ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.17 DOI 10.17223/20710410/55/5

О $\langle 2\rangle$-ЭКСПОНЕНТАХ ОРГРАФОВ НЕЛИНЕЙНОСТИ РЕГИСТРОВЫХ ПРЕОБРАЗОВАНИЙ

В. М. Фомичёв[*,**], В. М. Бобров[***]

[*] *Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*
[**] *Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, Россия*
[***] *Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия*

E-mail: fomichev.2016@yandex.ru, bvm_15@mail.ru

Матрично-графовый подход применяется для оценки множества существенных и нелинейных переменных координатных функций произведения преобразований векторных пространств. Для существенных переменных оценки получаются с помощью умножения двоичных перемешивающих матриц (или орграфов) умножаемых преобразований, для нелинейных переменных — с помощью умножения троичных матриц нелинейности умножаемых преобразований или соответствующих им орграфов нелинейности, дуги которых помечены числами множества $\{0, 1, 2\}$. Для степеней заданного преобразования область нетривиальных оценок ограничена: для множества существенных переменных — экспонентом перемешивающей матрицы (орграфа); для множества нелинейных переменных — $\langle 2\rangle$-экспонентом матрицы (орграфа) нелинейности. Для класса преобразований двоичных регистров сдвига получена достижимая оценка $\langle 2\rangle$-экспонентов, выраженная через длину регистра сдвига и множества номеров существенных и нелинейных переменных функции обратной связи. Для регистровых преобразований, орграф нелинейности которых имеет петлю, получена точная формула $\langle 2\rangle$-экспонента. Результаты могут быть использованы для оценки характеристик нелинейности криптографических функций, построенных на основе итераций регистровых преобразований.

Ключевые слова: *преобразование регистра сдвига, орграф нелинейности, $\langle 2\rangle$-примитивность, локальная $\langle 2\rangle$-примитивность, $\langle 2\rangle$-экспонент орграфа, локальный $\langle 2\rangle$-экспонент орграфа.*

$\langle 2\rangle$-EXPONENTS OF SHIFT REGISTER TRANSFORMATIONS NONLINEARITY DIPGRAPHS

V. M. Fomichev[*,**], V. M. Bobrov[***]

[*] *Financial University under the Government of the Russian Federation, Moscow, Russia*
[**] *Federal Research Center "Computer Science and Control", RAS, Moscow, Russia*
[***] *National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia*

The matrix-graph approach is used to estimate sets of essential and non-linear variables of coordinate functions of the vector space transformations product. Estimates are obtained by multiplying binary mixing matrices or digraphs of multiplied transformations in the case of the set of essential variables, or by multiplying ternary nonlinearity matrices or corresponding nonlinearity digraphs with the arcs marked by numbers from the set $\{0, 1, 2\}$. For powers of a given transformation the non-trivial estimates domain is limited by the mixing matrix (digraph) exponent in the case of the essential variables and by the nonlinearity matrix (digraph) $\langle 2\rangle$-exponent in the case of the nonlinear variables. Let $f(x_0, \ldots, x_{n-1})$ be the feedback function of shift register, $D = \{d_0, \ldots, d_m\}$ be the set of its essential variables (registers extraction points), $1 < m \leqslant n$, $0 = d_0 < d_1 < \ldots < d_m < n$, $E = \{e_0, \ldots, e_l\}$ be the set of its nonlinear variables (registers nonlinear extraction points), $1 < l \leqslant n$, $e_0 < e_1 < \ldots < e_m < n$, and shift register transformation nonlinearity digraph G be $\langle 2\rangle$-primitive. Then $\langle 2\rangle$-exponent of G is not greater than $F(L)+1+n+\Delta_f$, where $F(L)$ is a Frobenius number of the set L of the lengths of all digraph simple circuits, $\Delta_f = \max\limits_{i\in D^0\cup D^1} \mu(i-1)$,

$$\mu(u) = \begin{cases} \min\{u - e(u), u - d(u) + n - e_l\}, & e_0 \leqslant u < n; \\ u - d(u) + n - e_l, & 0 \leqslant u < e_0, \end{cases}$$

$$D^0 = \{d_s \in D, 1 \leqslant s \leqslant m : d_{s-1} - e(d_{s-1}) \leqslant \lambda, e_0 \leqslant d_{s-1} < n\} \cup S_0(n),$$

$$D^1 = \{d_s \in D, 1 \leqslant s \leqslant m : 0 \leqslant d_{s-1} < e_0 \text{ or } d_{s-1} - e(d_{s-1}) > \lambda\} \cup S_1(n),$$

where $d(u)$ is the greatest number of D such that $d(u) \leqslant u$, $0 \leqslant u < n$; $e(u)$ is the greatest number of E such that $e(u) \leqslant u$, $e_0 \leqslant u < n$; $S_0(n) = S_1(n) = \varnothing$, if $d_m = n - 1$; $S_0(n) = \{n\}$, if $d_m < n - 1$ and $d_m \in E$; and $S_1(n) = \{n\}$, if $d_m < n-1$ and $d_m \in E$. In the case of the variable x_{n-1} being essential for the function $f(x_0, \ldots, x_{n-1})$, the exact formula for the $\langle 2\rangle$-exponent of the nonlinearity digraph has been derived. Calculation examples are presented. The results can be used to estimate the nonlinearity characteristics of cryptographic functions constructed from iterated register transformations.

