

ТОЧНАЯ ФОРМУЛА ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ ОРГРАФОВ РЕГИСТРОВЫХ ПРЕОБРАЗОВАНИЙ

В. М. Фомичёв^{1,2,3,4,a}, Я. Э. Авезова^{2,b}

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

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

³ Институт проблем информатики ФИЦ «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, 119333 Москва, Россия

⁴ ООО «Код Безопасности»,
1-й Нагатинский пр-д, 10, стр. 1, 115230 Москва, Россия

E-mail: ^a fomichev.2016@yandex.ru, ^b avezovayana@gmail.com

Аннотация. Орграф называется примитивным, если его некоторая степень есть полный орграф (содержит все возможные дуги), а наименьшее такая степень называется экспонентом орграфа. В примитивном орграфе элементарным локальным экспонентом для вершин u и v называют наименьшее целое положительное γ такое, что в орграфе есть пути из u в v любой длины, не меньшей γ . Преобразованию двоичного n -мерного векторного пространства, заданному системой n координатных функций, соответствует n -вершинный ориентированный граф, где пара (u, v) есть дуга, если координатная функция с номером v зависит существенно от переменной с номером u . Такой орграф называют перемешивающим графом преобразования.

Исследованы перемешивающие графы широко используемых в криптологии преобразований регистров сдвига длины $n > 1$ с нелинейной булевой функцией обратной связи. Получена точная формула экспонента и элементарных локальных экспонентов для примитивного перемешивающего орграфа преобразования регистра сдвига. Результаты могут применяться для оценки длины холостого хода генераторов псевдослучайных последовательностей. Библиогр. 20.

Ключевые слова: перемешивающий орграф, примитивный орграф, локально примитивный орграф, регистр сдвига, экспонент орграфа.

Основные обозначения

- N — множество всех натуральных чисел, $p, q \in N$;
- Z — множество всех целых чисел;
- $\text{GF}(2)$ — поле Галуа порядка 2;
- $Z[p, q] = \{a \in Z \mid p \leq a \leq q\}$, $Z[p, q] = \emptyset$ при $p > q$;
- $Z[p, \dots)$ — множество целых чисел, не меньших p ;
- $I[p, q] = \{a \in Z[p, q] \mid a \text{ нечётное}\}$;
- $J[p, q] = \{a \in Z[p, q] \mid a \text{ чётное}\}$;
- $I(A)$ — множество нечётных чисел множества $A \subset Z[0, \dots)$;
- $J(A)$ — множество чётных чисел множества $A \subset Z[0, \dots)$;
- $F(l_1, \dots, l_m)$ — число Фробениуса для аргументов $l_1, \dots, l_m \in N$, где $\text{НОД}(l_1, \dots, l_m) = 1$;
- $\Gamma(g)$ — перемешивающий орграф преобразования g множества V_n ;
- $\text{exp } \Gamma$ — экспонент орграфа Γ ;
- (u, v) - $\text{exp } \Gamma$ — локальный экспонент орграфа Γ , где $0 \leq u, v < n$;
- (i, j) — дуга в орграфе, инцидентная вершинам i и j ;
- $w \bullet w'$ — конкатенация путей w и w' орграфа;
- $\text{len } w$ ($\text{len } C$) — длина пути w (контура C), равная числу дуг пути (контура);
- $W(u, v)$ — множество всех путей из u в v ;
- ΛW — множество длин всех путей из множества путей W ;
- $\langle A \rangle$ — аддитивная полугруппа, порождённая множеством $A \subset N$.

Введение

Начало исследований условий примитивности графов и неотрицательных матриц положено трудом Фробениуса (1912 г.) [1], где был поставлен вопрос: имеются ли положительные матрицы в циклической полугруппе $\langle M \rangle$, порождённой квадратной матрицей с неотрицательными элементами? Если имеются, то порождающая матрица M называется *примитивной*, и *экспонентом матрицы* M называют наименьшее натуральное число t такое, что все элементы матрицы M^t положительные [2].

В настоящее время исследование экспонентов графов и матриц относится к актуальной области дискретной математики. Матрично-графовый подход (МГП) применяется для оценки множества существенных переменных и характеристик нелинейности композиций преобразований векторного пространства.

Развитие МГП привело к нетривиальным обобщениям двух видов: примитивность и экспонент множества матриц, а также локальная примитивность и локальные экспоненты [3]. Множество матриц называется *примитивным*, если порождённая им мультипликативная полугруппа содержит положительную матрицу [4–7]. Локальная примитивность

связана с положительностью всех элементов заранее определённой части матрицы, например части, полученной из исходной матрицы вычёркиванием некоторых строк и столбцов [8–10].

Биекция между ориентированными графами и матрицами смежности вершин орграфов позволяет формулировать и решать задачи как на матричном, так и графовом языке. Так, ориентированный граф Γ называется *примитивным*, если порождённая им циклическая полугруппа $\langle \Gamma \rangle$ содержит полный орграф (орграф, в котором есть все возможные дуги), а наименьшее натуральное t , при котором Γ^t полный, называют *экспонентом орграфа* Γ . В примитивном орграфе Γ *элементарным локальным экспонентом для вершин u, v* называют наименьшее натуральное γ такое, что в Γ есть пути из вершины u в вершину v длины t при любом $t \geq \gamma$.

Большую часть результатов составляют верхние оценки экспонентов того или иного класса примитивных графов или матриц (см., например, [11–17]), намного реже встречаются нижние оценки. Весьма редки формулы точных значений экспонентов класса графов, которые в основном относятся к узким классам примитивных графов, имеющих петли. Такое положение объясняется в общем случае тремя обстоятельствами:

- (1) экспонент орграфа допускает множество оценок, связанных с различными множествами контуров в орграфе;
- (2) значение любой оценки есть наибольшее число довольно сложно устроенного конечного множества натуральных чисел;
- (3) точная формула требует объединения информации по большому числу оценок.

Задача объединения информации для орграфа тем сложнее, чем больше в нём имеется контуров и путей между различными парами вершин.

МПП позволяет оценивать некоторые характеристики преобразований, используемых в итеративных алгоритмах блочного шифрования, а также при синтезе генераторов псевдослучайных последовательностей. Преобразованию g векторного пространства размерности n , заданному системой координатных функций

$$g(x_0, \dots, x_{n-1}) = (g_0(x_0, \dots, x_{n-1}), \dots, g_{n-1}(x_0, \dots, x_{n-1})),$$

соответствует ориентированный граф $\Gamma(g)$ с множеством вершин $\{0, \dots, n-1\}$, в котором пара (u, v) образует дугу, если переменная x_u существенна для координатной функции g_v . Орграф $\Gamma(g)$ принято называть *перемешивающим графом преобразования g* .

В работе исследованы перемешивающие графы регистровых преобразований, которым посвящены многие работы российских и зарубежных математиков [18–20]. Преобразование g называется *преобразованием регистра левого сдвига над $\text{GF}(2)$ с обратной связью $f(x_0, \dots, x_{n-1})$* , если

$g = (x_1, \dots, x_{n-1}, f(x_0, \dots, x_{n-1}))$, где f — булева функция. Если функция обратной связи f нелинейна, то преобразование g также нелинейно.

