

О СТЕПЕНИ НЕЛИНЕЙНОСТИ КООРДИНАТНЫХ ПОЛИНОМОВ ПРОИЗВЕДЕНИЯ ПРЕОБРАЗОВАНИЙ ДВОИЧНОГО ВЕКТОРНОГО ПРОСТРАНСТВА

В. М. Фомичёв^{1, 2, 3}

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

² ООО «Код Безопасности»,

1-й Нагатинский пр-д, 10, стр. 1, 115230 Москва, Россия

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

E-mail: fomichev.2016@yandex.ru

Аннотация. Построена неотрицательная целочисленная матрица для оценки матрицы характеристик нелинейности координатных полиномов произведения преобразований двоичного векторного пространства. Матрица характеристик преобразования определяется степенями нелинейности производных всех координатных функций по каждой входной переменной. Элементы оценочной матрицы выражены через характеристики координатных полиномов умножаемых преобразований. Вычисление оценочной матрицы выполняется более просто по сравнению с вычислением точных значений характеристик. Метод оценивания распространён на произвольное количество умножаемых преобразований. Приведены вычислительные примеры, в частности, показывающие точность полученных оценок и область их нетривиальности. Табл. 1, библиогр. 18.

Ключевые слова: координатный полином преобразования, максимальный моном полинома, степень полинома.

Основные обозначения

- \mathbb{N} — множество натуральных чисел;
- $\mathbb{N}_n = \{0, \dots, n-1\}$, $n \in \mathbb{N}$;
- $2^{[n]}$ — булеан множества $\{0, \dots, n-1\}$;
- $(b)_n$ — квадратная матрица порядка n , каждый элемент которой равен $b \in \{0, \dots, n\}$;
- V_n — пространство двоичных векторов длины $n \in \mathbb{N}$;
- Π_n — множество преобразований пространства V_n .

Введение

Сложные функции, в том числе в криптографических алгоритмах, часто реализуют с помощью композиции относительно несложных функций, удобно реализуемых аппаратно и/или программно. Такой подход практикуется, например, в симметричных блочных шифрах, где зашифрование и расшифрование выполняется после нескольких раундов однотипных вычислений. Важной задачей анализа композиции нелинейных преобразований векторного пространства является определение таких характеристик координатных функций, как множества существенных переменных, нелинейных переменных, степень нелинейности координатных функций. Точное определение и даже оценка степени нелинейности координатных функций композиции преобразований двоичного векторного пространства является в общем случае нетривиальной задачей.

Для исследования множества существенных, в частности, нелинейных переменных композиций нелинейных преобразований векторных пространств активно применяется обоснованный в литературе матрично-графовый подход (МГП) [1–3]. Математическую основу МГП к исследованию существенных и нелинейных переменных составляют критерии примитивности и локальной примитивности множеств неотрицательных матриц (орграфов) и оценки их экспонентов и локальных экспонентов.

Инициированная в 1912 г. Фробениусом [4] постановка задачи получила поэтапное развитие в середине и конце XX века, а также в последние примерно 10 лет. История получения до 2018 г. основных результатов по этим направлениям отражена в [1]. Введённые Фробениусом изначальные понятия впоследствии были развиты рядом авторов [5–13], в том числе в работах прикладного характера [14–16]. Такие понятия, к которым относятся примитивность и локальная примитивность неотрицательных матриц и орграфов и др., имеют важное прикладное значение для исследования свойств множеств преобразований векторного пространства, связанных с существенными переменными и различными видами нелинейности. Введены количественные характеристики такого рода свойств, обобщающие известные понятия экспонентов примитивных матриц и орграфов. С помощью МГП получены оценки этих характеристик в различных условиях.

Нелинейность является фундаментальным свойством функций, применяемых в криптографических системах. Свойство нелинейности функций выражается через весьма обширное множество характеристик. Одна из них так и названа — нелинейность булевой функции [17], определяющая в метрике Хэмминга расстояние N_f от функции f до множества аффинных функций. Неравновероятность максимально нелинейных функций (для них N_f достигает наибольшего из возможных значений при фиксированном числе переменных) заметно ограничила их применение

в криптографических алгоритмах. Другие характеристики нелинейности булевых функций связаны с N_f в общем случае весьма сложно и зачастую требуют иных методов исследования. Математическую основу МГП при исследовании различных видов нелинейной зависимости множества координатных функций от входных переменных составляют критерии α -примитивности множеств троичных матриц (помеченных орграфов) и оценки их α -экспонентов [2, 3], где α — параметр, определяющий вид соответствующего нелинейного преобразования.

В данной работе получена формула для оценивания степеней нелинейности координатных функций произведения преобразований двоичного векторного пространства через характеристики умножаемых преобразований. Задача определения или оценки степеней нелинейности координатных функций является более глубокой и, следовательно, более сложной по сравнению с исследованием только наличия определённого вида нелинейной зависимости. Для её решения не удаётся применить МГП в той же мере эффективно, как это сделано в [2, 3]. Вместе с тем, получены оценки, которые в ряде случаев нетривиальны и могут рекурсивно применяться для оценки степеней нелинейности координатных функций произведения нескольких преобразований векторного пространства.

1. Свойства неотрицательных матриц и помеченных орграфов

Матрица $A = (a_{i,j})$ над кольцом целых чисел называется *неотрицательной* (записывается $A \geq 0$), если $a_{i,j} \geq 0$ для любой пары (i, j) , $0 \leq i, j < n$. Неотрицательная матрица называется *особенной*, если в ней имеются нулевые строки или столбцы, иначе — *неособенной*. Множество всех квадратных неособенных матриц порядка n обозначим через M_n .

На множестве неотрицательных матриц задан частичный порядок: если $A = (a_{i,j})$, $B = (b_{i,j})$, то $A \leq B$ тогда и только тогда, когда $a_{i,j} \leq b_{i,j}$ для любой пары (i, j) , $0 \leq i, j < n$. Если при этом $A \neq B$, то $A < B$.

Далее $A \in M_n$, $\alpha = \{k_1, \dots, k_s\}$ — непустой элемент булеана $2^{[n]}$, т. е. $s \geq 1$, $0 \leq k_1, \dots, k_s < n$.