Keywords: *shift register transformation, nonlinearity digraph, $\langle 2\rangle$-primitivity, local $\langle 2\rangle$-primitivity, $\langle 2\rangle$-exponent of digraph, local $\langle 2\rangle$-exponent of digraph.*

Введение

Матрично-графовый подход (МГП) [1] позволяет оценить множества существенных переменных координатных функций произведения преобразований векторных пространств. Основой МГП является исследование двоичной перемешивающей матрицы $M = (m_{i,j})$ преобразования g (или его перемешивающего орграфа, что равносильно в силу биекции между множеством орграфов и множеством их матриц смежности), где $m_{i,j} = 1$, если j-я координатная функция преобразования g зависит от i-й переменной существенно, и $m_{i,j} = 0$ в противном случае. Известно, что перемешивающая матрица произведения преобразований ограничена сверху (поэлементно) произведением перемешивающих матриц умножаемых преобразований. Это позволяет оценивать характеристики произведения преобразований с помощью произведения перемешивающих матриц (орграфов) сомножителей. Область нетривиальности таких оценок для степеней преобразования g ограничена экспонентом его перемешивающей матрицы (орграфа). Получению оценок экспонентов неотрицательных матриц посвящено много российских и зарубежных работ, результаты достаточно полно отражены в обзоре [1].

Исследование экспонентов неотрицательных матриц началось с поставленной Фробениусом [2] задачи по распознаванию положительной матрицы среди элементов цик-

лической полугруппы $\langle M\rangle$, порождённой квадратной матрицей M с неотрицательными элементами. При наличии положительной матрицы порождающая матрица M называется примитивной, а наименьшая степень t, при которой M^t положительная, называется экспонентом матрицы M [3]. Критерий примитивности получен в [4]: сильносвязный орграф примитивен, если длины его контуров взаимно просты. Много работ посвящено получению как универсальных, так и частных оценок экспонентов неотрицательных матриц и орграфов.

В [5, 6] представлено расширение МГП, позволяющее оценивать характеристики нелинейности произведения преобразований. Исследуется троичная матрица нелинейности M_θ, в которой зависимость j-й координатной функции от x_i кодируется двумя значениями: $m_{ij} = 2$, если указанная зависимость нелинейная, и $m_{ij} = 1$, если линейная. Таким образом, по сравнению с перемешивающей матрицей матрица M_θ более глубоко оценивает свойства преобразований.

Множеству троичных матриц биективно соответствует множество помеченных орграфов, для которых эти матрицы являются матрицами смежности вершин, где дуга (i, j) орграфа помечена элементом $m_{i,j}$ матрицы. Графовая модель вместо произведения троичных матриц позволяет изучать пути в помеченных орграфах, что нередко технически более удобно.

Орграф нелинейности преобразования двоичного векторного пространства размерности n имеет множество вершин $\{0, \ldots, n-1\}$, $n > 1$, и множество дуг, кодирующих характер зависимости каждой координатной функции преобразования от каждой переменной [5, 6]. Дуга (i, j) орграфа помечена символом «1» или «2», если j-я координатная функция зависит от x_i соответственно линейно или нелинейно; если j-я координатная функция несущественно зависит от x_i, то в орграфе дуги (i, j) нет. В произведении помеченных орграфов Γ_1 и Γ_2 дуга (i, j) помечена символом $\max\{a, b\}$, если в Γ_1 и Γ_2 имеются дуги (i, k) и (k, j) соответственно, $0 \leqslant k < n$, одна из которых помечена символом a и другая — символом b, $a, b \in \{1, 2\}$. Помеченный орграф называется $\langle 2\rangle$-примитивным, если его некоторая степень есть полный орграф с петлями и каждая дуга имеет метку «2». Указанная степень называется $\langle 2\rangle$-экспонентом орграфа.

В криптографических системах сложное преобразование часто построено с помощью итерации более простого, но удобно реализуемого преобразования. В частности, в симметричных блочных шифрах количество раундов, требуемое для обеспечения перемешивающих и нелинейных свойств, оценивается снизу $\langle 2\rangle$-экспонентом орграфа нелинейности раундовой подстановки [6].

В работе изучена зависимость $\langle 2\rangle$-экспонента орграфа нелинейности регистрового преобразования векторного пространства от длины регистра сдвига и множеств номеров существенных и нелинейных переменных функции обратной связи. Эта задача решена с помощью развития метода получения точной формулы экспонента перемешивающих орграфов регистровых преобразований [7]. Начальные результаты в этом направлении представлены в [8].