Нелинейные преобразования регистров сдвига используются при построении генераторов псевдослучайных последовательностей, в связи с чем анализ перемешивающих свойств преобразований данного класса имеет прикладное значение для ряда систем защиты информации. Хорошие перемешивающие свойства, т. е. существенная зависимость знаков вырабатываемой последовательности от начального состояния, имеет важное значение для противодействия методу последовательного опробования и методам дифференциального анализа. Экспонент перемешивающего графа преобразования регистра сдвига позволяет оценить длину холостого хода генератора — количество начальных тактов, в которых знаки выходной последовательности игнорируются.

Получена точная формула экспонента и всех элементарных локальных экспонентов перемешивающего орграфа $\Gamma(g)$ для произвольного регистрового преобразования g пространства n -мерных векторов.

Статья состоит из четырёх разделов. В разд. 1 описаны свойства перемешивающего графа $\Gamma(g)$ преобразования g регистра сдвига и доказаны леммы, которые используются для получения формул экспонентов. В разд. 2 представлен основной результат работы — точная формула экспонента орграфа $\Gamma(g)$. Она основана на точных формулах элементарных локальных экспонентов перемешивающего орграфа $\Gamma(g)$, зависящих от длины регистра n и от конфигурации множества номеров существенных переменных функции обратной связи регистра. Анализ множества всех элементарных локальных экспонентов орграфа Γ позволяет существенно сузить область пар вершин, на которых достигается максимум локальных экспонентов. В разд. 3 для случая, когда $\Gamma(g)$ имеет контур длины 2, формула экспонента уточнена. В заключительном разд. 4 получены легко вычисляемые оценки экспонента орграфа $\Gamma(g)$ и приведены вычислительные примеры.

1. Свойства перемешивающих орграфов регистровых преобразований

Обозначим через $R(n, m)$ класс преобразований g векторного пространства размерности n , реализуемых регистром левого сдвига с нелинейной обратной связью $f(x_0, \dots, x_{n-1})$, имеющей m существенных переменных, в том числе x_0 (иначе реальная длина регистра меньше n), $n \geq 3$, $2 \leq m \leq n$. Пусть множество вершин перемешивающего орграфа $\Gamma(g)$, соответствующих номерам входных переменных преобразования g , равно $\{0, \dots, n-1\}$.

Обозначим через $D(g) = \{d_1, \dots, d_m\}$ множество номеров существенных переменных функции $f(x_0, \dots, x_{n-1})$, где $0 = d_1 < \dots < d_m \leq n-1$.

Тогда преобразованию $g \in R(n, m)$ соответствует n -вершинный перемешивающий орграф $\Gamma(g)$, имеющий $n + m - 1$ дуг, где n дуг составляют гамильтонов контур $(n - 1, \dots, 0)$, а остальные дуги суть $(d_2, n - 1), \dots, (d_m, n - 1)$. Таким образом, связный орграф $\Gamma(g)$ есть объединение простых контуров C_1, \dots, C_m , где $C_t = (n - 1, n - 2, \dots, d_t)$, $t = 1, \dots, m - 1$, $C_m = (n - 1, n - 2, \dots, d_m)$ при $d_m < n - 1$ и C_m есть петля в вершине $n - 1$ при $d_m = n - 1$. Вершины $d_m, \dots, n - 1$ общие для всех простых контуров. Следовательно, орграф $\Gamma(g)$ примитивный тогда и только тогда, когда $\text{НОД}\{n - D(g)\} = 1$, и если $\text{НОД}\{n - D(g)\} = 1$, то орграф $\Gamma(g)$ является (u, v) -примитивным при любых $u, v \in \{0, \dots, n - 1\}$.

Пусть $S, Y \subseteq Z[0, \dots)$. Обозначим

$$\overline{S} = Z[0, \dots) \setminus S, \quad S + Y = \{s + y \mid s \in S, y \in Y\}$$

и положим $S + \emptyset = \emptyset$, $\max \emptyset = 0$.

Лемма 1. Для непустых подмножеств $S, Y \subseteq Z[0, \dots)$ и любого $l \in N$ верны следующие утверждения:

- (а) если $S \subseteq Y$, то $\overline{Y} \subseteq \overline{S}$;
- (б) $\overline{S_1 \cup \dots \cup S_t} = \overline{S_1} \cap \dots \cap \overline{S_t}$;
- (в) $\overline{S + l} = \{\overline{S} + l\} \cup Z[0, l - 1]$;
- (г) если множество \overline{S} конечно, то $\max \overline{S + l} = \max\{l + \max \overline{S}, l - 1\}$.

ДОКАЗАТЕЛЬСТВО. Пп. (а), (б) следуют из определения множества \overline{S} .

(в) По определению $\overline{S + l} \neq \emptyset$ при любом множестве S и любом числе $l \in N$. Пусть $a \in \overline{S + l}$, тогда $a \notin \{S + l\}$. Отсюда $a \in Z[0, l - 1]$ или $(a - l) \notin S$ при $a \geq l$; во втором случае $(a - l) \in \overline{S}$, что равносильно тому, что $a \in \{\overline{S} + l\}$. Следовательно, $a \in \{\overline{S} + l\} \cup Z[0, l - 1]$. Обратное включение следует из рассуждений в обратную сторону.

(г) В силу п. (в) $\max \overline{S + l} = \max\{\max\{\overline{S} + l\}, l - 1\}$. Если $\overline{S} \neq \emptyset$ и $\max \overline{S} = \mu \geq 0$, то $\max \overline{S + l} = \max\{\mu + l, l - 1\} = \mu + l$. Если $\overline{S} = \emptyset$, то $\max \overline{S + l} = l - 1$. Лемма 1 доказана.

При $0 \leq u, v < n$ введём следующие обозначения:

- $\tau(u)$ — наибольшее число из $\{1, \dots, m\}$ такое, что $d_{\tau(u)} \leq u$;
- $w_0(u, v) = (u, u - 1, \dots, v)$ — простой путь из u в v , где $v \leq u$ (при $v = u$ пустой путь);
- $w_t(u, v) = w_0(u, d_t) \bullet (d_t, n - 1) \bullet w_0(n - 1, v)$, $t = 1, \dots, \tau(u)$ — путь из u в v , $u < n - 1$;
- $l_t(u, v) = u - d_t + n - v$, $t = 1, \dots, \tau(u)$, $u < n - 1$;
- $L(u, v) = \{l_1(u, v), \dots, l_{\tau(u)}(u, v)\}$, $u < n - 1$.

При данных обозначениях $\tau(u) = 1, 0 \leq u < d_2; \tau(u) = m, d_m \leq u < n$; $\text{len } w_0(u, v) = u - v$; $w_t(u, v) = C_t$ при $u = v, t = 1, \dots, \tau(u)$; $\text{len } w_t(u, v) = l_t(u, v)$ при $u < n - 1, t = 1, \dots, \tau(u)$ и $l_1(u, v) > \dots > l_{\tau(u)}(u, v)$;

$$L(u, v) + \langle n - D(g) \rangle = \{l_1(u, v) + \langle n - D(g) \rangle\} \cup \dots \cup \{l_{\tau(u)}(u, v) + \langle n - D(g) \rangle\}. \quad (1)$$

Далее выражение «путь w проходит через контур C » означает, что у пути w и контура C есть общая вершина. Путь w проходит через множество контуров, если он проходит через каждый контур множества. При $k, t \in Z[0, \dots)$ обозначим через $kC(u)$ контур C , пройденный k -кратно из вершины u , а через $0C(u)$ — пустой контур.