Обозначим: $\sigma_j(A) = \max\{a_{0,j}, \dots, a_{n-1,j}\}$ — наибольший элемент j -го столбца матрицы A , $0 \leq j < n$; $\sigma_\alpha(A) = \sum_{j \in \alpha} \sigma_j(A)$; A_α — матрица размера $n \times s$, полученная удалением из A всех столбцов с номерами $j \notin \alpha$; $w_\alpha(i) = \max\{a_{i,k_1}, \dots, a_{i,k_s}\}$ — наибольший элемент i -й строки матрицы A_α ; для ненулевой i -й строки матрицы A_α

$$\mu_\alpha(i, A) = \sigma_\alpha(A) + \max_{k \in \alpha: a_{i,k} > 0} \{a_{i,k} - \sigma_k(A)\}, \quad (1)$$

в противном случае (при $a_{i,u} = 0$, $u = k_1, \dots, k_s$) $\mu_\alpha(i, A) = 0$, $0 \leq i < n$.

Теорема 1. (а) При любом $\alpha \in 2^{[n]}$ в матрице A_α имеются ненулевые строки. Если i -я строка ненулевая в матрице A_α , $0 \leq i < n$, то

$$\mu_\alpha(i, A) \geq w_\alpha(i) + s - 1,$$

в частности, $\mu_\alpha(i, A) = a_{i,k}$ при $s = 1$ и $\alpha = \{k\}$;

(б) функция $\mu_\alpha(i, A)$ монотонна на множестве M_n при любом фиксированном α ;

(в) функция $\mu_\alpha(i, A)$ монотонна на булеане $2^{[n]}$ при любой фиксированной матрице A .

ДОКАЗАТЕЛЬСТВО. (а) Пусть $\alpha = \{k_1, \dots, k_s\}$, $1 \leq s \leq n$. Так как столбцы матрицы A ненулевые, для любого $k \in \alpha$ найдётся число $i \in \mathbb{N}_n$ такое, что $a_{i,k} > 0$. Значит, в матрице A_α имеются ненулевые строки. Если i -я строка ненулевая в матрице A_α , $0 \leq i < n$, то с учётом неравенств $\sigma_j(A) \geq 1$, $j \in \alpha$, из (1) получаем

$$\mu_\alpha(i, A) \geq a_{i,k} + s - 1, \quad k \in \alpha.$$

Поскольку оценка верна для любого $k \in \alpha$, неравенство для $\mu_\alpha(i, A)$ доказано.

Равенства при $s = 1$ следуют из (1).

(б) Пусть $A = (a_{i,j})$, $B = (b_{i,j})$, $A \leq B$. Обозначим $\Delta(\mu) = \mu_\alpha(i, B) - \mu_\alpha(i, A)$. Покажем, что $\Delta(\mu) \geq 0$.

При $s = 1$ по теореме 1(а) $\Delta(\mu) = b_{i,k} - a_{i,k}$, где $b_{i,k} - a_{i,k} \geq 0$ в силу отношения $A \leq B$.

При $s > 1$ предположим, что

$$\max_{u \in \alpha: a_{i,u} > 0} \{a_{i,u} - \sigma_u(A)\} \text{ и } \max_{u \in \alpha: a_{i,u} > 0} \{b_{i,u} - \sigma_u(B)\}$$

достигаются при $u = k_1$ и $u = k_p$ соответственно, где $1 \leq p \leq s$. Тогда

$$b_{i,k_p} - \sigma_{k_p}(B) \geq b_{i,k_1} - \sigma_{k_1}(B). \quad (2)$$

Пусть B и A различаются элементами лишь k_1 -го столбца. Тогда $b_{i,j} = a_{i,j}$, $j \neq k_1$, и $b_{i,k_1} \geq a_{i,k_1}$, так как $A \leq B$, $0 \leq i < n$. Значит, $\sigma_{k_t}(B) = \sigma_{k_t}(A)$, $t = 2, \dots, s$, $\sigma_{k_1}(B) \geq \sigma_{k_1}(A)$. Отсюда и из (1) получаем

$$\begin{aligned} \Delta(\mu) &= \sigma_{k_1}(B) - \sigma_{k_1}(A) + b_{i,k_p} - \sigma_{k_p}(B) - a_{i,k_1} + \sigma_{k_1}(A) \\ &= \sigma_{k_1}(B) + b_{i,k_p} - \sigma_{k_p}(B) - a_{i,k_1}. \end{aligned}$$

Значит, с учётом (2) имеем $\Delta(\mu) \geq b_{i,k_1} - a_{i,k_1} \geq 0$.

Пусть матрица B отлична от A элементами, возможно, всех столбцов за исключением k_1 -го столбца. Тогда $b_{i,k_1} = a_{i,k_1}$ и $b_{i,j} \geq a_{i,j}$ при $j \neq k_1$,

так как $A \leq B$. Значит, $\sigma_{k_1}(B) = \sigma_{k_1}(A)$ и $\sigma_{k_t}(B) \geq \sigma_{k_t}(A)$, $t = 2, \dots, s$. В этом случае из (1) получаем

$$\Delta(\mu) = \sum_{t=2}^s (\sigma_{k_t}(B) - \sigma_{k_t}(A)) + b_{i,k_p} - \sigma_{k_p}(B) - a_{i,k_1} + \sigma_{k_1}(A).$$

С учётом (2) $b_{i,k_p} - \sigma_{k_p}(B) \geq b_{i,k_1} - \sigma_{k_1}(A)$, откуда

$$\Delta(\mu) = \sum_{t=2}^s (\sigma_{k_t}(B) - \sigma_{k_t}(A)) + b_{i,k_1} - a_{i,k_1},$$

где правая часть неравенства есть сумма s неотрицательных слагаемых.

В общем случае, когда $A \leq B$, возьмём матрицу C такую, что $A \leq C \leq B$, где C отлична от A элементами лишь k_1 -го столбца и B отлична от C элементами, возможно, всех столбцов за исключением k_1 -го столбца. Из доказанной неотрицательности величин $\mu_\alpha(i, C) - \mu_\alpha(i, A)$ и $\mu_\alpha(i, B) - \mu_\alpha(i, C)$ следует неотрицательность их суммы, равной $\Delta(\mu)$.