Орграф нелинейности преобразования двоичного регистра левого сдвига длины n с нелинейной обратной связью (ячейки регистра нумеруются слева направо числами от 0 до $n-1$) представляет собой объединение нескольких контуров с общей вершиной $n-1$. Для класса помеченных $\langle 2\rangle$-примитивных орграфов нелинейности регистровых преобразований получены оценки $\langle 2\rangle$-экспонентов и локальных $\langle 2\rangle$-экспонентов, выраженные через длину регистра сдвига и множества номеров существенных и нелинейных переменных функции обратной связи. Для регистровых преобразований, орграф нелинейности которых имеет петлю, получены точные формулы $\langle 2\rangle$-экспонентов и ло-

кальных $\langle 2\rangle$-экспонентов. Приведены примеры вычислений. Случаи регистров правого и левого сдвигов рассматриваются двойственно.

1. Основные определения

Исследуем двоичный регистр левого сдвига длины $n > 2$ с нелинейной булевой функцией обратной связи $f(x_0, \ldots, x_{n-1})$. Ячейки регистра занумеруем слева направо числами $0, \ldots, n-1$.

Обозначим:

- V_n — множество двоичных векторов длины n (состояний регистра);
- $F(A)$ — число Фробениуса для множества натуральных аргументов A, где НОД$(A) = 1$, определяемое как наибольшее целое число, не содержащееся в аддитивной полугруппе, порождённой множеством A;
- $Y_n = \{0, \ldots, n-1\}$ — множество номеров ячеек регистра сдвига;
- ϕ_f — преобразование множества V_n, реализуемое нелинейным регистром левого сдвига с обратной связью f;
- $D = \{d_0, \ldots, d_m\} \subseteq Y_n$, где $0 < m \leqslant n-1$, — непустое множество номеров существенных переменных функции $f(x_0, \ldots, x_{n-1})$ (точек съёма регистра); далее считаем $0 = d_0 < d_1 < \ldots < d_m < n$ (условие $d_0 = 0$ не ограничивает общность рассуждений, так как в случае $d_0 > 0$ реальная длина регистра меньше n);
- $E = \{e_0, \ldots, e_l\}$ — множество номеров переменных, от которых функция обратной связи f зависит нелинейно (нелинейных точек съёма), отсюда $E \subseteq D$, $0 < l \leqslant m$, $0 \leqslant e_0 < e_l \leqslant d_m$;
- $d(u)$ — наибольшее число из D, такое, что $d(u) \leqslant u$, $0 \leqslant u < n$, число $d(u)$ существует для любого u в силу равенства $0 = d_0$;
- $e(u)$ — наибольшее число из E, такое, что $e(u) \leqslant u$, где $e_0 \leqslant u < n$; при $0 \leqslant u < e_0$ число $e(u)$ не существует; по определению $e(u) \leqslant d(u)$ для любого $u \geqslant e_0$;
- (i, j) — дуга в орграфе, инцидентная вершинам i и j, (i, j) — петля при $i = j$;
- $w(i, j)$ — путь в орграфе из i в j; $w(i, j)$ — путь нулевой длины при $i = j$;
- $\circ$ — операция конкатенации (присоединения) путей, где конечная вершина первого пути совпадает с начальной вершиной второго пути;
- $\Gamma(\phi_f)$ — перемешивающий орграф преобразования ϕ_f регистра сдвига, имеющий множество вершин Y_n, дуга (i, j) имеется в графе $\Gamma(\phi_f)$ тогда и только тогда, когда j-я координатная функция преобразования ϕ_f зависит от переменной x_i существенно, $0 \leqslant i, j < n$; заметим, что при $d_m = n-1$ граф $\Gamma(\phi_f)$ имеет петлю в вершине $n-1$;
- $\Gamma_\theta(\phi_f)$ — орграф нелинейности преобразования ϕ_f регистра сдвига, имеющий множество вершин Y_n, дуга (i, j) которого помечена символом $a_{i,j}$, равным 0, 1 или 2 тогда и только тогда, когда j-я координатная функция преобразования ϕ_f зависит от переменной x_i несущественно, линейно или нелинейно соответственно, $0 \leqslant i, j < n$.

2. Определяющие свойства помеченных орграфов

Напомним определения и свойства [5, 6, 8], связанные с орграфами.

Определим полугрупповую коммутативную операцию умножения на множестве $G = \{0, 1, 2\}$. Для любых $a, b \in G$ положим: $0a = 0$, $b = \max\{a, b\}$, если $a, b \in \{1, 2\}$.

На множестве помеченных n-вершинных орграфов определена операция умножения орграфов: если в Γ_0 имеется дуга (i, j) с меткой $m_0 \in G$ и в Γ_1 имеется дуга (j, k) с меткой $m_1 \in G$, то в орграфе $\Gamma_0\Gamma_1$ имеется дуга (i, k) с меткой $m_0 m_1 \in G$, где умножение меток выполняется в полугруппе G.