Пусть путь $w = (u_0, u_1, \dots, u_t)$ длины t проходит через вершину u , общую для всех контуров множества $\widehat{C} = \{C_1, \dots, C_m\}$ (т. е. $u_s \in \{d_m, \dots, n - 1\}$ при некотором $s \in \{0, \dots, t\}$). Тогда при $0 < s < t$ путь w представим в виде конкатенации путей:

$$w = (u_0, \dots, u_{s-1}, u) \bullet (u, u_{s+1}, \dots, u_t).$$

Пути w и набору чисел $\hat{k} = (k_1, \dots, k_m) \in (Z[0, \dots))^m$ однозначно соответствует путь $w(\hat{k})$, называемый \widehat{C} -расширением пути w :

$$w(\hat{k}) = \begin{cases} \widehat{C}(u, k_1, \dots, k_m) \bullet (u, u_1, \dots, u_t), & \text{если } s = 0, \\ (u_0, \dots, u_{t-1}, u) \bullet \widehat{C}(u, k_1, \dots, k_m), & \text{если } s = t, \\ (u_0, \dots, u_{s-1}, u) \bullet \widehat{C}(u, k_1, \dots, k_m) \bullet (u, u_{s+1}, \dots, u_t), & \text{если } 0 < s < t, \end{cases}$$

где $\widehat{C}(u, k_1, \dots, k_m) = k_1 C_1(u) \bullet \dots \bullet k_m C_m(u)$. В каждом из трёх случаев все дуги пути w являются дугами пути $w(\hat{k})$ и порядок их следования в \widehat{C} -расширении сохраняется. В силу определения \widehat{C} -расширения пути начальные (и конечные) вершины путей w и $w(\hat{k})$ совпадают. Множество длин всех \widehat{C} -расширений пути w есть $\text{len } w + \langle \text{len } C_1, \dots, \text{len } C_m \rangle$.

Лемма 2. В $\Gamma(g)$ множество $\Lambda W(u, v)$ длин путей из u в v определено следующими равенствами:

- (а) если $u < v$, то $\Lambda W(u, v) = L(u, v) + \langle n - D(g) \rangle$;
- (б) если $u \geq v$, то

$$\Lambda W(u, v) = \begin{cases} u - v + \langle n - D(g) \rangle, & \text{если } d_m \leq u \leq n - 1, \\ \{L(u, v) + \langle n - D(g) \rangle\} \cup \{u - v\}, & \text{если } 0 \leq u < d_m. \end{cases}$$

Доказательство. Если $u < v$, то любой путь $w \in W(u, v)$ есть \widehat{C} -расширение одного из простых путей $w_1(u, v), \dots, w_{\tau(u)}(u, v)$, каждый

из которых проходит через вершину $n - 1$. Других путей из u в v в орграфе нет. Следовательно, $\Lambda W(u, v) = L(u, v) + \langle n - D(g) \rangle$.

Если $u \geq v$, то единственный простой путь из u в v есть $w_0(u, v)$, его длина равна $u - v$. Любой другой путь $w \in W(u, v)$ при $u \geq v$ не будет простым. Точнее, при $d_m \leq u < n$ вершина u общая для всех простых контуров в орграфе и путь w есть нетривиальное \widehat{C} -расширение пути $w_0(u, v)$. При $0 \leq u < d_m$ путь w является \widehat{C} -расширением одного из путей $w_1(u, v), \dots, w_{\tau(u)}(u, v)$. Следовательно, при $u \geq v$ формулы верны. Лемма 2 доказана.

2. Точные формулы экспонентов орграфа $\Gamma(g)$

Определим элементарные локальные экспоненты орграфа $\Gamma(g)$, где $g \in R(n, m)$ (для краткости $\Gamma(g) = \Gamma$). По определению локальный экспонент (u, v) -ехр Γ есть наименьшее натуральное число γ такое, что $W(u, v)$ содержит пути длины t при любом $t \geq \gamma$ [10]. Обозначая для краткости (u, v) -ехр $\Gamma = \gamma_{u,v}$, запишем

$$\gamma_{u,v} = 1 + \max \overline{\Lambda W}(u, v), \quad 0 \leq u, v < n, \quad (2)$$

$$\exp \Gamma(g) = \max_{0 \leq u, v < n} \gamma_{u,v}. \quad (3)$$

Если $u = v = n - 1$, то положим $\gamma_{n-1, n-1} = 1$.

Теорема 1. Пусть орграф $\Gamma(g)$ примитивный.

(а) Если $d_m = n - 1$, то

$$\gamma_{u,v} = \begin{cases} n - v - 1, & \text{если } u = n - 1, v < u, \\ l_{\tau(u)}(u, v), & \text{если } u < n - 1. \end{cases}$$

(б) Если $d_m < n - 1$, то

$$\gamma_{u,v} = \begin{cases} u - v + F(n - D(g)) + 1, & \text{если } d_m \leq u \leq n - 1, \\ \max_{t=1}^{\tau(u)} \bigcap \{ \{ \overline{\langle n - D(g) \rangle} + l_t(u, v) + 1 \} \\ \cup Z[l_{\tau(u)}(u, v), l_t(u, v)] \}, & \text{если } 0 \leq u < d_m. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Из (2) и лемм 1 и 2 получаем, что если $v \leq u$ и $d_m \leq u < n$, то

$$\begin{aligned} \gamma_{u,v} &= 1 + \max \overline{u - v + \langle n - D(g) \rangle} \\ &= 1 + u - v + \max \overline{\langle n - D(g) \rangle} = 1 + u - v + F(n - D(g)), \end{aligned}$$

так как по определению чисел Фробениуса $F(n - D(g)) = \max \overline{\langle n - D(g) \rangle}$. В частности, отсюда при $u = d_m = n - 1$ имеем $\langle n - D(g) \rangle = Z[0, \dots)$, $F(n - D(g)) = -1$; тогда $\gamma_{n-1, v} = n - v - 1$.

Пусть $0 \leq u < d_m$. Если $u < v$, то из (1) и лемм 1 и 2 следует, что

$$\overline{\Lambda W}(u, v) = \overline{L(u, v) + \langle n - D(g) \rangle} \\ = \bigcap_{t=1}^{\tau(u)} \{ \{ \overline{\langle n - D(g) \rangle} + l_t(u, v) \} \cup Z[0, l_t(u, v) - 1] \}. \quad (4)$$

Значит, $Z[0, l_{\tau(u)}(u, v) - 1] \subseteq \overline{\Lambda W}(u, v)$ в силу упорядоченности $l_1(u, v) > \dots > l_{\tau(u)}(u, v)$. Отсюда $\max \overline{\Lambda W}(u, v) \geq l_{\tau(u)}(u, v) - 1$, и из равенства (4) имеем

$$\max \overline{\Lambda W}(u, v) = \max \bigcap_{t=1}^{\tau(u)} \{ \{ \overline{\langle n - D(g) \rangle} + l_t(u, v) \} \\ \cup Z[l_{\tau(u)}(u, v) - 1, l_t(u, v) - 1] \}, \quad (5)$$

откуда в силу (2) получаем формулу для $\gamma_{u,v}$.