(в) Пусть $\{k_1, \dots, k_s\} = \alpha \subset \beta = \{l_1, \dots, l_r\}$, $s < r$. Обозначим $\rho(\mu) = \mu_\beta(i, A) - \mu_\alpha(i, A)$. Покажем, что $\rho(\mu) \geq 0$. Без ущерба для общности положим $k_1 = l_1, \dots, k_s = l_s$. Тогда из (1) имеем

$$\rho(\mu) = \sigma_{l_{s+1}}^A + \dots + \sigma_{l_r}^A + \max_{u \in \beta} \{a_{i,u} - \sigma_u^A\} - \max_{u \in \alpha} \{a_{i,u} - \sigma_u^A\},$$

где разность максимумов неотрицательна, так как $\alpha \subset \beta$. Следовательно, $\rho(\mu)$ есть сумма неотрицательных чисел. Теорема 1 доказана.

Назовём оргграф *особенным* (неособенным), если он имеет вершину с нулевой полустепенью захода или исхода (не имеет таких вершин).

Множеству матриц M_n биективно соответствует класс неособенных помеченных оргграфов с множеством вершин $\{0, \dots, n-1\}$ (обозначим это множество оргграфов через $\Gamma(M_n)$): если $A \in M_n$, то в соответствующем оргграфе $\Gamma(A)$ дуга (i, j) помечена числом $a_{i,j}$ и вершина j помечена числом $\sigma_j(A)$, $0 \leq i, j < n$, а метка «0» дуги равносильна отсутствию этой дуги в оргграфе. Дугу (i, j) с меткой $a_{i,j}$ запишем также как тройку $(i, a_{i,j}, j)$. Назовём набор чисел $(\sigma_0(A), \dots, \sigma_{n-1}(A))$ и матрицу A *набором меток* вершин и *матрицей меток* дуг оргграфа $\Gamma(A)$ соответственно.

На множестве оргграфов $\Gamma(M_n)$ задан частичный порядок: $\Gamma(A) \leq \Gamma(B)$, где $A, B \in M_n$, тогда и только тогда, когда $A \leq B$. Пусть $\bar{b} = (b_0, \dots, b_{n-1})$ — набор чисел из множества $\{0, \dots, n\}$. Обозначим через $\Gamma_{\bar{b}}(M_n)$ множество графов из $\Gamma(M_n)$, у которых набор меток вершин не меньше чем \bar{b} : $\sigma_j(A) \geq b_j$, $0 \leq j < n$.

2. О характеристиках нелинейности произведения преобразований

Обозначим: $x = (x_0, \dots, x_{n-1})$ — строка входных переменных; W_n — множество всех мономов от x_0, \dots, x_{n-1} ; $x^\alpha = x_{k_1} \dots x_{k_s} \in W_n$ — моном степени $s \geq 1$, где $\alpha = \{k_1, \dots, k_s\}$, $x^\alpha = 1$ при $\alpha = \emptyset$.

На множестве W_n задан частичный порядок, согласованный с частичным порядком на $2^{[n]}$: если $\alpha, \beta \in 2^{[n]}$, $\alpha = \{k_1, \dots, k_s\}$, $\beta = \{l_1, \dots, l_r\}$, то $x^\alpha \leq x^\beta$ тогда и только тогда, когда $\{k_1, \dots, k_s\} \subseteq \{l_1, \dots, l_r\}$.

Булевой функции $f(x)$ однозначно соответствует множество мономов её алгебраической нормальной формы, обозначим его через $W(f)$. Моном $x^\alpha \in W(f)$ называется *максимальным* для $f(x)$, если отношение $x^\alpha \leq x^\beta$ неверно для любого другого монома $x^\beta \in W(f)$.

Для булевой функции f введём следующие обозначения, $0 \leq i < n$: $S(f)$ — множество номеров существенных переменных; $\deg f$ — степень нелинейности; $d(i, f)$ — наибольшая степень зависящего от x_i монома; $\frac{df(x)}{dx_i}$ — производная функции $f(x)$ по переменной x_i [18]; $L(f)$ — множество всех максимальных для f мономов. Для $A \in M_n$ обозначим

$$\mu_f(i, A) = \max_{\alpha: x^\alpha \in L(f)} \mu_\alpha(i, A), \quad 0 \leq i, j < n.$$

Из данных обозначений непосредственно следуют свойства:

- 1) $\deg f = \max\{d(0, f), \dots, d(n-1, f)\}$;
- 2) $d(i, f) = \deg\left(\frac{df(x)}{dx_i}\right) + 1$, если $\frac{df(x)}{dx_i} \neq 0$, иначе $d(i, f) = 0$, где $\frac{df(x)}{dx_i} \neq 0$ тогда и только тогда, когда $i \in S(f)$.

Теорема 2. (а) Если булевы функции $f(x)$ и $\Psi(x)$ не являются константами и $L(f) \subseteq L(\Psi)$, то

$$\mu_f(i, A) \leq \mu_\Psi(i, A), \quad 0 \leq i < n.$$

- (б) Если $f(x) = x_{k_1} \oplus \dots \oplus x_{k_s} \oplus c$ — аффинная булева функция, то

$$\mu_f(i, A) = w_\alpha(i).$$

ДОКАЗАТЕЛЬСТВО. П. (а) следует из определения функции $\mu_f(i, A)$.

- (б) Если $f(x)$ — аффинная функция, то $L(f) = \{x_{k_1}, \dots, x_{k_s}\}$. Тогда $\mu_f(i, A) = \max\{a_{i, k_1}, \dots, a_{i, k_s}\} = w_\alpha(i)$ в соответствии с теоремой 1(а), $0 \leq i < n$. Теорема 2 доказана.

Для преобразования $g(x)$ пространства V_n введём следующие обозначения: $\{g_0(x), \dots, g_{n-1}(x)\}$ — множество координатных булевых полиномов; $d_j^g = \deg g_j(x)$; $d^g = \max\{d_0^g, \dots, d_{n-1}^g\}$; $D_g = (d(i, g_j)) \in M_n$; $\sigma_\alpha(D_g) = \sum_{j \in \alpha} d_j^g$; $\Phi_\mu^g(A) = (\mu_{g_j}(i, A))$, $A \in M_n$; $0 \leq i, j < n$. Матрицу D_g назовём *deg-матрицей* преобразования $g(x)$.

Преобразование назовём *вырожденным*, если множество его координатных булевых полиномов содержит константу или каждый координатный булев полином не зависит от некоторой переменной x_i , $i \in \{0, \dots, n-1\}$, иначе преобразование *невырожденное*. Множество всех невырожденных преобразований пространства V_n обозначим через Π_n . Преобразование $g(x)$ невырожденное тогда и только тогда, когда матрица D_g неособенная.

