УДК 519.1 DOI 10.17223/2226308X/12/9

ОЦЕНКА С ПОМОЩЬЮ МАТРИЧНО-ГРАФОВОГО ПОДХОДА ХАРАКТЕРИСТИК ЛОКАЛЬНОЙ НЕЛИНЕЙНОСТИ ИТЕРАЦИЙ ПРЕОБРАЗОВАНИЙ ВЕКТОРНЫХ ПРОСТРАНСТВ

В. М. Фомичёв, В. М. Бобров

В порядке обобщения матрично-графового подхода к исследованию характеристик нелинейности преобразований векторных пространств, предложенного В. М. Фомичевым, развивается математический аппарат для локальной нелинейности преобразований. Пусть $G = \{0, 1, 2\}$ — мультипликативная полугруппа, где $a0 = 0$ для любого $a \in G$; $ab = \max\{a, b\}$ для любых $a, b \neq 0$. Троичная матрица (то есть матрица над G) называется α-матрицей, $\alpha \in \Pi(2) = \{\langle 2c\rangle; \langle 2s\rangle; \langle 2sc\rangle; \langle 2\rangle\}$, если все её строки ($\langle 2s\rangle$-матрица), столбцы ($\langle 2c\rangle$-матрица), строки и столбцы ($\langle 2sc\rangle$-матрица) содержат 2 или если все элементы равны 2 ($\langle 2\rangle$-матрица). Обозначим $M_n^\alpha(I \times J)$ множество троичных матриц M порядка n, чьи $I \times J$-подматрицы (полученные вычеркиванием строк с номерами не из I и столбцов с номерами не из J) являются α-матрицами, $I, J \in \{1, \ldots, n\}$. На множестве троичных матриц определено умножение. Если $A = (a_{i,j})$, $B = (b_{i,j})$, то $AB = C = (c_{i,j})$, где $c_{i,j} = \max\{a_{i,1}b_{1,j}, \ldots, a_{i,n}b_{n,j}\}$ и для любых допустимых i, j умножение элементов выполняется в группе G. Матрицу M назовём $I{\times}J$-α-примитивной, если существует $\gamma \in \mathbb{N}$, такое, что $M^t \in M_n^\alpha(I \times J)$ при всех натуральных $t \geqslant \gamma, \alpha \in \Pi(2)$. Наименьшее из таких чисел γ обозначим $I \times J$-α-$\exp M$ и назовём $I \times J$-α-экспонентом матрицы M. Троичным матрицам порядка n биективно соответствуют n-вершинные орграфы с множеством G меток дуг, поэтому на орграфы распространены определения $I \times J$-α-примитивности и $I \times J$-α-экспонента. Получены достаточные условия того, что $I \times J$-α-экспонент матрицы равен наименьшей её степени, в которой $I \times J$-подматрица является α-матрицей, $\alpha \in \Pi(2)$. При $I = \{i\}$, $J = \{j\}$ для частных классов помеченных орграфов получены верхние оценки $I{\times}J$-α-экспонентов, в частности для орграфа, в котором имеется путь из i в j, проходящий через компоненту сильной связности.

Ключевые слова: *матрично-графовый подход, троичная матрица, помеченный орграф, локальная нелинейность, локальный α-экспонент.*

Введение

В некоторых приложениях, в том числе криптографических, важно определить множество переменных, от которых нелинейно зависит каждая функция из заданного подмножества координатных функций преобразования векторного пространства. Эта информация может быть использована для оценки эффективности некоторых методов линеаризации при получении оценки стойкости криптографических алгоритмов.

Представленные результаты направлены на получение оценок множеств переменных, по которым нелинейны те или иные координатные функции преобразования векторного пространства, построенного по итеративному принципу.

Приведём ряд определений [1]. Преобразованию $g(x_1, \ldots, x_n)$ множества V_n двоичных n-мерных векторов с координатными функциями $g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)$ соответствует n-вершинный орграф $\Gamma_\theta(g)$, где дуга (i, j) помечена числом 0, 1 или 2 тогда и только тогда, когда $g_j(x_1, \ldots, x_n)$ зависит от x_i соответственно фиктивно, линейно или нелинейно, $1 \leqslant i, j \leqslant n$. Преобразование $g(x_1, \ldots, x_n)$ называется $I \times J$-$\langle 2\rangle$-нелинейным, если любая дуга $(i, j) \in I{\times}J$ в орграфе $\Gamma_\theta(g)$ помечена символом «2». Преобразование $g(x_1, \ldots, x_n)$ называется $I \times J$-$\langle 2\rangle$-перфективным, если при некотором на-