Меткой пути (контура) назовём наибольшую ненулевую метку всех дуг, составляющих данный путь (контур). Путь с меткой «2» назовём 2-путём.

Сильносвязный орграф Γ называется примитивным, если существует $\gamma \in \mathbb{N}$, такое, что орграф Γ^γ (с петлями) является полным. Наименьшее такое число γ обозначается $\exp\Gamma$ и называется экспонентом орграфа Γ [1].

Сильносвязный помеченный орграф Γ называется $\langle 2\rangle$-примитивным, если существует $\gamma \in \mathbb{N}$, такое, что орграф Γ^γ (с петлями) есть полный 2-граф, то есть полный граф, в котором каждая дуга имеет метку «2». Наименьшее такое число γ обозначается $\langle 2\rangle$-$\exp\Gamma$ и называется $\langle 2\rangle$-экспонентом орграфа Γ.

Орграф Γ $\langle 2\rangle$-примитивный тогда и только тогда, когда он примитивный и имеет дугу с меткой «2», при этом

$$\langle 2\rangle\text{-}\exp\Gamma \leqslant \max\{\omega_2, \delta_2\} + \exp\Gamma, \tag{1}$$

где в Γ обозначено: ω_2 — наибольшая из длин кратчайших 2-путей, исходящих из всех вершин; δ_2 — наибольшая из длин кратчайших 2-путей, заходящих во все вершины.

Орграф Γ называется $i\times j$-$\langle 2\rangle$-примитивным, если существует $\gamma \in \mathbb{N}$, такое, что для любого $t \geqslant \gamma$ в орграфе Γ^t метка дуги (i, j) есть «2». Наименьшее такое γ обозначается $\gamma_{i,j}^{[2]} = i \times j$-$\langle 2\rangle$-$\exp\Gamma$ и называется $i \times j$-$\langle 2\rangle$-экспонентом (локальным экспонентом) орграфа Γ [8]. Из данных определений следует, что

$$\langle 2\rangle\text{-}\exp\Gamma = \max_{0\leqslant i,j<n}\{i \times j\text{-}\langle 2\rangle\text{-}\exp\Gamma\}. \tag{2}$$

В связи с операцией в G определена операция умножения на множестве троичных матриц с элементами из полугруппы G. Если $A = (a_{i,j})$, $B = (b_{i,j})$, $AB = C = (c_{i,j})$, то

$$c_{i,j} = \max_{0\leqslant k<n}\{a_{i,k}b_{k,j}\},\ 0 \leqslant i < n,\ 0 \leqslant j < n,$$

где умножение элементов матриц выполняется в полугруппе G.

Матрица смежности вершин орграфа, дуги которого помечены символами «1» и «2», — это троичная матрица, где нулевой элемент в i-й строке и j-м столбце означает отсутствие дуги (i, j) в орграфе.

Матрица смежности произведения помеченных орграфов равна произведению троичных матриц смежности умножаемых орграфов. Если дуги (i, k) и (k, j) умножаемых орграфов помечены числами $a, b \in \{1, 2\}$, то в произведении орграфов дуга (i, j) имеет метку $\max\{a, b\}$. Орграф, в котором все дуги имеют метку «2», называется 2-графом.

В данной работе оценка (1) уточнена в терминах характеристик регистрового преобразования пространства V_n.

3. Свойства орграфа нелинейности регистра сдвига

Преобразование g множества V_n называется преобразованием регистра левого сдвига с обратной связью $f(x_0, \ldots, x_{n-1})$, если $g(x_0, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, f(x_0, \ldots, x_{n-1}))$.

Отметим свойства орграфа нелинейности $\Gamma_\theta(\phi_f)$ и функций, связанных с регистром сдвига. Для краткости используем обозначение $\Gamma_\theta(\phi_f) = \Gamma$.

Свойство 1. В соответствии с определением преобразования регистра сдвига множество дуг орграфа нелинейности Γ с меткой «1» равно

$$\{(1, 0), (2, 1), \ldots, (n-1, n-2)\} \cup \bigcup_{s\in D\setminus E}\{(s, n-1)\},$$

и множество дуг орграфа нелинейности Γ с меткой «2» — это

$$\bigcup_{s\in E}\{(s, n-1)\}.$$

Следовательно, орграф нелинейности Γ есть объединение $m+1$ контуров $C_0, \ldots, C_m$, где $C_s = (n-1, n-2, \ldots, d_s)$, $s = 0, \ldots, m-1$; $C_m = (n-1, \ldots, d_m)$, если $d_m < n-1$, и $C_m = (n-1)$ — петля в вершине $n-1$ при $d_m = n-1$. Отсюда следует:

— орграф Γ сильносвязный;

— контур C_s есть 2-контур тогда и только тогда, когда $d_s \in E$.

Свойство 2. Длина контура C_s равна $n - d_s$, $s = 0, \ldots, m$. Наименьшая из длин 2-контуров равна $(n - e_l)$, наименьшая — $(n - d_m)$.