Далее рассматриваем только невырожденные преобразования.

Теорема 3. (а) Преобразование Φ_μ^g множества M_n монотонно при любом $g(x) \in \Pi_n$.

(б) Для любых преобразований $g(x), h(x) \in \Pi_n$ верно $D_{gh} \leq \Phi_\mu^h(D_g)$.

ДОКАЗАТЕЛЬСТВО. (а) По теореме 1(а) величина $\mu_\alpha(i, A)$ неотрицательна при любом $\alpha \in 2^{[n]}$. Значит, $\mu_f(i, A) \geq 0$ при любой булевой функции $f(x) \neq \text{const}$. Отсюда $\Phi_\mu^g \in M_n$ при любом $g(x) \in \Pi_n$, т. е. Φ_μ^g — преобразование множества M_n .

Если $A \leq B$, то $\mu_\alpha(i, A) \leq \mu_\alpha(i, B)$ в соответствии с теоремой 1(б) при любом $\alpha \in 2^{[n]}$, $0 \leq i < n$. Тогда для любой булевой функции $f(x) \neq \text{const}$ выполнено

$$\mu_f(i, A) = \max_{\alpha: x^\alpha \in L(f)} \mu_\alpha(i, A) \leq \max_{\alpha: x^\alpha \in L(f)} \mu_\alpha(i, B) = \mu_f(i, B).$$

В частности, $\mu_{g_j}(i, A) \leq \mu_{g_j}(i, B)$ для булевой функции $g_j(x)$, $0 \leq i, j < n$, откуда $\Phi_\mu^g(A) \leq \Phi_\mu^g(B)$.

(б) По определению произведения преобразований двоичного пространства

$$(gh)_j(x) = h_j(g_0(x), \dots, g_{n-1}(x)), \quad 0 \leq j < n. \quad (3)$$

Алгебраическая нормальная форма булевой функции есть сумма по модулю 2 её мономов:

$$h_j(x) = \bigoplus_{\alpha: x^\alpha \in W(h_j)} x_{k_1} \dots x_{k_s},$$

где $\alpha = \{k_1, \dots, k_s\}$. Тогда в соответствии с (3)

$$(gh)_j(x) = \bigoplus_{\alpha: x^\alpha \in W(h_j)} h_j(g_{k_1}(x) \dots g_{k_s}(x)).$$

Отсюда если в полиноме $h_j(x)$ имеется моном $x^\alpha = x_{k_1} \dots x_{k_s}$, $s > 0$, то частью полинома $(gh)_j(x)$ является полином $q_\alpha(x) = g_{k_1}(x) \dots g_{k_s}(x)$ степени не выше $\sigma_\alpha(D_g) = d_{k_1}^g + \dots + d_{k_s}^g$. Если $\alpha \subseteq \beta$, то $\sigma_\alpha(D_g) \leq \sigma_\beta(D_g)$.

Значит, оценка $\sigma_\alpha(D_g)$ принимает наибольшее значение при α таком, что $x^\alpha \in L(h_j)$, $0 \leq j < n$, откуда

$$\deg(gh)_j(x) \leq \max_{\alpha: x^\alpha \in L(h_j)} \sigma_\alpha(D_g).$$

Уточним данное неравенство для оценки сверху величин $d(i, (gh)_j)$ с помощью функций $\mu_\alpha(i, D_g)$ и $\mu_f(i, D_g)$. По определению $\sigma_j(D_g) = d_j^g$, и ввиду (1)

$$\mu_\alpha(i, D_g) = \sigma_\alpha(D_g) + \max_{u \in \alpha: d(i, g_u) > 0} \{d(i, g_u) - d_u^g\},$$

если $d(i, g_u) = 0$, $u = k_1, \dots, k_s$, то $\mu_\alpha(i, D_g) = 0$; $0 \leq i < n$. Для зависимости от x_i функции $q_\alpha(x)$ необходимо, чтобы некоторая из функций $g_{k_1}(x), \dots, g_{k_s}(x)$ зависела от x_i — только в этом случае i -я строка матрицы $(D_g)_\alpha$ ненулевая. Если от x_i зависит функция $g_u(x)$, $u \in \alpha$, то полином $q_\alpha(x)$ может иметь зависящие от x_i мономы степени не больше $\sigma_\alpha(D_g) + d(i, g_u) - d_u^g$. Эта оценка верна при тех $u \in \alpha$, при которых $d(i, g_u) > 0$. При остальных значениях $u \in \alpha$ (если такие имеются) оценка равна 0, так как полином $q_\alpha(x)$ не зависит от x_i . Итак, если i -я строка матрицы $(D_g)_\alpha$ ненулевая, то $d(i, q_\alpha) \leq \mu_\alpha(i, D_g)$. Это неравенство верно при любом непустом α , в том числе если x^α — максимальный моном функции $h_j(x)$. Так как полином $q_\alpha(x)$ — часть полинома $(gh)_j(x)$, откуда $d(i, (gh)_j) \leq \mu_{h_j}(i, D_g)$. Теорема 3 доказана.

Координатные полиномы преобразования $g^t(x)$ обозначим через $g_0^t(x), \dots, g_{n-1}^t(x)$. Назовём *deg-графом* преобразования $g(x)$ орграф $\Gamma(D_g)$. Множество его вершин есть $\{0, \dots, n-1\}$, вершина j и дуга (i, j) помечены числами $\deg g_j$ и $d(i, g_j)$ соответственно (отсутствие дуги (i, j) в $\Gamma(D_g)$ равносильно отношению $i \notin S(g_j)$). В соответствии с обозначениями $\Gamma(D_g) \in \Gamma_{\bar{b}}(M_n)$ при $\bar{b} = (1, \dots, 1)$.