туральном t преобразование g^t является $I{\times}J$-нелинейным, наименьшее такое t называется показателем полной $I{\times}J$- $\langle 2\rangle$-нелинейности преобразования $g(x_1,\ldots,x_n)$ (обозначается $I{\times}J$- $\langle 2\rangle$-nlg). Характеристики орграфа $\Gamma_\theta(g^t)$ можно оценить с помощью матрицы меток орграфа $\Gamma_\theta(g)$, обозначаемой $M_\theta(g)$, что следует из неравенства для любых преобразований $g^{(1)},\ldots,g^{(t)}$ множества V_n [1]: $M_\theta\left(g^{(1)},\ldots,g^{(t)}\right)\geqslant M_\theta\left(g^{(1)}\right)\ldots M_\theta\left(g^{(t)}\right)$. Проекция этого неравенства на подмножества $I\times J$ даёт следующую оценку:

$$M_\theta\left(g^{(1)},\ldots,g^{(t)}\right)(I\times J)\geqslant M_\theta\left(g^{(1)}\right)(I\times J)\ldots M_\theta\left(g^{(t)}\right)(I\times J),\quad I,J\subseteq\{1,\ldots,n\}.$$

Таким образом, локальные характеристики матрицы нелинейности $M_\theta\left(g^{(1)},\ldots,g^{(t)}\right)$ можно оценить с помощью локальных характеристик матрицы $M_\theta\left(g^{(1)}\right)\ldots M_\theta\left(g^{(t)}\right)$. В частности, локальные характеристики матрицы нелинейности $M_\theta(g^t)$ можно оценить с помощью локальных характеристик t-й степени матрицы нелинейности $M_\theta(g)$.

1. Локальная α-примитивность троичных матриц и помеченных орграфов

Троичная матрица называется особенной, если она имеет нулевую строку или нулевой столбец. Обозначим: M_n — множество квадратных неособенных троичных матриц порядка n; $M(I\times J)$ — подматрица матрицы $M\in M_n$ (называемая $I{\times}J$-подматрицей), полученная вычеркиванием из M строк с номерами из I и столбцов с номерами из J, где $I,J\subseteq\{1,\ldots,n\}$.

Неособенная матрица называется:

— $\langle 2c\rangle$-матрицей, если каждый столбец матрицы содержит элемент 2;
— $\langle 2s\rangle$-матрицей, если каждая строка матрицы содержит элемент 2;
— $\langle 2sc\rangle$-матрицей, если она является $\langle 2c\rangle$-матрицей и $\langle 2s\rangle$-матрицей;
— $\langle 2\rangle$-матрицей, если каждый элемент матрицы равен 2.

Для $\alpha\in\Pi(2)$ обозначим $M_n^\alpha(I\times J)$ множество всех матриц $M\in M_n$, чьи $I\times J$-подматрицы являются α-матрицами.

Матрицу M назовём $I\times J$-α-примитивной, если существует $\gamma\in\mathbb{N}$, такое, что $M^t\in$ $\in M_n^\alpha(I\times J)$ при всех натуральных $t\geqslant\gamma$, $\alpha\in\Pi(2)$. Наименьшее из таких чисел γ обозначим $I\times J$-α-$\exp M$ и назовём $I\times J$-α-экспонентом матрицы M.

Обобщённо назовём свойства $I\times J$-α-примитивности матриц в случае I и J, не равных $\{1,\ldots,n\}$, свойством локальной α-примитивности матриц для всех $\alpha\in\Pi(2)$. Случай $I=J=\{1,\ldots,n\}$ называется α-примитивностью и исследован в [1].

В случае α-примитивности наименьшее $t\in\mathbb{N}$, такое, что $M^t\in M_n^\alpha$, равно α-экспоненту, в то время как для локальной α-примитивности в общем случае это не верно.

Обозначим $Q_s(I\times J)$, $Q_c(I\times J)$ множества матриц $M\in M_n$, чьи $I\times J$-подматрицы не имеют нулевых строк и столбцов соответственно; $Q_{sc}(I\times J)=Q_s(I\times J)\cap Q_c(I\times J)$. Для случая $I=J$ обозначим эти множества $Q_s(I^2)$, $Q_c(I^2)$, $Q_{sc}(I^2)$.