Обозначим через L множество длин всех контуров орграфа Γ:

$$L = \{n, n-d_1, \ldots, n-d_m\}.$$

Отсюда следует, что орграф Γ примитивный тогда и только тогда, когда НОД$(L) = 1$. В частности, наличие петли в графе Γ достаточно для его примитивности.

Свойство 3. В силу нелинейности функции обратной связи примитивный орграф Γ является $\langle 2\rangle$-примитивным.

Свойство 4. Функции $d(u)$ и $e(u)$ монотонны по аргументу u на множествах $\{0, \ldots, n-1\}$ и $\{e_0, \ldots, n-1\}$ соответственно.

4. Оценка $\langle 2\rangle$-экспонента орграфа нелинейности

Получим сначала оценку $i \times j$-$\langle 2\rangle$-экспонента орграфа Γ.

Обозначим: $\gamma^{[2]} = \langle 2\rangle\text{-}\exp\Gamma$; $w(n-1, j)$ — путь длины $n-1-j$, являющийся частью контура C_0; C — кратчайший 2-контур длины $n - e_l$, пройденный из вершины $n-1$; $C'(t)$ — контур длины t, пройденный из вершины $n-1$ через некоторые контуры (возможно, неоднократно) орграфа Γ;

$$\mu(u) = \begin{cases} \min\{u - e(u), u - d(u) + n - e_l\}, & e_0 \leqslant u < n; \\ u - d(u) + n - e_l, & 0 \leqslant u < e_0. \end{cases}$$

Таким образом, $\mu(u)+1$ есть длина проходящего через дугу с меткой «2» кратчайшего пути из вершины u в вершину $n-1$, $u \in Y_n$.

Теорема 1. Если орграф Γ примитивный, то

$$\gamma^{[2]}_{i,j} \leqslant F(L) + 1 + n - j + \mu(i).$$

Доказательство. Оценим наименьшее τ, при котором из вершины i в вершину j имеется 2-путь любой длины, не меньшей τ.

Построим 2-пути w_0 и w_1 из i в j с помощью конкатенации:

$$w_0(i,j) = w(i, e(i)) \circ (e(i), n-1) \circ C'(t) \circ w(n-1, j), \quad e_0 \leqslant i < n;$$
$$w_1(i,j) = w(i, d(i)) \circ (d(i), n-1) \circ C \circ C'(t) \circ w(n-1, j), \quad 0 \leqslant i < n.$$

Каждый из них есть 2-путь, так как проходит либо через дугу $(e(i), n-1)$ с меткой «2», либо через 2-контур C.

В силу взаимной простоты чисел множества L, вытекающей из примитивности орграфа Γ, при подходящем построении последовательности контуров орграфа Γ

длина контура $C'(t)$ может быть равна любому значению $t > F(L)$. Следовательно, если $e_0 \leqslant i < n$, то длина 2-пути $w_0(i,j)$ может быть любой не меньшей $i - e(i) + F(L) + 1 + n - j$, если $e_0 \leqslant i < n$, а длина 2-пути $w_1(i,j)$ может быть любой не меньшей $i - d(i) + F(L) + 1 + n - j + n - e_l$, если $0 \leqslant i < n$. Следовательно, в орграфе Γ имеется 2-путь из i в j любой длины $\tau \geqslant F(L) + 1 + n - j + \mu(i)$. ■

Обозначим: z_m — метка контура C_m; λ — длина кратчайшего 2-контура.

Следствие 1. Если переменная x_{n-1} существенная для $f(x_0, \ldots, x_{n-1})$, то

$$\gamma_{i,j}^{[2]} = \begin{cases} i - e(i) + n - j, & e_0 \leqslant i < n,\ d(i) - e(i) \leqslant \lambda, \\ i - d(i) + 1 + n - j, & 0 \leqslant i < e_0 \text{ или } d(i) - e(i) > \lambda,\ z_m = 2, \\ i - d(i) + \lambda + n - j, & 0 \leqslant i < e_0 \text{ или } d(i) - e(i) > \lambda,\ z_m = 1. \end{cases}$$

Доказательство. В этих условиях контур C_m — это петля в вершине $n-1$, значит, $1 \in L$ и по определению $F(L) = -1$. Тогда из теоремы 1 следует, что

$$\gamma_{i,j}^{[2]} \leqslant n - j + \mu(i).$$

Заметим, что в Γ кратчайший 2-путь из i в j при $e_0 \leqslant i < n$ — это

$w(i, e(i)) \circ (e(i), n-1) \circ w(n-1, j)$, если $d(i) - e(i) \leqslant \lambda$;
$w(i, d(i)) \circ (d(i), n-1) \circ C_m \circ w(n-1, j)$, если $d(i) - e(i) > \lambda$ и $z_m = 2$;
$w(i, d(i)) \circ (d(i), n-1) \circ C \circ w(n-1, j)$, если $d(i) - e(i) > \lambda$, $z_m = 1$ и C есть кратчайший 2-контур.