Пример 1. Пусть $x = (x_0, \dots, x_5)$ и $g(x)$ — преобразование множества V_6 с координатными функциями $x_2, x_0 \oplus x_1, x_2 \oplus x_0x_1, x_4 \oplus x_1, x_5, x_0 \oplus x_3x_4$. В deg-графе данного преобразования метки вершин заданы набором $(1, 1, 2, 1, 1, 2)$, а метки дуг — матрицей

$$(d(i, g_j)) = \begin{pmatrix} 0 & 1 & 2 & 0 & 0 & 1 \\ 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Для преобразований $g^{(1)}(x), \dots, g^{(t)}(x)$, $t \in \mathbb{N}$, введём обозначение $g^{[t]}(x) = g^{(1)} \dots g^{(t)}(x)$ — произведение t преобразований, а множества

координатных полиномов преобразований $g^{(t)}(x)$ и $g^{[t]}(x)$ обозначим через $\{g_0^{(t)}(x), \dots, g_{n-1}^{(t)}(x)\}$ и $\{g_0^{[t]}(x), \dots, g_{n-1}^{[t]}(x)\}$ соответственно.

Определим оценочные матрицы $E_{g^{[t]}}$ для deg-матриц $D_{g^{[t]}}$ произведения преобразований. Заметим, что оценка степени нелинейности булевой функции тривиальна, если её значение не меньше n ; если $g(x)$ — подстановка, то $\deg g_j < n$, $0 \leq j < n$. Положим

$$E_{g^{[1]}} = D_{g^{[1]}}, \quad E_{g^{[t]}} = (e_{i,j}^{[t]}) = \Phi_\mu^{g^{(t)}}(E_{g^{[t-1]}}), \quad t > 1. \quad (4)$$

Теорема 4. Для любых преобразований $g^{(1)}(x), \dots, g^{(t)}(x)$, $t > 1$,

$$D_{g^{[t]}} \leq E_{g^{[t]}}.$$

Доказательство. Индукция по t . При $t = 2$ оценка верна в силу теоремы 3(б). Пусть $t > 2$ и оценка верна при $t - 1$. Докажем её для t .

По теореме 3(б) $D_{g^{[t]}} \leq \Phi_\mu^{g^{(t)}}(D_{g^{[t-1]}})$, где по предположению индукции $D_{g^{[t-1]}} \leq E_{g^{[t-1]}}$. Отсюда в силу теоремы 3(а) с учётом (4) получаем

$$\Phi_\mu^{g^{(t)}}(D_{g^{[t-1]}}) \leq \Phi_\mu^{g^{(t)}}(E_{g^{[t-1]}}) = E_{g^{[t]}}.$$

Теорема 4 доказана.

Замечание 1. Вычисление оценочной матрицы $E_{g^{[t]}}$ с помощью рекуррентного соотношения (4) при $t > 2$ выполняется за $t - 1$ шагов при начальной матрице $D_{g^{[1]}}$, где матрица $E_{g^{[l]}}$ вычисляется на $(l - 1)$ -м шаге, $l = 2, \dots, t$. Для матрицы $D_{g^{[t]}}$ оценка $E_{g^{[t]}}$ менее точная, но и вычислительно менее сложная, чем $\Phi_\mu^{g^{(t)}}(D_{g^{[t-1]}})$, так как для вычисления не требуются матрицы $D_{g^{[l]}}$, $l > 1$. Оценки $E_{g^{[t]}}$ при некоторых t получаются нетривиальными.

Пример 2. Пусть $x = (x_0, \dots, x_5)$ и $g(x)$ — преобразование множества V_6 с координатными функциями $x_1, x_2 \oplus x_5, x_3, x_4, x_5, x_0 \oplus x_3x_4$. Отсюда $L(g_0) = \{x_1\}$, $L(g_1) = \{x_2, x_5\}$, $L(g_2) = \{x_3\}$, $L(g_3) = \{x_4\}$, $L(g_4) = \{x_5\}$, $L(g_5) = \{x_0, x_3x_4\}$, $(\sigma_0(A), \dots, \sigma_5(A)) = (d_0^g, \dots, d_5^g) = (1, 1, 1, 1, 1, 2)$, где

$$A = D_g = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Так как $\deg g(x) = 2$, для преобразования множества V_6 грубые оценки следующие: $\deg g^2(x) \leq 4$, $\deg g^t(x) \leq 6$, $t > 2$. С помощью теоремы 4

оценим deg-матрицы для $g^2(x)$ и $g^3(x)$, не вычисляя их координатные полиномы.

Обозначив $E_{g^{[t]}} = (e_{i,j}^{g^{[t]}})$ и используя (4), получаем

$$e_{i,j}^{g^{[2]}} = \mu_{g_j}(i, A) = \mu_{\alpha}(i, A), \quad 0 \leq i, j < 6.$$

$\alpha: x^\alpha \in L(g_j)$

Находим столбцы матрицы $B = (b_{i,j}) = E_{g^{[2]}}$:

$$b_{i,0} = \mu_{g_0}(i, A) = \mu_{\{1\}}(i, A) = d(i, g_1);$$

$$b_{i,1} = \mu_{g_1}(i, A) = \max\{\mu_{\{2\}}(i, A), \mu_{\{5\}}(i, A)\} = \max\{d(i, g_2), d(i, g_5)\};$$

$$b_{i,2} = \mu_{g_2}(i, A) = \mu_{\{3\}}(i, A) = d(i, g_3);$$

$$b_{i,3} = \mu_{g_3}(i, A) = \mu_{\{4\}}(i, A) = d(i, g_4);$$

$$b_{i,4} = \mu_{g_4}(i, A) = \mu_{\{5\}}(i, A) = d(i, g_5);$$

$$b_{i,5} = \mu_{g_5}(i, A) = \max\{\mu_{\{0\}}(i, A), \mu_{\{3,4\}}(i, A)\} = \max\{d(i, g_0), \delta_3, \delta_4\},$$

где $\delta_3 = d_3^g + d(i, g_4)$, если $d(i, g_4) > 0$, иначе $\delta_3 = 0$, и $\delta_4 = d_4^g + d(i, g_3)$, если $d(i, g_3) > 0$, иначе $\delta_4 = 0$.

$$\text{Результаты вычислений: } B = E_{g^{[2]}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 0 \\ 0 & 2 & 1 & 0 & 2 & 2 \\ 1 & 0 & 0 & 1 & 0 & 2 \end{pmatrix}.$$

Вновь используя (4), получаем

$$e_{i,j}^{g^{[3]}} = \mu_{g_j}(i, B) = \mu_{\alpha}(i, B), \quad 0 \leq i, j < 6.$$