В соответствии с определением $l_t(u, v) - 1 = n - d_t - 1 + u - v$, значит, $l_t(u, v) - 1 > u - v$ тогда и только тогда, когда $d_t < n - 1$, и $l_t(u, v) - 1 = u - v$ при $d_t = n - 1$, $t \in \{1, \dots, \tau(u)\}$. Значит, в силу упорядоченности $0 = d_1 < \dots < d_m \leq n - 1$ равенство $l_t(u, v) - 1 = u - v$ верно только при $t = m$ и $d_m = n - 1$. Тогда $\max \overline{\Lambda W}(u, v) > u - v$, если $v \leq u < d_m$ и $d_m < n - 1$. Следовательно, формула (5) для (u, v) -exp $\Gamma(g)$ верна при $d_m < n - 1$, $0 \leq u < d_m$.

Если $d_m = n - 1$ и $u < v$, то в силу того, что $\langle n - D(g) \rangle = Z[0, \dots]$, получаем

$$\max \overline{\Lambda W}(u, v) = \max \bigcap_{t=1}^{\tau(u)} \{ \{ \overline{Z[0, \dots]} + l_t(u, v) \} \\ \cup Z[l_{\tau(u)}(u, v) - 1, l_t(u, v) - 1] \} = l_{\tau(u)}(u, v) - 1.$$

Если $v \leq u < d_m$, то $u - v < l_{\tau(u)}(u, v) - 1$, откуда также $\max \overline{\Lambda W}(u, v) = l_{\tau(u)}(u, v) - 1$. Следовательно, в соответствии с (2) при $d_m = n - 1$ в обоих случаях $\gamma_{u,v} = l_{\tau(u)}(u, v)$. Теорема 1 доказана.

Получим формулу экспонента орграфа $\Gamma(g)$. При фиксированном u рассмотрим $\gamma_{u,v}$ как функцию от v , определённую на $\{0, \dots, n - 1\}$.

Лемма 3. При $d_m < n - 1$ и любом фиксированном u функция $\gamma_{u,v}$ монотонно убывает.

ДОКАЗАТЕЛЬСТВО. При $d_m \leq u < n$ лемма непосредственно следует из теоремы 1.

Пусть $0 \leq u < d_m$. По условию леммы величина $\tau(u)$ фиксирована и $l_t(u, v) + 1 = l_t(u, v - 1)$. Тогда из теоремы 1 следует, что $\gamma_{u,v}$ монотонно убывает по v . Лемма 3 доказана.

Обозначим:

- $d_{m+1} = n - 1$, $D_{[s]} = \{d_1, \dots, d_{s-1}\}$, $s = 2, \dots, m$;
- $\Delta(D) = \max\{d_2 - d_1, \dots, d_m - d_{m-1}, d_{m+1} - d_m\}$;
- $E(D) = \{d_2 - 1, \dots, d_m - 1, d_{m+1} - 1\}$ ($E(D) = \{d_2 - 1, \dots, d_m - 1\}$ при $d_m = n - 1$).

Лемма 4. (а) $\max_{0 \leq u < n-1} \{u - d_{\tau(u)}\} = \max_{u \in E(D)} \{u - d_{\tau(u)}\} = \Delta(D) - 1$;

(б) $\max_{0 \leq u < d_s} \{u - d_{\tau(u)}\} = \max_{u \in E(D_{[s]})} \{u - d_{\tau(u)}\} = \Delta(D_{[s]}) - 1$.

ДОКАЗАТЕЛЬСТВО. Если $d_r \leq q \leq u$, то $q - d_r \leq u - d_r$, и в силу определения числа $\tau(u)$

$$\begin{aligned} \max_{0 \leq u < n-1} \{u - d_{\tau(u)}\} &= \max_{u \in E(D)} \{u - d_{\tau(u)}\} \\ &= \max\{d_2 - d_1 - 1, \dots, d_m - d_{m-1} - 1, n - 2 - d_m\} = \Delta(D) - 1. \end{aligned}$$

Равенство (б) доказывается аналогично. Лемма 4 доказана.

Теорема 2. Пусть орграф $\Gamma(g)$ примитивный. Тогда

$$\exp \Gamma(g) = \begin{cases} n + \Delta(D) - 1, & \text{если } d_m = n - 1, \\ \max\{\gamma_{d_2-1,0}, \dots, \gamma_{d_m-1,0}\}, & \text{если } d_m < n - 1, \end{cases}$$

где $\gamma_{d_s-1,0} = n + \max_{t=1}^{s-1} \{\overline{\langle n - D(g) \rangle} + d_s - d_t\} \cup Z[d_s - d_{s-1} - 1, d_s - d_t - 1]$,
 $s = 2, \dots, m$.

ДОКАЗАТЕЛЬСТВО. При $d_m = n - 1$ в соответствии с (3), теоремой 1 и леммой 3 имеем

$$\exp \Gamma(g) = \max\{\gamma_{n-1,0}, \max_{0 \leq u < n-1} l_{\tau(u)}(u, 0)\} = \max_{0 \leq u < n-1} l_{\tau(u)}(u, 0),$$

так как $\gamma_{n-1,0} = n - 1 < n = l_1(0, 0) = \gamma_{0,0}$.

По определению числа $l_{\tau(u)}(u, 0)$ получаем

$$\max_{0 \leq u < n-1} l_{\tau(u)}(u, 0) = n + \max_{0 \leq u < n-1} \{u - d_{\tau(u)}\}.$$

Отсюда и из леммы 4 следует нужная формула.

Пусть $d_m < n - 1$. Тогда в силу (3) и леммы 3

$$\exp \Gamma(g) = \max\left\{\max_{d_m \leq u \leq n-1} u + F(n - D(g)) + 1, \max_{0 \leq u < d_m} \gamma_{u,0}\right\} = \max_{0 \leq u < d_m} \gamma_{u,0},$$

так как $\gamma_{0,0} = n + 1 + F(n - D(g)) > n + F(n - D(g))$. Далее, если $0 \leq q < u < d_m$ и $\tau(q) = \tau(u)$, то из теоремы 1 вытекает, что $\gamma_{u,0} - \gamma_{q,0} = u - q > 0$. Значит, $\max_{0 \leq u < d_m} \gamma_{u,0} = \max_{u \in E(D_{[m]})} \gamma_{u,0}$. Отсюда и из теоремы 1

имеем $\exp \Gamma(g) = \max\{\gamma_{d_2-1,0}, \dots, \gamma_{d_m-1,0}\}$, где выражение для $\gamma_{d_s-1,0}$ следует из теоремы 1. Теорема 2 доказана.

