notes Comput. Sci.; V. 6147).
14. **Wielandt H.** Unzerlegbare, nicht negative Matrizen // Math. Z. 1950. Bd. 52. S. 642–648. [German].
15. **Perkins P.** A theorem on regular graphs // Pac. J. Math. 1961. V. 2. P. 1529–1533.
16. **Dulmage A. L., Mendelsohn N. S.** The exponent of a primitive matrix // Can. Math. Bull. 1962. V. 5, No. 3 P. 241–244.
17. **Neufeld S. W.** A diameter bound on the exponent of a primitive directed graph // Lin. Algebra Appl. 1996. V. 245. P. 27–47.
18. **Nyberg K.** Generalized Feistel networks // Advances in cryptology—ASIACRYPT’96. Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. (Kyongju, Korea, Nov. 3–7, 1996). Heidelberg: Springer, 1996. P. 91–104. (Lect. Notes Comput. Sci.; V. 1163).

Владимир Михайлович Фомичёв

Статья поступила

4 марта 2026 г.

После доработки —

10 марта 2026 г.

Принята к публикации

23 марта 2026 г.

LOCAL NONLINEARITY OF TRANSFORMATION ITERATIONS

V. M. Fomichev^{1,2}¹RUDN University,

6 Miklukho-Maklay Street, 117198 Moscow, Russia

²Institute of Informatics Problems of FRC CSC RAS,

44 Bld. 2 Vavilov Street, 119333 Moscow, Russia

E-mail: fomichev.2016@yandex.ru

Abstract. In accordance with Shannon's concept of the mixing properties of information transformations, a previously proposed matrix-graph approach is developed for assessing the characteristics of nonlinearity in the product of transformations in vector spaces. This approach makes it possible to evaluate local nonlinear properties of the product of transformations using ternary matrices and labeled digraphs that correspond unambiguously to the transformations. For ternary matrices and labeled digraphs, the property of local 2-primitivity and assessments of local 2-exponents, including exact values, is defined using path lengths. Criteria for local 2-primitivity is established. The results for matrices and labeled digraphs are applied to evaluate the characteristics of the product of transformations in vector spaces. Examples are considered. Bibliogr. 18.

Keywords: ternary matrix, locally primitive matrix, 2-primitive matrix, 2-exponent of a matrix, 2-primitive labeled orgraph.

References

1. V. M. Fomichev and A. M. Koreneva, Encryption performance and security of certain wide block ciphers, *J. Comput. Virol. Hacking Tech.* **16**, 197–216 (2020).
2. V. M. Fomichev, Ya. A. Avezova, A. M. Koreneva, and S. N. Kyazhin, Primitivity and local primitivity of digraphs and nonnegative matrices, *Diskretn. Anal. Issled. Oper.* **25** (3), 95–125 (2018) [Russian] [*J. Appl. Ind. Math.* **12** (3), 453–469 (2018)].

3. **V. M. Fomichev**, Estimating nonlinearity characteristics for iterative transformations of a vector space, *Diskretn. Anal. Issled. Oper.* **27** (4), 131–151 (2020) [Russian] [*J. Appl. Ind. Math.* **14** (4), 610–622 (2020)].
4. **G. Frobenius**, Über Matrizen aus nicht negativen Elementen, *Berl. Ber.*, 456–477 (1912) [German].
5. **A. L. Dulmage** and **N. S. Mendelsohn**, Gaps in the exponent set of primitive matrices, *Ill. J. Math.* **8** (4), 642–656 (1964).
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** (7), 2074–2089 (2016).
7. **T. Berger**, **M. Minier**, and **G. Thomas**, Extended generalized Feistel networks using matrix representation, in *Selected Areas in Cryptography — SAC 2013*, Proc. 20th Int. Conf. (Burnaby, Canada, Aug. 14–16, 2013) (Springer, Heidelberg, 2014), pp. 289–305 (Lect. Notes Comput. Sci., Vol. 8282).
8. **R. A. Brualdi** and **B. Liu**, Generalized exponents of primitive directed graphs, *J. Graph Theory* **14** (4), 483–499 (1990).
9. **Y. Huang** and **B. Liu**, Generalized r -exponents of primitive digraphs, *Taiwan. J. Math.* **15** (5), 1999–2012 (2011).
10. **B. Liu**, Generalized exponents of Boolean matrices, *Lin. Algebra Appl.* **373**, 169–182 (2003).
11. **Z. Miao** and **K. Zhang**, The local exponent sets of primitive digraphs, *Lin. Algebra Appl.* **307**, 15–33 (2000).
12. **J. Shen** and **S. Neufeld**, Local exponents of primitive digraphs, *Lin. Algebra Appl.* **268**, 117–129 (1998).
13. **T. Suzaki** and **K. Minematsu**, Improving the generalized Feistel, in *Fast Software Encryption*, Proc. 17th Int. Workshop (Seoul, Korea, Feb. 7–10, 2010) (Springer, Heidelberg, 2010), pp. 19–39 (Lect. Notes Comput. Sci., Vol. 6147).
14. **H. Wielandt**, Unzerlegbare, nicht negative Matrizen, *Math. Z.* **52**, 642–648 (1950). [German].
15. **P. Perkins**, A theorem on regular graphs, *Pac. J. Math.* **2**, 1529–1533 (1961).
16. **A. L. Dulmage** and **N. S. Mendelsohn**, The exponent of a primitive matrix, *Can. Math. Bull.* **5** (3), 241–244 (1962).
17. **S. W. Neufeld**, A diameter bound on the exponent of a primitive directed graph, *Lin. Algebra Appl.* **245**, 27–47 (1996).
18. **K. Nyberg**, Generalized Feistel networks, in *Advances in Cryptology — ASIACRYPT’96*, Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. (Kyongju, Korea, Nov. 3–7, 1996) (Springer, Heidelberg, 1996), pp. 91–104 (Lect. Notes Comput. Sci., Vol. 1163).

Vlaimir M. Fomichev

Received March 4, 2026

Revised March 10, 2026

Accepted March 23, 2026