$\alpha: x^\alpha \in L(g_j)$

Находим столбцы матрицы $C = (c_{i,j}) = E_{g^{[3]}}$:

$$c_{i,0} = \mu_{g_0}(i, B) = \mu_{\{1\}}(i, B) = b_{i,1};$$

$$c_{i,1} = \mu_{g_1}(i, B) = \max\{\mu_{\{2\}}(i, B), \mu_{\{5\}}(i, B)\} = \max\{b_{i,2}, b_{i,5}\};$$

$$c_{i,2} = \mu_{g_2}(i, B) = \mu_{\{3\}}(i, B) = b_{i,3};$$

$$c_{i,3} = \mu_{g_3}(i, B) = \mu_{\{4\}}(i, B) = b_{i,4};$$

$$c_{i,4} = \mu_{g_4}(i, B) = \mu_{\{5\}}(i, B) = b_{i,5};$$

$$c_{i,5} = \mu_{g_5}(i, B) = \max\{\mu_{\{0\}}(i, B), \mu_{\{3,4\}}(i, B)\} = \max\{b_{i,0}, \varepsilon_3, \varepsilon_4\}, \text{ где}$$

$\varepsilon_3 = \sigma_3(B) + b_{i,4}$, если $b_{i,4} > 0$, иначе $\varepsilon_3 = 0$, и $\varepsilon_4 = \sigma_4(B) + b_{i,3}$, если $b_{i,3} > 0$, иначе $\varepsilon_4 = 0$.

$$\text{Результаты вычислений: } C = E_{g^{[3]}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 2 & 0 & 3 \\ 2 & 2 & 0 & 2 & 2 & 3 \\ 0 & 2 & 1 & 0 & 2 & 3 \end{pmatrix}.$$

Для характеристики точности данных оценок посчитаны deg-матрицы преобразований $g^2(x)$ и $g^3(x)$. Установлено, что

$$D_{g^{[2]}} = E_{g^{[2]}}, \quad D_{g^{[3]}} = E_{g^{[3]}}.$$

3. О нетривиальности оценок характеристик нелинейности

К важным для приложений характеристикам преобразований $g^t(x)$, $t \geq 1$, относятся степени нелинейности производных их координатных полиномов и область нетривиальности таких оценок, т. е. значения t , при которых соответствующие оценки нетривиальны. Важны также значения оценочной функции в области нетривиальности.

Оценки можно получить с помощью оценочных матриц E_{g^t} и с помощью характеристик орграфа $\Gamma(D_g)$. Если способ оценивания основан на вычислении монотонных по t функций, то для определения области нетривиальности оценок достаточно найти наибольшее значение t , при котором оценка нетривиальна.

Оценим области нетривиальности с помощью орграфа $\Gamma(D_g)$. Если преобразование $g(x)$ невырожденное, то орграф $\Gamma(D_g)$ содержит несколько компонент сильной связности (КСС). Напомним, что КСС — это максимальный подграф, где любые две вершины, не обязательно различные, взаимно достижимы, т. е. существует как путь из одной вершины в другую, так и обратный путь. В частности, КСС может состоять из одной вершины с петлёй, откуда любые две КСС не являются взаимно достижимыми.

В орграфе $\Gamma(D_g)$ обозначим через $V_j^{(t)}$ множество вершин, из которых существует путь в вершину j длины t , $0 \leq j < n$, $t \geq 1$.

Теорема 5. Для характеристик преобразования $g^t(x)$ верны следующие оценки, $0 \leq i, j < n$:

$$(a) \ S(g_j^t) \subseteq V_j^{(t)}, \ t \geq 1;$$

$$(b) \ d(i, g_j^t) \leq \min\{|V_j^{(t)}|, e_{i,j,t}\}, \text{ если } i \in V_j^{(t)}, \text{ иначе } d(i, g_j^t) = 0, \text{ где в соответствии с (4)}$$

$$E_{g^t} = (e_{i,j,t}) = \Phi_\mu^g(E_{g^{t-1}}), \quad t > 1.$$

ДОКАЗАТЕЛЬСТВО. (а) Индукция по t . При $t = 1$ теорема следует из определения deg-графа преобразования g . Пусть теорема верна для $t - 1$, докажем её для t .

Без ущерба для общности положим $V_j^{(1)} = \{0, \dots, r - 1\}$, $1 \leq r \leq n$. Тогда в силу свойства путей в орграфе

$$V_j^{(t)} = \bigcup_{k=0}^{r-1} V_k^{(t-1)}.$$

В соответствии с определением произведения преобразований

$$g_j^t(x) = g_j(g_0^{t-1}(x), \dots, g_{n-1}^{t-1}(x)).$$

Тогда в силу равенства $S(g_j) = V_j^{(1)}$ и с учётом предположения индукции отсюда получаем

$$S(g_j^t) \subseteq \bigcup_{k=0}^{r-1} S(g_k^{t-1}) \subseteq \bigcup_{k=0}^{r-1} V_k^{t-1} = V_j^{(t)}.$$

(б) Неравенство $d(i, g_j^t) \leq e_{i,j,t}$ следует из биекции $M_n \leftrightarrow \Gamma(M_n)$ и теоремы 4. Неравенство $d(i, g_j^t) \leq |V_j^{(t)}|$ следует из теоремы 5(а) и соотношения $d(i, g_j^t) \leq |S(g_j^t)|$. Теорема 5 доказана.

Ещё один способ основан на определении экспонента примитивного орграфа $\Gamma(D_g)$. При удалении всех меток орграф $\Gamma(D_g)$ преобразуется в перемешивающий орграф преобразования $g(x)$: пара (i, j) является дугой тогда и только тогда, когда $g_j(x)$ зависит существенно от x_i , $0 \leq i, j < n$. Значит, если орграф $\Gamma(D_g)$ примитивный, то матрица D_{g^t} допускает нетривиальную оценку при $t < \exp D_g$. Отсюда наибольшую область нетривиальности имеет преобразование, перемешивающий орграф которого есть орграф Виландта (с наибольшим экспонентом), т. е. орграф, являющийся объединением контуров $(0, 1, \dots, n-1)$ и $(1, \dots, n-1)$. Экспонент такого орграфа равен $n^2 - 2n + 2$.