При $0 \leqslant i < e_0$ кратчайший 2-путь из i в j — это

$w(i, d(i)) \circ (d(i), n-1) \circ C_m \circ w(n-1, j)$, если $z_m = 2$;
$w(i, d(i)) \circ (d(i), n-1) \circ C \circ w(n-1, j)$, если $z_m = 1$.

Во всех случаях не существует 2-пути меньшей длины в силу размещения меток «2» в орграфе Γ (свойство 1). Пути любой длины больше указанной имеются, так как каждый путь проходит через вершину $n-1$ с петлей. ■

Следствие 2. Если функция обратной связи $f(x_0, \ldots, x_{n-1})$ нелинейна по всем своим существенным переменным, то

$$\gamma_{i,j}^{[2]} \leqslant F(L) + 1 + n - j + i - e(i);$$

если при этом переменная x_{n-1} существенная для $f(x_0, \ldots, x_{n-1})$, то

$$\gamma_{i,j}^{[2]} = n - j + i - e(i).$$

Доказательство. В данных условиях $e(i) = d(i)$ для всех i и $e_0 = 0$, значит, $\mu(u) = u - e(u)$, где $0 \leqslant u < n$. Отсюда из теоремы 1 следует нужная оценка.

Если переменная x_{n-1} существенная, то из следствия 1 получаем значение локального экспонента. ■

Для оценки $\gamma_{i,j}^{[2]}$ обозначим:

$$D^0 = \{d_s \in D, 1 \leqslant s \leqslant m : d_{s-1} - e(d_{s-1}) \leqslant \lambda, e_0 \leqslant d_{s-1} < n\} \cup S_0(n),$$
$$D^1 = \{d_s \in D, 1 \leqslant s \leqslant m : 0 \leqslant d_{s-1} < e_0 \text{ или } d_{s-1} - e(d_{s-1}) > \lambda\} \cup S_1(n),$$

где $S_0(n) = S_1(n) = \varnothing$ при $d_m = n-1$; $S_0(n) = \{n\}$ при $d_m < n-1$ и $d_m \in E$; $S_1(n) = \{n\}$ при $d_m < n-1$ и $d_m \notin E$;

$$\Delta_f = \max_{i \in D^0 \cup D^1} \mu(i-1).$$

По определению $D^1 = \varnothing$, если при $d_m < n-1$ нелинейны все существенные переменные функции $f(x_0, \ldots, x_{n-1})$ или при $d_m = n-1$ нелинейны все существенные переменные, кроме, быть может, x_{d_m}.

Теорема 2. Если орграф Γ примитивный, то

$$\gamma^{[2]} \leqslant F(L) + 1 + n + \Delta_f.$$

Доказательство. В силу теоремы 1 при любом фиксированном i значение $\gamma^{[2]}_{i,j}$ наибольшее при $j = 0$. Тогда из равенства (2) и теоремы 1 имеем

$$\gamma^{[2]} \leqslant F(L) + 1 + n + \max_{0 \leqslant i < n} \mu(i). \tag{3}$$

Функция $\mu(u)$ монотонна по переменной u при $d_{s-1} \leqslant u < d_s$, $s = 1, \ldots, m$, и при $d_m \leqslant u < n$, если $d_m < n-1$. При этом если $d_{s-1} \leqslant i \leqslant u < d_s$, то

$$i - e(i) + n - e_l \leqslant u - e(u) + n - e_l.$$

Поэтому в правой части неравенства (3) можно сузить множество, по которому берется максимум, то есть выполнено неравенство

$$\gamma^{[2]} \leqslant F(L) + 1 + n + \max_{i \in D^0 \cup D^1} \{\mu(i-1)\}.$$

Теорема 2 доказана. ■

Следствие 3. Если переменная x_{n-1} существенная для $f(x_0, \ldots, x_{n-1})$, то

$$\gamma^{[2]} = n + \max\{\max_{i \in D^0}(i - e(i-1)), \xi(z_m) + \max_{i \in D^1}(i - d(i-1))\} - 1,$$

где $\xi(z_m) = \begin{cases} 1, & z_m = 2, \\ \lambda, & z_m = 1. \end{cases}$

Доказательство. В данных условиях из следствия 1 при $j = 0$ с учётом теоремы 2 получаем

$$\max_{i \in D^0} \gamma^{[2]}_{i,j} = n + \max_{i \in D^0}(i - e(i-1)) - 1,$$

$$\max_{i \in D^1} \gamma^{[2]}_{i,j} = \begin{cases} n + 1 + \max\limits_{i \in D^1}(i - d(i-1)) - 1, & z_m = 2, \\ n + \lambda + \max\limits_{i \in D^1}(i - d(i-1)) - 1, & z_m = 1. \end{cases}$$

Отсюда в соответствии с равенством (2) следует нужная формула. ■

Пример 1. Определим точные значения $\langle 2 \rangle$-экспонентов и локальных $\langle 2 \rangle$-экспонентов орграфа нелинейности регистрового преобразования с обратной связью $f(x_0, \ldots, x_{11}) = x_0 \oplus x_3x_5 \oplus x_7x_8x_{11}$ (рис. 1).

