ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь–декабрь 2020. Т. 27, № 4. С. 131–151

УДК 519.17 DOI 10.33048/daio.2020.27.686

ОЦЕНКА ХАРАКТЕРИСТИК НЕЛИНЕЙНОСТИ ИТЕРАТИВНЫХ ПРЕОБРАЗОВАНИЙ ВЕКТОРНОГО ПРОСТРАНСТВА

В. М. Фомичёв [1, 2, 3]

[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

E-mail: fomichev.2016@yandex.ru

Аннотация. Представлены теоретические основы матрично-графового подхода (МГП) к оценке характеристик множеств существенных и нелинейных переменных композиции преобразований n-мерного векторного пространства над полем. Преобразованию соответствует троичная матрица нелинейности, где в i-й строке и j-м столбце матрицы записано число 0, 1 или 2 тогда и только тогда, когда j-я координатная функция преобразования зависит от i-й переменной фиктивно, линейно или нелинейно соответственно, $0 \leqslant i, j < n$. Основой МГП является неравенство, согласно которому матрица нелинейности произведения преобразований не больше (неравенство поэлементное) произведения матриц нелинейности тех же преобразований.

Определена операция умножения троичных матриц. Исследованы свойства мультипликативного моноида всех троичных матриц порядка n без нулевых строк и столбцов и биективно соответствующего ему моноида $\mathbb{\Gamma}_n$ всех n-вершинных орграфов с дугами, помеченными числами $0, 1, 2$, где каждая вершина имеет ненулевые полустепени захода и исхода. С помощью МГП оценена глубина итерации (число умножаемых) преобразований, при которой могут быть достигнуты 4 вида нелинейности преобразований, при которых каждая или некоторые координатные функции произведения преобразований могут зависеть нелинейно от всех или хотя бы от некоторых переменных.

Представлены результаты исследования нелинейности итераций раундовых подстановок блочных шифров DES и «Магма». Библиогр. 18.

Ключевые слова: матрица (орграф) нелинейности преобразования, $\langle\alpha\rangle$-примитивная матрица (орграф), $\langle\alpha\rangle$-экспонент матрицы (орграфа), $\langle\alpha\rangle$-перфективное преобразование.

Основные обозначения

- $\mathbb{N}$ — множество всех натуральных чисел, $n \in \mathbb{N}$;
- $\mathbb{N}_p^*$ — множество всех слов в алфавите $\{1, \ldots, p\}$, $p \in \mathbb{N}$;
- $w(i, j)$ — путь в орграфе из вершины i в вершину j;
- $\operatorname{len} w$ — длина пути w в орграфе, равная числу составляющих дуг;
- $w \bullet w'$ — конкатенация путей w и w', где совпадают последняя вершина пути w и первая вершина пути w';
- $(b)_n$ — квадратная матрица порядка n, где все элементы равны b, $b = 0, 1, \ldots$;
- $\mathbb{M}_n^{0,1}$ — множество квадратных $(0,1)$-матриц порядка n без нулевых строк и столбцов;
- $\mathbb{M}_n^{0,1,2}$ — множество квадратных матриц порядка n над множеством $\{0,1,2\}$ без нулевых строк и столбцов;
- $\langle\widehat{M}\rangle$ — мультипликативная полугруппа, порождённая множеством матриц $\widehat{M}$;
- $\langle\widehat{G}\rangle$ — мультипликативная полугруппа, порождённая множеством $\widehat{G}$ преобразований векторного пространства;
- $\mathbb{\Gamma}_n$ — класс всех орграфов с множеством дуг, помеченных числами $0, 1, 2$, и с множеством вершин $\{0, \ldots, n-1\}$, где любая вершина имеет ненулевые полустепени захода и исхода;
- $Z(2) = \{2c, 2s, 2sc, 2\}$ — множество символов;
- $\langle\alpha\rangle\text{-}\exp\Gamma$ — α-экспонент орграфа Γ, $\alpha \in Z(2)$;
- $\langle\alpha\rangle\text{-}\exp M$ — α-экспонент матрицы M, $\alpha \in Z(2)$;
- $\mathbb{\Pi}(X)$ — множество всех преобразований множества X;
- МГП — матрично-графовый подход.

Введение

Одной из задач анализа композиции нелинейных преобразований векторного пространства является определение характеристик координатных функций, таких как множества существенных переменных и нелинейных переменных.