3. Упрощение формул экспонентов при $d_m = n - 2$

Получим формулы для чисел $\gamma_{u,v}$ и $\exp \Gamma(g)$ при $d_m = n - 2$. По условию $\Gamma(g)$ содержит контур длины 2 и в силу примитивности орграфа $\Gamma(g)$ содержит контур нечётной длины.

Обозначим через $n - d_\mu$ наименьшую нечётную длину контура в $\Gamma(g)$. Тогда d_μ есть наибольшее число множества $D(g)$, чётность которого не совпадает с чётностью числа n .

Заметим, что при $d_m = n - 2$ множество $D(g)$ содержит нечётные числа, т. е. $I(D(g)) \neq \emptyset$. Действительно, если n нечётное, то число $n - 2 \in D(g)$ также нечётное; если n чётное, то оба множества $n - D(g)$ и $D(g)$ содержат хотя бы одно нечётное число в силу примитивности орграфа $\Gamma(g)$.

Обозначим $d_\lambda = \min I(D(g))$ и определим условия при фиксированных v и u , где $u < n - 1$, при которых множество $L(u, v)$ разбивается на подмножества чётных и нечётных чисел $J(L(u, v))$ и $I(L(u, v))$ соответственно.

Лемма 5. При $u < n - 1$ оба множества $I(L(u, v))$ и $J(L(u, v))$ непустые тогда и только тогда, когда $u \geq d_\lambda$.

ДОКАЗАТЕЛЬСТВО. Множество $L(u, v)$ состоит из чисел $u - d_t + n - v$, $t = 1, \dots, \tau(u)$, $u < n - 1$. Следовательно, при $u \geq d_\lambda$ множество $L(u, v)$ содержит числа $n - d_\lambda + u - v$ и $n + u - v$, которые по определению имеют различную чётность. Если $u < d_\lambda$, то чётность любого числа из $L(u, v)$ совпадает с чётностью числа $u + n - v$. Лемма 5 доказана.

Для множеств $I(L(u, v))$ и $J(L(u, v))$, $0 \leq u < n - 1$, $0 \leq v < n$, введём обозначения:

- $T_0(u, v) = \{1 \leq t \leq \tau(u) \mid l_t(u, v) \in J(L(u, v))\}$, где $T_0(u, v) = \emptyset$ при $J(L(u, v)) = \emptyset$;
- $T_1(u, v) = \{1 \leq t \leq \tau(u) \mid l_t(u, v) \in I(L(u, v))\}$, где $T_1(u, v) = \emptyset$ при $I(L(u, v)) = \emptyset$;
- $H_0(u, v) = \bigcap_{t \in T_0(u, v)} \{\overline{\{n - D(g)\}} + l_t(u, v)\} \cup Z[l_{\tau(u)}(u, v) - 1, l_t(u, v) - 1]$,
где $H_0(u, v) = \emptyset$ при $J(L(u, v)) = \emptyset$;
- $H_1(u, v) = \bigcap_{t \in T_1(u, v)} \{\overline{\{n - D(g)\}} + l_t(u, v)\} \cup Z[l_{\tau(u)}(u, v) - 1, l_t(u, v) - 1]$,
где $H_1(u, v) = \emptyset$ при $I(L(u, v)) = \emptyset$;
- $l^0(u, v) = \min J(L(u, v))$, если $J(L(u, v)) \neq \emptyset$;
- $l^1(u, v) = \min I(L(u, v))$, если $I(L(u, v)) \neq \emptyset$;
- $\chi(u, v) = |l^1(u, v) - l^0(u, v)|$.

При $u \geq d_\lambda$ выполнены следующие свойства:

(1°) величины $l^0(u, v)$ и $l^1(u, v)$ существуют и

$$l_{\tau(u)} = \min\{l^0(u, v), l^1(u, v)\};$$

(2°) величина $\chi(u, v)$ существует, не зависит от v и равна $|\mu(u) - \eta(u)|$, где $\mu(u)$ и $\eta(u)$ — наибольшие числа различной чётности множества $\{d_1, \dots, d_{\tau(u)}\}$.

Свойство (2°) вытекает из того, что

$$|l^1(u, v) - l^0(u, v)| = |n - \eta(u) + u - v - n + \mu(u) - u + v| = |\mu(u) - \eta(u)|.$$

Далее пишем $\chi(u, v) = \chi(u)$.

Теорема 3. Если орграф $\Gamma(g)$ примитивный, $n \geq 3$, то при $d_m = n - 2$

$$\gamma_{u,v} = \begin{cases} 2n - d_\mu - v - 2, & \text{если } u = n - 1, \\ 2n - d_\mu - v - 1 + u - d_{\tau(u)}, & \text{если } u < d_\lambda, \\ n + \min\{n - d_\mu, \chi(u)\} - v - 1 + u - d_{\tau(u)}, & \text{если } d_\lambda \leq u < n - 1. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Пусть для краткости $n - d_\mu = k$. Тогда

$$\langle n - D(g) \rangle = \langle 2, k \rangle = J[0, k - 1] \cup Z[k, \dots],$$

$$\overline{\langle n - D(g) \rangle} = I[1, k - 2],$$

$$\max \overline{\langle n - D(g) \rangle} = F(n - D(g)) = k - 2.$$

Отсюда и из теоремы 1(б) получаем

$$\gamma_{n-1,v} = n - v + k - 2 = 2n - v - d_\mu - 2.$$

Пусть $u < n - 1$. Тогда из (5) и теоремы 1(б) следует, что

$$\gamma_{u,v} = \begin{cases} 1 + \max\{H_0(u, v) \cap H_1(u, v)\}, & \text{если } u \geq d_\lambda, \\ 1 + \max H_0(u, v), & \text{если } u < d_\lambda, I(L(u, v)) = \emptyset, \\ 1 + \max H_1(u, v), & \text{если } u < d_\lambda, J(L(u, v)) = \emptyset. \end{cases} \quad (6)$$

Поскольку $d_m = n - 2$, ввиду леммы 5 с учётом равенства $\overline{\langle n - D(g) \rangle} = I[1, k - 2]$ для множеств $H_0(u, v)$ и $H_1(u, v)$ получаем

$$H_0(u, v) = Z[l_{\tau(u)}(u, v) - 1, l^0(u, v) - 1] \cup I[l^0(u, v) + 1, l^0(u, v) + k - 2], \quad (7)$$

$$H_1(u, v) = Z[l_{\tau(u)}(u, v) - 1, l^1(u, v) - 1] \cup J[l^1(u, v) + 1, l^1(u, v) + k - 2]. \quad (8)$$

Если $u < d_\lambda$ и $I(L(u, v)) = \emptyset$, то $l_{\tau(u)}(u, v) = l^0(u, v)$, и в соответствии с (6) и (7) имеем

$$H_0(u, v) = I[l^0(u, v) - 1, l^0(u, v) + k - 2], \quad \gamma_{u,v} = l^0(u, v) + k - 1.$$

Если $u < d_\lambda$ и $J(L(u, v)) = \emptyset$, то $l_{\tau(u)}(u, v) = l^1(u, v)$, и в силу (6) и (8) получаем

$$H_1(u, v) = J[l^1(u, v) - 1, l^1(u, v) + k - 2], \quad \gamma_{u,v} = l^1(u, v) + k - 1.$$

Следовательно, при $u < d_\lambda$ в обоих случаях

$$\gamma_{u,v} = l_{\tau(u)}(u, v) + k - 1 = 2n - d_\mu - v - 1 + u - d_{\tau(u)}.$$

Пусть $u \geq d_\lambda$. Тогда ввиду свойства (1°) и чётности чисел $l^0(u, v)$ и $l^1(u, v)$ либо $l^1(u, v) = l^0(u, v) + 2c - 1$, либо $l^0(u, v) = l^1(u, v) + 2c - 1$, где $c \in N$. В обоих случаях $\chi(u) = 2c - 1$.