Если $M^t\in M_n^\alpha(I\times J)$, то в соответствии с определением этого недостаточно для того, чтобы выполнялось равенство $t=I\times J$-α-$\exp M$. Укажем условие, когда наименьшее $t\in\mathbb{N}$, при котором $M^t\in M_n^\alpha(I\times J)$, равно $I\times J$-α-экспоненту матрицы.

Теорема 1 (обобщение утверждения 1,а [2]). Пусть $t\in N$ — наименьшее натуральное число, при котором $A^t\in M_n^\alpha(I\times J)$, $\alpha\in\Pi(2)$, тогда A является $I\times J$-α-примитивной и $t=I\times J$-α-$\exp A$, если

$$\alpha=\langle 2s\rangle,\ A\in Q_s\left(I^2\right)\cup Q_s\left(J^2\right);$$
$$\alpha=\langle 2c\rangle,\ A\in Q_c\left(I^2\right)\cup Q_c\left(J^2\right);$$

$$\alpha = \langle 2sc \rangle\,,\ A \in Q_{sc}\left(I^2\right) \cup Q_{sc}\left(J^2\right);$$
$$\alpha = \langle 2 \rangle\,,\ A \in Q_{s}\left(I^2\right) \cup Q_{c}\left(J^2\right).$$

При $n > 1$ троичной матрице $M = (m_{i,j})$ порядка n биективно соответствует помеченный n-вершинный орграф Γ, у которого дуга (i, j) имеет метку $m_{i,j}$, $0 \leqslant i, j < n$, где метка «0» равносильна отсутствию дуги в орграфе [1]. Неособенной матрице соответствует орграф, каждая вершина которого имеет ненулевые полустепени исхода и захода, такие орграфы назовём также неособенными. Помеченный орграф называется $I \times J$-α-примитивным, если $I \times J$-α-примитивна его матрица меток $(m_{i,j})$.

На множестве Γ_n неособенных помеченных орграфов порядка n определена полугрупповая операция умножения орграфов Γ и Γ': если в Γ имеется дуга $(i, m_{i,r}, r)$, а в Γ' имеется дуга $(r, \mu_{r,i}, j)$, то в орграфе $\Gamma\Gamma'$ имеется дуга $(i, m_{i,r}\mu_{r,j}, j)$, где операция умножения меток выполняется в полугруппе G. Доказано [1, следствие 1], что в орграфе Γ^t дуга (i, j) имеет метку «0», если и только если в Γ вершина j недостижима из вершины i за t шагов; «1», если и только если в Γ любой путь из i в j длины t состоит только из дуг с меткой «1»; «2», если и только если в Γ имеется путь из i в j длины t, содержащий дугу с меткой «2».

2. Оценки локальных α-экспонентов некоторых классов орграфов

В случае $I = \{i\}, J = \{j\}$ свойства $I \times J$-α-примитивности для любого $\alpha \in \Pi(2)$ одинаковы. Назовём этот случай $i \times j$- $\langle 2 \rangle$-примитивностью, а соответствующий экспонент орграфа Γ обозначим $i \times j$- $\langle 2 \rangle \exp \Gamma$.

Сильносвязный подграф Γ' с множеством вершин V орграфа Γ называется i, j-связывающим, если в Γ существует путь из i в j, проходящий через некоторую вершину множества $V \subseteq \{1, \ldots, n\}$.

Теорема 2.

а) Орграф Γ $I \times J$- $\langle 2 \rangle$-примитивный, если и только если Γ $i \times j$- $\langle 2 \rangle$-примитивный для всех $(i, j) \in I \times J$; в этом случае $I \times J$- $\langle 2 \rangle \exp \Gamma = \max\limits_{(i,j) \in I \times J} \{i \times j\text{- } \langle 2 \rangle \exp \Gamma\}$.

б) Орграф Γ $I \times J$- $\langle 2s \rangle$-примитивный, если и только если Γ $i \times J$- $\langle 2s \rangle$-примитивный для всех $i \in I$; в этом случае $I \times J$- $\langle 2s \rangle \exp \Gamma = \max\limits_{i \in I} \{i \times J\text{- } \langle 2s \rangle \exp \Gamma\}$.

в) Орграф Γ $I \times J$- $\langle 2c \rangle$-примитивный, если и только если Γ $I \times j$- $\langle 2c \rangle$-примитивный для всех $j \in J$; в этом случае $I \times J$- $\langle 2c \rangle \exp \Gamma = \max\limits_{j \in J} \{I \times j\text{- } \langle 2c \rangle \exp \Gamma\}$.