Для исследования множества существенных переменных композиций нелинейных преобразований векторных пространств активно применяется матрично-графовый подход (МГП) [1–4]. Суть МГП состоит в том, что наличие или отсутствие зависимости координатных функций преобразований от входных переменных кодируется нулём или единицей соответственно и устанавливается отношение между произведением матриц

(или орграфов), связанных с рядом нелинейных преобразований, и матрицей (или орграфом), связанной с композицией этих преобразований. Умножение матриц и орграфов определено как полугрупповая операция.

Важным для приложений свойством является положительность произведения перемешивающих матриц (полнота произведения перемешивающих орграфов) преобразований, что определено как примитивность множества перемножаемых матриц (орграфов). Наименьшее число перемножаемых матриц (орграфов), при которых достигается данное свойство, называется экспонентом соответствующего множества матриц (орграфов). Основные математические задачи МГП состоят в получении критериев примитивности и локальной примитивности множеств $(0,1)$-матриц (орграфов) и оценок их экспонентов и локальных экспонентов. Инициированная постановкой задачи Фробениусом [5] в 1912 г. история получения основных результатов, связанных с оценками экспонентов матриц и графов, отражена в [4]. Начальные фундаментальные результаты по оценке экспонентов получены в [6–12].

Одно из прикладных направлений связано с построением оперирующих с блоками большого размера симметричных блочных алгоритмов из класса WBC (wide block ciphers), например, алгоритмов с размером блока 256 бит и более, раундовая подстановка которых построена на основе регистра сдвига с несколькими обратными связями (обобщение сетей Фейстеля). В ряде работ исследован класс $R(n,r,m)$ регистров сдвига длины n с m обратными связями, где в каждой ячейке регистра записан двоичный r-битовый вектор, $1 \leqslant m < n$, $n,r,m \in \mathbb{N}$. Класс $R(2,32,1)$ соответствует оригинальным сетям Фейстеля, классы $R(n,r,1)$, $R(n,r,n/2)$, $R(n,r,n-1)$ соответствуют обобщённым сетям Фейстеля 1, 2 и 3-го типов [13, 14]. Расширенные обобщённые сети Фейстеля исследованы в [15, 16]. Производительность блочных алгоритмов, построенных на основе класса $R(n,r,m)$, изучена в [17].

Нелинейность является фундаментальным свойством функций, применяемых в криптографических системах. Свойство нелинейности выражается через весьма обширное множество характеристик. Одна из них так и названа — нелинейность булевой функции (работы Ньюберг и многих др.), определяющая в метрике Хэмминга расстояние N_f от f до множества аффинных функций. Неравновероятность максимально нелинейных функций (для них N_f достигает наибольшего из возможных значений при фиксированном чётном числе переменных) заметно ограничила их применение в криптографических алгоритмах. Другие характеристики нелинейности булевых функций связаны с N_f в общем случае достаточно сложно и зачастую требуют иных методов исследования.

В работе с использованием положений теории признаков в полугруппах [2, гл. 9] МГП распространён на оценки важнейших характеристик

нелинейности композиций преобразований векторного n-мерного пространства. С помощью троичных матриц порядка n над мультипликативной полугруппой $G = \{0, 1, 2\}$ и n-вершинных орграфов с помеченными дугами исследованы условия, при которых возможна нелинейная зависимость каждого бита двоичного выходного вектора от каждого бита двоичного входного вектора.

Важные для приложений криптографические функции часто реализуют с помощью композиции относительно несложных функций, удобно реализуемых аппаратно и/или программно, например, как в симметричных блочных шифрах, где зашифрование и расшифрование выполняется за несколько раундов однотипных вычислений. Точное определение характеристик нелинейности композиции функций в общем случае — нетривиальная задача.

В работе исследованы 4 вида нелинейности композиций преобразований векторного n-мерного пространства, в частности, зависимость

(а) каждого бита выходного вектора от некоторых битов входного вектора;

(б) некоторых битов выходного вектора от каждого бита входного вектора;

(в) при которой совместно выполнены условия (а) и (б);

(г) каждого бита выходного вектора от каждого бита входного вектора.

Ряд результатов по исследованию нелинейности вида (г) получен в [18].