В первом случае $l_{\tau(u)}(u, v) = l^0(u, v)$, а значит,

$$H_0(u, v) = I[l^0(u, v) - 1, l^0(u, v) + k - 2],$$

$$H_1(u, v) = Z[l^0(u, v) - 1, l^1(u, v) - 1] \cup J[l^1(u, v) + 1, l^1(u, v) + k - 2].$$

Множества $I[l^0(u, v) - 1, l^0(u, v) + k - 2]$ и $J[l^1(u, v) + 1, l^1(u, v) + k - 2]$ содержат числа различной чётности. Следовательно, в соответствии с (6)

$$\gamma_{u,v} = \max\{Z[l^0(u, v), l^1(u, v)] \cap J[l^0(u, v), l^0(u, v) + k - 1]\}.$$

Значит, $\gamma_{u,v} = l^0(u, v) + k - 1$, если $k \leq \chi(u)$, или $\gamma_{u,v} = l^1(u, v) - 1 = l^0(u, v) + 2c - 2$, если $k > \chi(u)$. Стало быть, в первом случае

$$\gamma_{u,v} = l_{\tau(u)}(u, v) - 1 + \min\{k, \chi(u)\}.$$

Во втором случае $l_{\tau(u)}(u, v) = l^1(u, v)$, а значит,

$$H_0(u, v) = Z[l^1(u, v) - 1, l^0(u, v) - 1] \cup I[l^0(u, v) + 1, l^0(u, v) + k - 2],$$

$$H_1(u, v) = J[l^1(u, v) - 1, l^1(u, v) + k - 2].$$

Следовательно, ввиду (6)

$$\gamma_{u,v} = \max\{Z[l^1(u, v), l^0(u, v)] \cap I[l^1(u, v), l^1(u, v) + k - 1]\}.$$

Тогда $\gamma_{u,v} = l^1(u, v) + k - 1$, если $k \leq \chi(u)$, или $\gamma_{u,v} = l^0(u, v) - 1 = l^1(u, v) + 2c - 2$, если $k > \chi(u)$. Стало быть, во втором случае также

$$\gamma_{u,v} = l_{\tau(u)}(u, v) - 1 + \min\{k, \chi(u)\}.$$

Итак, при $u \geq d_\lambda$ имеем

$$\gamma_{u,v} = l_{\tau(u)}(u, v) - 1 + \min\{k, \chi(u)\} = n + \min\{n - d_\mu, \chi(u)\} - \nu - 1 + u - d_{\tau(u)}.$$

Теорема 3 доказана.

Следствие 1. Если оргграф $\Gamma(g)$ примитивен, $n \geq 3$, то при $d_m = n - 2$

$$\exp \Gamma(g) = \begin{cases} 2n - d_\mu - 2 + \Delta(D_{[m]}), & \text{если } d_\lambda = d_m, \\ 2n - d_\mu - 2 + \max\{\Delta(D_{[\lambda]}), p_\lambda, \dots, p_{m-1}\}, & \text{если } d_\lambda < d_m, \end{cases}$$

где $p_s = d_{s+1} - d_s + \min\{0, \chi(d_s) - n + d_\mu\}$, $s = \lambda, \dots, m - 1$.

ДОКАЗАТЕЛЬСТВО. Если $d_\lambda = d_m$, то в соответствии с теоремой 2 $\exp \Gamma(g) = \max\{\gamma_{d_2-1,0}, \dots, \gamma_{d_m-1,0}\}$. Тогда по теореме 3 и лемме 4(б)

$$\exp \Gamma(g) = 2n - d_\mu - 1 + \max_{\substack{u \in \{d_2-1, \\ \dots, d_m-1\}}} \{u - d_{\tau(u)}\} = 2n - d_\mu - 2 + \Delta(D_{[m]}).$$

Пусть $d_\lambda < d_m$. В силу теоремы 2 имеем $\exp \Gamma(g) = \max\{a, b\}$, где

$$a = \max\{\gamma_{d_2-1,0}, \dots, \gamma_{d_\lambda-1,0}\}, \quad b = \max\{\gamma_{d_{\lambda+1}-1,0}, \dots, \gamma_{d_m-1,0}\}.$$

Тогда по теореме 3 и лемме 4(б)

$$a = 2n - d_\mu - 1 + \max_{\substack{u \in \{d_2-1, \\ \dots, d_\lambda-1\}}} \{u - d_{\tau(u)}\} = 2n - d_\mu - 2 + \Delta(D_{[\lambda]}),$$

$$b = n - 2 + \max\{d_{\lambda+1} - d_\lambda + \min\{n - d_\mu, \chi(d_{\lambda+1} - 1)\}, \\ \dots, d_m - d_{m-1} + \min\{n - d_\mu, \chi(d_m - 1)\}\}.$$

Отсюда, учитывая, что $\chi(d_s - 1) = \chi(d_{s-1})$, $s = \lambda + 1, \dots, m$, получаем

$$b = 2n - d_\mu - 2 + \max\{p_\lambda, \dots, p_{m-1}\}.$$

Следствие 1 доказано.

4. Оценки экспонента и примеры

Если вычисление точного значения $\exp \Gamma(g)$ является сложной задачей, то можно использовать оценки величины $\exp \Gamma(g)$.

Теорема 4. Если оргграф $\Gamma(g)$ примитивный, то при $d_m < n - 2$

$$F(n - D(g)) + n + d_2 \leq \exp \Gamma(g) \leq F(n - D(g)) + n + \Delta(D).$$

ДОКАЗАТЕЛЬСТВО. В соответствии с теоремами 1 и 2 при $d_m < n - 2$ $\exp \Gamma(g) \geq \gamma_{d_2-1,0} = F(n - D(g)) + l_1(d_2 - 1, 0) + 1 = F(n - D(g)) + n + d_2$.

По определению $\Delta(D) = d_r - d_{r-1}$, где $2 \leq r \leq m$, или $\Delta(D) = n - 1 - d_m$.

В первом случае в соответствии с теоремой 1 верна следующая оценка при $u = d_r - 1$:

$$\exp \Gamma(g) \leq \max \overline{\langle n - D(g) \rangle} + l_{\tau(u)}(u, 0) + 1,$$

где правая часть неравенства равна $F(n - D(g)) + n + \Delta(D)$.

При $\Delta(D) = n - 1 - d_m$ согласно теореме 1 верна оценка при $u = n - 2$:

$$\exp \Gamma(g) \leq \max \overline{\langle n - D(g) \rangle} + l_{\tau(u)}(u, 0) + 1,$$

где правая часть неравенства также равна $F(n - D(g)) + n + \Delta(D)$. Теорема 4 доказана.