Соответствующее преобразование $g(x)$ является преобразованием двоичного регистра левого сдвига длины n множеством координатных полиномов:

$$g(x) = \{x_1, \dots, x_{n-1}, x_0 x_1\}. \quad (5)$$

Известно, что координатные функции различных степеней регистрового преобразования $g(x)$ совпадают с точностью до сдвига δ , а именно, $g_j^t(x) = g_{j-\delta}^{t+\delta}(x)$, $0 \leq j - \delta < j < n$, $t \geq 1$. Значит, достаточно оценить характеристики нелинейности полиномов из последовательности $\{g_0^t(x)\}$, $t \geq 0$, где $g^0(x)$ — тождественное преобразование.

Обозначим через $\overline{x^\alpha}$ минимальный моном, дополняющий моном x^α до монома $x_0 x_1 \dots x_{n-1}$, т. е. конъюнкцию наименьшего ранга со свойством $\overline{x^\alpha} x^\alpha = x_0 x_1 \dots x_{n-1}$.

Теорема 6. Для регистрового преобразования $g(x)$, заданного (5), имеем

$$\deg g_0^t(x) = \begin{cases} 1, & t = 0, \dots, n-1; \\ k, & (k-1)(n-1) + 1 \leq t \leq k(n-1), \quad k = 2, \dots, n-1; \\ n, & t > (n-1)^2. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Из (5) следует, что

$$g_0^t(x) = g_0^{t-n}(x)g_0^{t-n+1}(x), \quad t \geq n.$$

Последовательно применяя это рекуррентное соотношение для $t = n, n+1, \dots$, получаем, что последовательность $\{g_0^t(x)\}$ разбивается на n отрезков, где каждый отрезок состоит из функций одинаковой степени нелинейности, а именно,

- 1-й отрезок состоит из n функций x_t степени 1, $t = 0, \dots, n-1$;
- 2-й отрезок состоит из $n-1$ функций вида x_tx_{t+1} степени 2, $t = 0, \dots, n-2$;
- 3-й отрезок состоит из функции $x_0x_1x_{n-1}$ и $n-2$ функций вида $x_tx_{t+1}x_{t+2}$ степени 3, $t = 0, \dots, n-3$ (заметим, что $x_0x_1x_{n-1} = \overline{x_2 \dots x_{n-2}}$) и т. д.;
- k -й отрезок состоит из $k-2$ функций вида $\overline{x_tx_{t+1} \dots x_{t+n-k-1}}$, где $t = 2, 3, \dots, k-1$, и $n-k+1$ функций вида $x_tx_{t+1} \dots x_{t+k-1}$ степени k , где $t = 0, \dots, n-k$, $k = 3, \dots, n-1$;

Таблица 1

deg-Матрицы и оценочные матрицы для степеней преобразования $g(x)$

t	deg-матрица D_{g_t}	оценка E_{g_t}	t	deg-матрица D_{g_t}	оценка E_{g_t}
1	$\begin{pmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	6	$\begin{pmatrix} 0 & 3 & 3 & 0 \\ 0 & 3 & 3 & 3 \\ 2 & 0 & 3 & 3 \\ 2 & 3 & 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 0 & 3 & 4 & 0 \\ 0 & 3 & 4 & 4 \\ 2 & 0 & 4 & 4 \\ 2 & 3 & 0 & 4 \end{pmatrix}$
2	$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	7	$\begin{pmatrix} 3 & 3 & 0 & 4 \\ 3 & 3 & 3 & 4 \\ 0 & 3 & 3 & 4 \\ 3 & 0 & 3 & 4 \end{pmatrix}$	$\begin{pmatrix} 3 & 4 & 0 & 4 \\ 3 & 4 & 4 & 4 \\ 0 & 4 & 4 & 4 \\ 3 & 0 & 4 & 4 \end{pmatrix}$
3	$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 1 & 0 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 1 & 0 & 0 & 2 \end{pmatrix}$	8	$\begin{pmatrix} 3 & 0 & 4 & 4 \\ 3 & 3 & 4 & 4 \\ 3 & 3 & 4 & 4 \\ 0 & 3 & 4 & 4 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 0 & 4 & 4 & 4 \end{pmatrix}$
4	$\begin{pmatrix} 2 & 0 & 0 & 3 \\ 2 & 2 & 0 & 3 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 & 0 & 3 \\ 2 & 2 & 0 & 3 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 3 \end{pmatrix}$	9	$\begin{pmatrix} 0 & 4 & 4 & 4 \\ 3 & 4 & 4 & 4 \\ 3 & 4 & 4 & 4 \\ 3 & 4 & 4 & 4 \end{pmatrix}$	$\begin{pmatrix} 0 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$
5	$\begin{pmatrix} 0 & 0 & 3 & 3 \\ 2 & 0 & 3 & 3 \\ 2 & 2 & 0 & 3 \\ 0 & 2 & 3 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 3 & 4 \\ 2 & 0 & 3 & 4 \\ 2 & 2 & 0 & 4 \\ 0 & 2 & 3 & 0 \end{pmatrix}$	10	$\begin{pmatrix} 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$\begin{pmatrix} 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$

• при $t > n^2 - 2n + 1$ имеет место $g_0^t(x) = x_0x_1 \dots x_{n-1}$, т. е. в этом случае степень $g_0^t(x)$ равна n .

Таким образом определены степени нелинейности всех функций. Теорема 6 доказана.

Сравним оценочные матрицы с результатами теоремы 6 на примере при $n = 4$.

Пример 3. Сравнение deg-матриц D_g^t с оценками E_g^t при $g(x)$, заданном (5), $n = 4$, $t \geq 1$. Из (5) следует, что

$$\{g_0^t(x)\} = \{x_0, x_1, x_2, x_3, x_0x_1, x_1x_2, x_2x_3, \\ x_0x_1x_3, x_0x_1x_2, x_1x_2x_3, x_0x_1x_2x_3, x_0x_1x_2x_3, x_0x_1x_2x_3, \dots\},$$

отсюда определяются deg-матрицы D_g^t , $t \geq 1$.

Учитывая, что

$$L(g_j) = \{x_{j+1}\}, j = 0, 1, 2, \quad L(g_3) = \{x_0, x_1\}, \\ (\sigma_0(A), \dots, \sigma_3(A)) = (d_0^g, \dots, d_3^g) = (1, 1, 1, 2),$$

определяем с помощью (1) оценочные матрицы. Полученные результаты представлены в табл. 1.