1. Положения теории признаков в полугруппах

Пусть G' — конечная полугруппа, $S = \{s_1, \dots, s_p\} \subset G'$, $p \in \mathbb{N}$, $G = \langle S \rangle$ — полугруппа, порождённая множеством S. Любой элемент полугруппы G представим словом $(s_{i_1}, \dots, s_{i_t})$ в алфавите S, где $i_1, \dots, i_t \in \{1, \dots, p\}$, $t \in \mathbb{N}$. Будем писать, что *слово* $(s_{i_1}, \dots, s_{i_t})$ *в алфавите* S *принадлежит* $H \subseteq G$ (*равно* $g \in G$), если $s_{i_1} \dots s_{i_t} \in H$ ($s_{i_1} \dots s_{i_t} = g$). *Длиной элемента* g *в системе* S, обозначаемой $\mathrm{len}(g, S)$, называют наименьшую длину слова в алфавите S, равного g.

Подмножество H полугруппы G', состоящее из всех элементов с определённым свойством, назовём *признаком* H *в полугруппе* G'. Элемент g полугруппы G' *имеет признак* H, если $g \in H$. Непустое множество $Q \subseteq G'$ *имеет признак* H, если в $Q \cap H \neq \varnothing$; Q *не имеет признака* H или *имеет пустой признак* H, если $Q \cap H = \varnothing$. *Показателем* признака H в системе S называется $\min\limits_{g \in H} \mathrm{len}(g, S)$ — наименьшая из длин всех элементов множества H в системе S. Если полугруппа $\langle S \rangle$ не имеет признака H, то показатель признака H в системе S равен ∞. В частности, показатель признака H в одноэлементной системе $\{g\}$ есть наименьшее $t \in \mathbb{N}$ такое, что $g^t \in H$.

Признак H в полугруппе G называется *идеальным,* если $G \cap H$ — двусторонний идеал полугруппы G. Если слово w в алфавите S принадлежит идеальному признаку H в полугруппе $\langle S\rangle$, то любое продолжение слова w также принадлежит H. Если H — идеальный признак в циклической полугруппе $\langle g\rangle$, то $g^\tau \in H$ при любом τ, не меньшем показателя признака H.

Используя данные положения, исследуем свойства мультипликативных полугрупп матриц, полугрупп орграфов и полугрупп преобразований векторных пространств.

2. Свойства мультипликативных моноидов троичных матриц

В комбинаторном анализе активно исследуются *неотрицательные* матрицы, все элементы которых суть неотрицательные действительные числа. Свойство неотрицательности матрицы M записывают так: $M \geqslant 0$. Матрицу M, все элементы которой положительны, называют *положительной,* в этом случае пишут $M > 0$.

При замене всех положительных элементов единицами мультипликативный моноид всех неотрицательных матриц гомоморфно отображается на конечный мультипликативный моноид $\mathbb{M}_n^{0,1}$ всех $(0,1)$-матриц (все элементы которых суть 0 или 1). Умножение $(0,1)$-матриц $A = (a_{i,j})$ и $B = (b_{i,j})$ порядка n определено формулой: $AB = C = (c_{i,j})$, где

$$c_{i,j} = \max\{a_{i,1}b_{1,j}, \ldots, a_{i,n}b_{n,j}\}. \tag{1}$$

Назовём неотрицательную матрицу *особенной,* если она имеет нулевую строку или нулевой столбец. В противном случае матрица неособенная.

Множество $\mathbb{M}_n^{0,1}$ образует мультипликативный моноид. Пусть $\mathbb{M}_n^{0,1} \supseteq \widehat{M} = \{M_1, \ldots, M_p\}$ — множество неособенных $(0,1)$-матриц, $p \in \mathbb{N}$. Если полугруппа $\langle\widehat{M}\rangle$ содержит матрицу $(1)_n$, то множество $\widehat{M}$ называется *примитивным* и наименьшая длина слова w в алфавите $\widehat{M}$, равного $(1)_n$, называется *экспонентом* множества $\widehat{M}$ и обозначается через $\exp\widehat{M}$. В противном случае множество $\widehat{M}$ не примитивное и $\exp\widehat{M} = \infty$. Одноэлементное множество $\{(1)_n\}$ есть идеальный признак в полугруппе $\langle\widehat{M}\rangle$, порождённой примитивным множеством матриц $\widehat{M}$, и $\exp\widehat{M}$ есть показатель этого признака. В частности, при $p = 1$ наименьшее $\gamma \in \mathbb{N}$, при котором $M^\gamma > 0$, есть экспонент *примитивной* матрицы M, который обозначается через $\exp M$. Все особенные матрицы непримитивные.