Так как переменная x_{11} существенная для функции обратной связи $f(x_0, \ldots, x_{11})$, точное значение $\langle 2 \rangle$-экспонента орграфа нелинейности регистрового преобразования определяется следствием 3, а локальные $\langle 2 \rangle$-экспоненты орграфа — следствием 1.

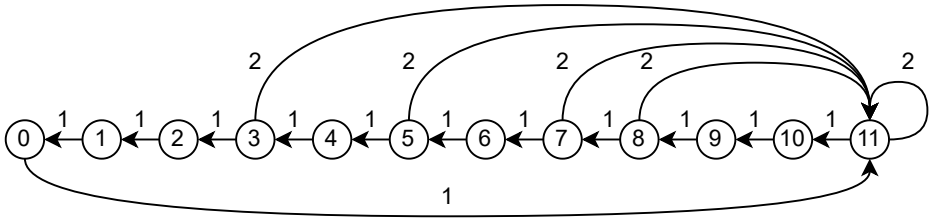

Рис. 1. Орграф нелинейности преобразования из примера 1

Параметры данного регистра сдвига: $n = 12$, $m = 5$, $l = 4$, $D = \{0, 3, 5, 7, 8, 11\}$, $E = \{3, 5, 7, 8, 11\}$, отсюда $e_0 = 3$, $D^0 = \{5, 7, 8, 11\}$, $D^1 = \{3\}$, так как все точки съёма являются нелинейными, за исключением нулевой. Метка пятого контура $z_5 = 2$, отсюда $\xi(z_5) = 1$, длина кратчайшего 2-контура $\lambda = 1$. Так как $d(2) = 0$, то

$$\xi(z_5) + \max_{i \in D^1}\{i - d(i-1)\} = \xi(z_5) + 3 - d(2) = 4.$$

Так как $e(4) = 3$, $e(6) = 5$, $e(7) = 7$, $e(10) = 8$, то

$$\max_{i \in D^0}\{i - e(i-1)\} = \max\{5-3, 7-5, 8-7, 11-8\} = 3.$$

Тогда, согласно следствию 3, $\gamma^{[2]} = 12 + \max\{4, 3\} - 1 = 15$.

Определим значения локальных $\langle 2 \rangle$-экспонентов орграфа.

Если $3 \leqslant i < 12$, то $d(i) - e(i) \leqslant \lambda$ и $\gamma^{[2]}_{i,j} = i - e(i) + 12 - j$.

При $0 \leqslant i < 3$ имеем $\gamma^{[2]}_{i,j} = i - d(i) + 1 + 12 - j$.

Наибольшие значения получаются при $j = 0$, максимальное из них равно 15.

Пример 2. Оценим значения $\langle 2 \rangle$-экспонентов и локальных $\langle 2 \rangle$-экспонентов орграфа нелинейности регистрового преобразования с обратной связью $f(x_0, \ldots, x_{11}) = x_0 \oplus x_3x_5 \oplus x_4x_6x_7$ (рис. 2).

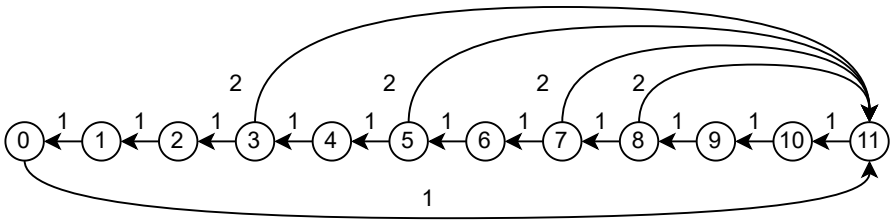

Рис. 2. Орграф нелинейности преобразования из примера 2

Параметры данного регистра сдвига: $n = 12$, $m = 5$, $l = 4$, множество длин простых контуров $L = \{12, 9, 8, 7, 6, 5\}$, $D = \{0, 3, 4, 5, 6, 7\}$, $E = \{3, 4, 5, 6, 7\}$, отсюда $e_0 = 3$, $D^0 = \{4, 5, 6, 7\}$, $D^1 = \{3\}$, так как все точки съёма являются нелинейными, за исключением нулевой. Длина кратчайшего 2-контура $\lambda = 5$.

Оценим сверху с помощью теоремы 1 локальные $\langle 2 \rangle$-экспоненты орграфа. Так как НОД$(L) = 1$, то по свойству 2 орграф нелинейности $\langle 2 \rangle$-примитивный и верны оценки теоремы 1. Вычисляем: $F(L) = 4$, так как любое число больше 4 представимо линейной комбинацией чисел из L с неотрицательными целыми коэффициентами.