Следствие 2. Если $\Delta(D) = d_2$, то $\exp \Gamma(g) = n + d_2 + F(n - D(g))$.

ДОКАЗАТЕЛЬСТВО следует из двусторонней оценки теоремы 4.

Вычислим $\exp \Gamma(g)$ для нескольких регистровых преобразований.

Пример 1. Длина регистра $n = 7$, $D(g) = \{0, 3, 4\}$. Вычисляем $\Delta(D) = d_2 = 3$, $7 - D(g) = \{3, 4, 7\}$. Орграф $\Gamma(g)$ примитивный, далее, $F(3, 4, 7) = F(3, 4) = 5$, откуда $\exp \Gamma(g) = 15$ по следствию 2.

Пример 2. Длина регистра $n = 8$, $D(g) = \{0, 2, 3\}$. Вычисляем $d_2 = 2$, $8 - D(g) = \{5, 6, 8\}$, $\Delta(D) = 3$. Орграф $\Gamma(g)$ примитивный, $\overline{\langle 8 - D(g) \rangle} = \{1, 2, 3, 4, 7, 9\}$, число Фробениуса $F(5, 6, 8) = 9$. Тогда по теореме 4 имеем $19 \leq \exp \Gamma(g) \leq 20$.

По теореме 2 получаем, что $\exp \Gamma(g) = \max\{\gamma_{1,0}, \gamma_{2,0}\}$. Вычисляем, используя теорему 1:

$$\begin{aligned} l_1(1, 0) &= 1 + 8 = 9, \quad \gamma_{1,0} = \max\{9, 11, 12, 13, 14, 17, 19\} = 19, \\ l_1(2, 0) &= 2 + 8 = 10, \quad l_2(2, 0) = 8, \\ \gamma_{2,0} &= \max\{\{\dots, 14, 15, 18, 20\} \cap \{\dots, 12, 13, 16, 18\}\} = 18. \end{aligned}$$

Следовательно, $\exp \Gamma(g) = \max\{19, 18\} = 19$.

Пример 3. Длина регистра $n = 11$, $D(g) = \{0, 2, 6\}$. Вычисляем $d_2 = 2$, $11 - D(g) = \{5, 9, 11\}$, $\Delta(D) = 4$. Орграф $\Gamma(g)$ примитивный, $\overline{\langle 11 - D(g) \rangle} = \{1, 2, 3, 4, 6, 7, 8, 12, 13, 17\}$, $F(5, 9, 11) = 17$. Тогда по теореме 4 имеем $30 \leq \exp \Gamma(g) \leq 32$.

По теореме 2 получаем, что $\exp \Gamma(g) = \max\{\gamma_{1,0}, \gamma_{5,0}\}$. Вычисляем, используя теорему 1:

$$\begin{aligned} l_1(1, 0) &= 12, \quad \gamma_{1,0} = \max\{14, 15, 16, 17, 19, 20, 21, 25, 26, 30\} = 30, \\ l_1(5, 0) &= 16, \quad l_2(5, 0) = 14, \\ \gamma_{5,0} &= \max\{\{\dots, 21, 23, 24, 25, 29, 30, 34\} \cap \{\dots, 22, 23, 27, 28, 32\}\} = 23. \end{aligned}$$

Следовательно, $\exp \Gamma(g) = \max\{30, 23\} = 30$.

Пример 4. Длина регистра $n = 7$, $D(g) = \{0, 2, 5\}$. Вычисляем $d_2 = 2$, $7 - D(g) = \{2, 5, 7\}$, $\Delta(D) = 3$. Орграф $\Gamma(g)$ примитивный, $\overline{\langle 7 - D(g) \rangle} = \{1, 3\}$, $F(2, 5, 7) = 3$. Тогда по теореме 4 имеем $12 \leq \exp \Gamma(g) \leq 13$.

По теореме 2 получаем, что $\exp \Gamma(g) = \max\{\gamma_{1,0}, \gamma_{4,0}\}$. Вычисляем, используя теорему 1:

$$\begin{aligned} l_1(1, 0) &= 8, \quad \gamma_{1,0} = \max\{8, 10, 12\} = 12, \\ l_1(4, 0) &= 11, \quad l_2(4, 0) = 9, \\ \gamma_{4,0} &= \max\{\{9, 10, 11, 13, 15\} \cap \{9, 11, 13\}\} = 13. \end{aligned}$$

Следовательно, $\exp \Gamma(g) = \max\{12, 13\} = 13$.

Найдём $\exp \Gamma(g)$, используя следствие 1. Вычисляем $d_\mu = 2$, $d_\lambda = d_m = 5$, $D_{[m]} = \{0, 2\}$, $\Delta(D_{[m]}) = 3$. Тогда $\exp \Gamma(g) = 14 - 2 - 2 + 3 = 13$.

Пример 5. Длина регистра $n = 8$, $D(g) = \{0, 1, 6\}$. Найдём $\exp \Gamma(g)$, используя следствие 1. Вычисляем $d_\mu = d_\lambda = 1$, $d_m = 6$. Тогда при $d_\lambda < d_m$ находим $D_{[\lambda]} = \{0\}$, $\Delta(D_{[\lambda]}) = 1$, $\chi(d_2) = 1$ и $p_2 = 6 - 1 + \min\{0, 1 - 8 + 1\} = -1$. В итоге $\exp \Gamma(g) = 16 - 1 - 2 + \max\{1, -1\} = 14$.

Замечание. Для более широкого класса преобразований векторных пространств, отличных от регистровых, задача получения компактной аналитической формулы экспонента перемешивающих орграфов представляется весьма сложной. Определение формулы точных значений локальных экспонентов и экспонента орграфа сводится к задаче переборного характера описания в орграфе множества путей определённых длин.

ЛИТЕРАТУРА

1. **Frobenius G.** Über Matrizen aus nicht negativen Elementen // Berl. Ber. 1912. S. 456–477. [German].
2. **Dulmage A. L., Mendelsohn N. S.** The exponent of a primitive matrix // Can. Math. Bull. 1962. Vol. 5, No. 3. P. 241–244.
3. **Фомичёв В. М., Авезова Я. Э., 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.
4. **Фомичёв В. М.** Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
5. **Протасов В. Ю.** Полугруппы неотрицательных матриц // Успехи мат. наук. 2010. Т. 65, вып. 6. С. 191–192.
6. **Protasov V. Yu., Voynov A. S.** Sets of nonnegative matrices without positive products // Linear Algebra Appl. 2012. Vol. 437, No. 3. P. 749–765.
7. **Voynov A. S.** Shortest positive products of nonnegative matrices // Linear Algebra Appl. 2013. Vol. 439, No. 6. P. 1627–1634.
8. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. Vol. 14, No. 4. P. 483–499.
9. **Liu B.** Generalized exponents of Boolean matrices // Linear Algebra Appl. 2003. Vol. 373. P. 169–182.
10. **Фомичёв В. М., Кяжин С. Н.** Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24, № 1. С. 97–119.