Вычисления показывают, что оценочные матрицы нетривиальны для $g(x)$, $g^2(x)$, \dots , $g^9(x)$, что согласуется со значением экспонента орграфа, равным 10, и полностью совпадают с deg-матрицами для $g(x)$, $g^2(x)$, $g^3(x)$ и $g^4(x)$.

ЛИТЕРАТУРА

1. Фомичёв В. М., Авезова Я. Э., Коренева А. М., Кяжин С. Н. Прimitивность и локальная примитивность орграфов и неотрицательных матриц // Дискрет. анализ и исслед. операций. 2018. Т. 25, № 3. С. 95–125.
2. Fomichev V. M., Koreneva A. M. Encryption performance and security of certain wide block ciphers // J. Comput. Virol. Hack. Tech. 2020. Vol. 16. P. 197–216.
3. Фомичёв В. М., Бобров В. М. Оценка с помощью матрично-графового подхода характеристик локальной нелинейности итераций преобразований векторных пространств // Прикл. дискрет. математика. Прил. 2019. № 12. С. 32–35.
4. Frobenius G. Über Matrizen aus nicht negativen Elementen // Berl. Ber. 1912. S. 456–477. [German].
5. Wielandt H. Unzerlegbare, nicht negative Matrizen // Math. Z. 1950. Bd. 52. S. 642–648. [German].
6. Perkins P. A theorem on regular graphs // Pac. J. Math. 1961. Vol. 2. P. 1529–1533.

7. **Dulmage A. L., Mendelsohn N. S.** The exponent of a primitive matrix // Can. Math. Bull. 1962. Vol. 5, No. 3. P. 241–244.
8. **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.
9. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. Vol. 14, No. 4. P. 483–499.
10. **Neufeld S. W.** A diameter bound on the exponent of a primitive directed graph // Lin. Algebra Appl. 1996. Vol. 245. P. 27–47.
11. **Liu B.** Generalized exponents of Boolean matrices // Lin. Algebra Appl. 2003. Vol. 373. P. 169–182.
12. **Sachkov V. N., Tarakanov V. E.** Combinatorics of nonnegative matrices. Providence, RI: AMS, 2002. 269 p. (Transl. Math. Monogr.; Vol. 213).
13. **Фомичёв В. М., Кяжин С. Н.** Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24, № 1. С. 97–119.
14. **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.; Vol. 6147).
15. **Berger T., Francq J., Minier M., Thomas G.** Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput // IEEE Trans. Comput. 2016. Vol. 65, No. 7. P. 2074–2089.
16. **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.; Vol. 8282).
17. **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.; Vol. 1163).
18. **Логачёв О. А., Сальников А. А., Яценко В. В.** Булевы функции в теории кодирования и криптологии. М: МЦНМО, 2004. 470 с.

Фомичёв Владимир Михайлович

Статья поступила

28 сентября 2020 г.

После доработки —

15 февраля 2021 г.

Принята к публикации

19 февраля 2021 г.

ON DEGREE OF NONLINEARITY OF THE COORDINATE
POLYNOMIALS FOR A PRODUCT OF TRANSFORMATIONS
OF A BINARY VECTOR SPACE

V. M. Fomichev^{1,2,3}

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

² Security Code LLC,
10 Bld. 1 Pervyi Nagatinskii Driveway, 115230 Moscow, Russia

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

E-mail: `fomichev.2016@yandex.ru`

Abstract. We construct a nonnegative integer matrix to evaluate the matrix of nonlinearity characteristics for the coordinate polynomials of a product of transformations of a binary vector space. The matrix of the characteristics of the transformation is defined by the degrees of nonlinearity of the derivatives of all coordinate functions with respect to each input variable. The entries of the evaluation matrix are expressed in terms of the characteristics of the coordinate polynomials of the multiplied transformations. Calculation of the evaluation matrix is easier than calculating the exact values of the characteristics. The estimation method is extended to an arbitrary number of multiplied transformations. Computational examples are given that in particular show the accuracy of the obtained estimates and the domain of their nontriviality. Tab. 1, bibliogr. 18.

Keywords: coordinate polynomial of transformation, maximal monomial of a polynomial, degree of a polynomial.

REFERENCES

1. **V. M. Fomichev, Ya. Eh. 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)].
2. **V. M. Fomichev and A. M. Koreneva**, Encryption performance and security of certain wide block ciphers, *J. Comput. Virol. Hack. Tech.* **16**, 197–216 (2020).
3. **V. M. Fomichev and V. M. Bobrov**, Estimation of local nonlinearity characteristics of vector space transformation iteration using matrix-graph approach, *Prikl. Diskretn. Mat., Prilozh.*, No. 12, 32–35 (2019) [Russian].
4. **G. Frobenius**, Über Matrizen aus nicht negativen Elementen, *Berl. Ber.*, 456–477 (1912) [German].
5. **H. Wielandt**, Unzerlegbare, nicht negative Matrizen, *Math. Z.* **52**, 642–648 (1950) [German].
6. **P. Perkins**, A theorem on regular graphs, *Pac. J. Math.* **2**, 1529–1533 (1961).
7. **A. L. Dulmage and N. S. Mendelsohn**, The exponent of a primitive matrix, *Can. Math. Bull.* **5** (3), 241–244 (1962).
8. **A. L. Dulmage and N. S. Mendelsohn**, Gaps in the exponent set of primitive matrices, *Ill. J. Math.* **8** (4), 642–656 (1964).
9. **R. A. Brualdi and B. Liu**, Generalized exponents of primitive directed graphs, *J. Graph Theory.* **14** (4), 483–499 (1990).
10. **S. W. Neufeld**, A diameter bound on the exponent of a primitive directed graph, *Lin. Algebra Appl.* **245**, 27–47 (1996).
11. **B. Liu**, Generalized exponents of Boolean matrices, *Lin. Algebra Appl.* **373**, 169–182 (2003).
12. **V. N. Sachkov and V. E. Tarakanov**, *Combinatorics of Nonnegative Matrices* (AMS, Providence, RI, 2002) (Transl. Math. Monogr., Vol. 213).
13. **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)].
14. **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).
15. **T. 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).
16. **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).

17. **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).
18. **O. A. Logachyov, A. A. Salnikov, and V. V. Yashchenko**, *Boolean Functions in Coding Theory and Cryptology* (MTsNMO, Moscow, 2004).

Vladimir M. Fomichev

Received September 28, 2020

Revised February 15, 2021

Accepted February 19, 2021