Так как $\lambda = 5$, то $\mu(i) = i - e(i)$, если $3 \leqslant i < 12$, и $\mu(i) = i - d(i) + 5$, если $0 \leqslant i < 3$. В табл. 1 приведены значения функции $\mu(i)$ при $0 \leqslant i < 12$, в табл. 2 — значения оценок локальных $\langle 2 \rangle$-экспонентов.

Таблица 1

Значения функции $\mu(i)$ из примера 2

i	0	1	2	3	4	5	6	7	8	9	10	11
$\mu(i)$	5	6	7	0	0	0	0	0	1	2	3	4

Таблица 2

Верхние оценки значений $i \times j$-$\langle 2 \rangle$-экспонентов из примера 2

i	j											
	0	1	2	3	4	5	6	7	8	9	10	11
0	22	21	20	19	18	17	16	15	14	13	12	11
1	23	22	21	20	19	18	17	16	15	14	13	12
2	24	23	22	21	20	19	18	17	16	15	14	13
3	17	16	15	14	13	12	11	10	9	8	7	6
4	17	16	15	14	13	12	11	10	9	8	7	6
5	17	16	15	14	13	12	11	10	9	8	7	6
6	17	16	15	14	13	12	11	10	9	8	7	6
7	17	16	15	14	13	12	11	10	9	8	7	6
8	18	17	16	15	14	13	12	11	10	9	8	7
9	19	18	17	16	15	14	13	12	11	10	9	8
10	20	19	18	17	16	15	14	13	12	11	10	9
11	21	20	19	18	17	16	15	14	13	12	11	10

Из табл. 2 в соответствии с (2) получаем оценку $\langle 2 \rangle$-экспонента орграфа нелинейности: $\gamma^{[2]} \leqslant 24$.

ЛИТЕРАТУРА

1. *Фомичёв В. М., Авезова Я Э., Коренева А. М., Кяжин С. Н.* Примитивность и локальная примитивность орграфов и неотрицательных матриц // Дискретный анализ и исследование операций. 2018. Т. 25. № 3. С. 95–125.
2. *Frobenius G.* Über Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss. Berlin, 1912. P. 456–477.
3. *Dulmage A. L. and Mendelsohn N. S.* The exponent of a primitive matrix // Canadian Math. Bull. 1962. No. 5. P. 241–244.
4. *Perkins P.* A theorem on regular graphs // Pacific J. Math. 1961. V. 2. P. 1529–1533.
5. *Фомичёв В. М.* Оценка характеристик нелинейности итеративных преобразований векторного пространства // Дискретный анализ и исследование операций. 2020. Т. 27. № 4. С. 131–151.
6. *Fomichev V. M. and Koreneva A. M.* Encryption performance and security of certain wide block ciphers // J. Computer Virology Hacking Tech. 2020. V. 16. No. 1. P. 197–216.
7. *Фомичёв В. М., Авезова Я. Э.* Точная формула экспонентов перемешивающих орграфов регистровых преобразований // Дискретный анализ и исследование операций. 2020. Т. 27. № 2. С. 117–135.
8. *Фомичёв В. М., Бобров В. М.* Оценка с помощью матрично-графового подхода характеристик локальной нелинейности итераций преобразований векторных пространств // Прикладная дикретная математика. Приложение. 2019. № 12. С. 32–35.

REFERENCES

1. *Fomichev V. M., Avezova Ya. E., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices. J. Appl. Industr. Math., 2018, vol. 12, no. 3, pp. 453–469.
2. *Frobenius G.* Über Matrizen aus nicht negativen Elementen. Sitzungsber K. Preuss. Akad. Wiss., Berlin, 1912, pp. 456–477.
3. *Dulmage A. L. and Mendelsohn N. S.* The exponent of a primitive matrix. Canadian Math. Bull., 1962, no. 5, pp. 241–244.
4. *Perkins P.* A theorem on regular graphs. Pacific J. Math., 1961, vol. 2, pp. 1529–1533.
5. *Fomichev V. M.* Estimating nonlinearity characteristics for iterative transformations of a vector space. Appl. Industr. Math., 2020, vol. 14, no. 4, pp. 610–622.
6. *Fomichev V. M. and Koreneva A. M.* Encryption performance and security of certain wide block ciphers. J. Computer Virology Hacking Tech., 2020, vol. 16, no. 1, pp. 197–216.
7. *Fomichev V. M. and Avezova Ya. E.* Exact formula for exponents of mixing digraphs for register transformations. J. Appl. Industr. Math., 2020, vol. 14, no. 2, pp. 308–319.
8. *Fomichev V. M. and Bobrov V. M.* Otsenka s pomoshch'yu matrichno-grafovogo podkhoda kharakteristik lokal'noy nelineynosti iteratsiy preobrazovaniy vektornykh prostranstv [Estimation of local nonlinearity characteristics of vector space transformation iteration using matrix-graph approach]. Prikladnaya Diksretnaya Matematika. Prilozheniye, 2019, no. 12, pp. 32–35. (in Russian)