Обозначим $\rho(i, V)$ — наименьшее расстояние от вершины i до подмножества вершин V; $\rho(V, j)$ — расстояние от подмножества вершин V до вершины j; $d(i, V)$ $(d(V, j))$ — длина кратчайшего пути из i до V (от V до j), содержащего дугу с меткой «2».

Теорема 3 (обобщение теоремы 2, а [2]). Если связный помеченный орграф Γ содержит примитивный i, j-связывающий подграф Γ' с множеством вершин V, $|V| = n$, то Γ является $i \times j$- $\langle 2 \rangle$-примитивным, если выполняется хотя бы одно из следующих условий:

а) в подграфе Γ' есть дуга с меткой «2», тогда

$$i \times j\text{- } \langle 2 \rangle \exp \Gamma \leqslant \rho(i, V) + n + \exp \Gamma' + \rho(V, j);$$

б) в кратчайшем пути из i до множества вершин подграфа V или от множества вершин подграфа V до вершины j есть дуга с меткой «2», тогда

$$i \times j\text{-}\langle 2 \rangle \exp \Gamma \leqslant \rho(i, V) + \exp \Gamma' + \rho(V, j);$$

в) существует путь из i до множества вершин подграфа V, содержащий дугу с меткой «2», тогда

$$i\times j\text{-}\langle 2\rangle\exp\Gamma \leqslant d\,(i,V)+\exp\Gamma'+\rho\,(V,j)\,;$$

г) существует путь от множества вершин подграфа V до вершины j, содержащий дугу с меткой «2», тогда

$$i\times j\text{-}\langle 2\rangle\exp\Gamma \leqslant \rho\,(i,V)+\exp\Gamma'+d\,(V,j)\,.$$

Пример 1. Рассмотрим преобразование регистра левого сдвига длины 6 с функцией обратной связи $f\,(x_0,x_1,x_2,x_3,x_4,x_5)=x_0\oplus x_2x_4\oplus x_5$. Орграф Γ этого преобразования представлен на рис. 1, матрица M — на рис. 2. Определим оценку значения 1×3-$\langle2\rangle$-экспонента для этого орграфа. Вершины 5 и 4 образуют 1,3-связывающий подграф Γ', где $n=|V|=2$, $\exp\Gamma'=1$, $\rho\,(1,V)=2$, $\rho\,(V,3)=1$, $d\,(1,V)=4$, $d\,(V,3)=3$. Оценки 1×3-$\langle2\rangle$-экспонента графа Γ приведены в таблице.

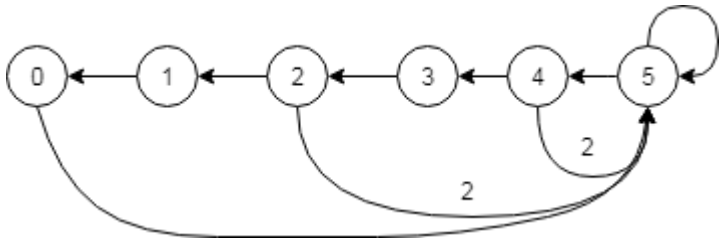

Рис. 1. Орграф нелинейности преобразования регистра сдвига

$$\begin{pmatrix}0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&2\\0&0&1&0&0&0\\0&0&0&1&0&2\\0&0&0&0&1&1\end{pmatrix}$$

Рис. 2. Матрица нелинейности преобразования регистра сдвига

Сравнение оценок 1×3-$\langle2\rangle$-экспонента графа Γ

Значение оценки $i\times j$-$\langle2\rangle$-экспонента	Формула оценки $i\times j$-$\langle2\rangle$-экспонента
6	$i\times j\text{-}\langle2\rangle\exp\Gamma\leqslant\rho\,(i,V)+n+\exp\Gamma'+\rho\,(V,j)$
6	$i\times j\text{-}\langle2\rangle\exp\Gamma\leqslant d\,(i,V)+\exp\Gamma'+\rho\,(V,j)$
6	$i\times j\text{-}\langle2\rangle\exp\Gamma\leqslant\rho\,(i,V)+\exp\Gamma'+d\,(V,j)$

При возведении матрицы M в степень получаем, что 1×3-$\langle2\rangle$-$\exp\Gamma=6$, что соответствует полученным оценкам.

ЛИТЕРАТУРА

1. *Фомичёв В. М.* О производительности некоторых итеративных алгоритмов блочного шифрования из класса WBC // New Trends in Coding Systems and Techniques. LDN: Intech Publishing, 2019. P. 14.
2. *Кяжин С. Н.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.