11. **Wielandt H.** Unzerlegbare, nicht negative Matrizen // Math. Z. 1950. Bd. 52. S. 642–648. [German].
12. **Perkins P.** A theorem on regular graphs // Pac. J. Math. 1961. Vol. 11, No. 4. P. 1529–1533.
13. **Dulmage A. L., Mendelsohn N. S.** Gaps in the exponent set of primitive matrices // Ill. J. Math. 1964. Vol. 8, No. 4. P. 642–656.
14. **Neufeld S. W.** A diameter bound on the exponent of a primitive directed graph // Linear Algebra Appl. 1996. Vol. 245. P. 27–47.
15. **Князев А. В.** Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов // Дис. ... докт. физ.-мат. наук: 01.01.09. Москва, 2002. 203 с.
16. **Фомичёв В. М.** Новая универсальная оценка экспонентов графов // Прикл. дискрет. математика. 2016. № 3. С. 78–84.
17. **Фомичёв В. М.** Об улучшенной универсальной оценке экспонентов орграфов // Прикл. дискрет. математика. 2019. № 43. С. 115–123.
18. **Golomb S. W.** Shift register sequences – A retrospective account // Sequences and Their Applications – SETA 2006. Proc. 4th Int. Conf. (Beijing, China, Sept. 24–28, 2006). Heidelberg: Springer, 2012. P. 1–4 (Lect. Notes Comput. Sci.; Vol. 4086).
19. **Goresky M., Klapper A.** Algebraic shift register sequences. Cambridge: Camb. Univ. Press, 2012. 514 p.
20. **Солодовников В. И.** Регистры сдвига и криптоалгоритмы на их основе. Саарбрюккен: Lambert Acad. Publ., 2017. 112 с.

Фомичёв Владимир Михайлович
Авезова Яна Эдуардовна

Статья поступила
6 сентября 2019 г.
После доработки —
27 сентября 2019 г.
Принята к публикации
19 февраля 2020 г.

EXACT FORMULA FOR EXPONENTS OF MIXING DIGRAPHS FOR REGISTER TRANSFORMATIONS

V. M. Fomichev^{1,2,3,4,a} and Ya. E. Avezova^{2,b}

¹ Financial University under the Government of Russian Federation,
49 Leningradskii Avenue, 125993 Moscow, Russia

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

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

⁴ Security Code LLC,
10 Bld. 1 Pervyi Nagatinskii Driveway, 115230 Moscow, Russia

E-mail: ^afomichev.2016@yandex.ru, ^bavezovayana@gmail.com

Abstract. A digraph is primitive if some positive degree of it is a complete digraph, i. e. has all possible edges. The least degree of this kind is called the exponent of the digraph. Given a primitive digraph, the elementary local exponent for some vertices u and v is the least positive integer γ such that there exists a path from u to v of every length at least γ . For transformation on the binary n -dimensional vector space that is given by a set of n coordinate functions, the n vertex digraph corresponds such that a pair (u, v) is an edge if the v th coordinate component of transformation essentially depends on u th variable. Such a digraph we call a mixing digraph of transformation.

We study the mixing digraphs of widely used in cryptography n -bit shift registers with nonlinear Boolean feedback function (NFSR), $n > 1$. We find the exact formulas for the exponent and elementary local exponents for n -vertex primitive mixing digraph associated to NFSR. For pseudo-random sequences generators based on the NFSRs, our results can be applied to evaluate the length of blank run. Bibliogr. 20.

Keywords: mixing digraph, primitive digraph, locally primitive digraph, feedback shift register, exponent of a digraph.

REFERENCES

1. **G. Frobenius**, Über Matrizen aus nicht negativen Elementen, *Berl. Ber.*, 456–477 (1912) [German].
2. **A. L. Dulmage** and **N. S. Mendelsohn**, The exponent of a primitive matrix, *Can. Math. Bull.* **5** (3), 241–244 (1962).
3. **V. M. Fomichev**, **Ya. E. 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)].
4. **V. M. Fomichev**, *Methods of Discrete Mathematics in Cryptology* (Dialog-MIFI, Moscow, 2010) [Russian].
5. **V. Yu. Protasov**, Semigroups of non-negative matrices, *Usp. Mat. Nauk*, No. 6, 191–192 (2010) [Russian] [*Rus. Math. Surv.* **65** (6), 1186–1188 (2010)].
6. **V. Yu. Protasov** and **A. S. Voynov**, Sets of nonnegative matrices without positive products, *Linear Algebra Appl.* **437** (3), 749–765 (2012).
7. **A. S. Voynov**, Shortest positive products of nonnegative matrices, *Linear Algebra Appl.* **439** (6), 1627–1634 (2013).
8. **R. A. Brualdi** and **B. Liu**, Generalized exponents of primitive directed graphs, *J. Graph Theory* **14** (4), 483–499 (1990).
9. **B. Liu**, Generalized exponents of Boolean matrices, *Linear Algebra Appl.* **373**, 169–182 (2003).
10. **V. M. Fomichev** and **S. N. Kyazhin**, Local primitivity of matrices and graphs, *Diskretn. Anal. Issled. Oper.* **24** (1), 97–119 (2017) [Russian] [*J. Appl. Ind. Math.* **11** (1), 26–39 (2017)].
11. **H. Wielandt**, Unserlegbare, nicht negative Matrizen, *Math. Z.* **52**, 642–648 (1950) [German].
12. **P. Perkins**, A theorem on regular graphs, *Pac. J. Math.* **11** (4), 1529–1533 (1961).
13. **A. L. Dulmage** and **N. S. Mendelsohn**, Gaps in the exponent set of primitive matrices, *Ill. J. Math.* **8** (4), 642–656 (1964).
14. **S. W. Neufeld**, A diameter bound on the exponent of a primitive directed graph, *Linear Algebra Appl.* **245**, 27–47 (1996).
15. **A. V. Knyazev**, Estimations for extreme values of principal metric characteristics of pseudosymmetrical graphs, *Dr. Sci. Diss.* (VTs RAN, Moscow, 2016) [Russian].
16. **V. M. Fomichev** The new universal estimation for exponents of graphs, *Prikl. Diskretn. Mat.*, No. 3, 78–84 (2016) [Russian].
17. **V. M. Fomichev** On improved universal estimation of exponents of digraphs, *Prikl. Diskretn. Mat.*, No. 43, 115–123 (2019) [Russian].
18. **S. W. Golomb** Shift register sequences – A retrospective account, in *Sequences and Their Applications* (Proc. 4th Int. Conf. SETA–2006, Beijing, China, Sept. 24–28, 2006) (Springer, Heidelberg, 2012), pp. 1–4 (Lect. Notes Comput. Sci., Vol. 4086).

-
- 19. M. Goresky** and **A. Klapper**, *Algebraic Shift Register Sequences* (Camb. Univ. Press, Cambridge, 2012).
- 20. V. I. Solodovnikov**, *Shift Registers and Cryptographic Algorithms Based on Them* (Lambert Acad. Publ., Saarbrücken, 2017) [Russian].

Vladimir M. Fomichev
Yana E. Avezova

Received September 6, 2019
Revised September 27, 2019
Accepted February 19, 2020