Множество неотрицательных матриц частично упорядочено: если $A = (a_{i,j})$ и $B = (b_{i,j})$, то $A \leqslant B$ тогда и только тогда, когда $a_{i,j} \leqslant b_{i,j}$ для всех пар (i,j). Для экспонентов примитивных матриц выполнено свойство антимонотонности: если $A \leqslant B$ и матрица A примитивная, то матрица B также примитивная и $\exp A \geqslant \exp B$.

Важным для приложений обобщением свойства примитивности множества матриц является так называемая локальная примитивность матрицы M, связанная с положительностью определённой части матриц [3, с. 190]. Основные результаты исследования экспонентов и локальных экспонентов матриц (орграфов), а также примитивности и экспонентов множеств матриц (орграфов) см. в [4].

Пусть G — коммутативная полугруппа, где $\tau 0 = 0$ для любого $\tau \in G$ и $\tau\sigma = \max\{\tau, \sigma\}$ для любых $\tau, \sigma \neq 0$. Матрицы над $G = \{0, 1, 2\}$ назовём *троичными матрицами.* Множество неособенных троичных матриц, обозначаемое $\mathbb{M}_n^{0,1,2}$, образует мультипликативный моноид, где умножение определено формулой (1) и при вычислении $c_{i,j}$ для любых i, j умножение элементов матрицы выполняется в полугруппе G.

Определим множество символов $Z(2) = \{2c, 2s, 2sc, 2\}$. Назовём троичную неособенную матрицу M *α-матрицей,* $\alpha \in Z(2)$, если

а) при $\alpha = 2c$ каждый столбец M содержит элемент 2;

б) при $\alpha = 2s$ каждая строка M содержит элемент 2;

в) при $\alpha = 2sc$ все строки и столбцы M содержат элемент 2;

г) $M = (2)_n$ при $\alpha = 2$.

Обозначим через $\mathbb{M}_n^{\langle\alpha\rangle}$ множество всех α-матриц, $\alpha \in Z(2)$. В силу определения выполнено

$$\mathbb{M}_n^{\langle 2\rangle} \subseteq \mathbb{M}_n^{\langle 2sc\rangle} = \mathbb{M}_n^{\langle 2c\rangle} \cap \mathbb{M}_n^{\langle 2s\rangle}.$$

Утверждение 1. *Множество $\mathbb{M}_n^{\langle\alpha\rangle}$ есть двусторонний идеал моноида $\mathbb{M}_n$ при любом $\alpha \in Z(2)$.*

Доказательство. Покажем, что $\mathbb{M}_n^{\langle 2c\rangle}$ — двусторонний идеал, т. е. $\mathbb{M}_n\mathbb{M}_n^{\langle 2c\rangle} \subseteq \mathbb{M}_n^{\langle 2c\rangle}$ и $\mathbb{M}_n^{\langle 2c\rangle}\mathbb{M}_n \subseteq \mathbb{M}_n^{\langle 2c\rangle}$. Пусть $A = (a_{i,j}) \in \mathbb{M}_n$, $B = (b_{i,j}) \in \mathbb{M}_n^{\langle 2c\rangle}$, $AB = C = (c_{i,j})$, $BA = D = (d_{i,j})$, $0 \leqslant i, j < n$.

По определению множества $\mathbb{M}_n^{\langle 2c\rangle}$ имеем $b_{r(j),j} = 2$ при некотором $r(j) \in \{0, \ldots, n-1\}$, $j = 0, \ldots, n-1$. По условию $a_{i,r(j)} > 0$ при некотором $i \in \{0, \ldots, n-1\}$. Тогда в соответствии с операцией умножения троичных матриц $c_{i,j} \geqslant a_{i,r(j)}b_{r(j),j} = 2$, а значит, $c_{i,j} = 2$ при некотором $i \in \{0, \ldots, n-1\}$, $j = 0, \ldots, n-1$. Тем самым $\mathbb{M}_n^{\langle 2c\rangle}$ — левый идеал.

По условию $a_{s,j} > 0$ при некотором $s \in \{0, \ldots, n-1\}$, $j = 0, \ldots, n-1$. Тогда в соответствии с операцией умножения троичных матриц $d_{r(s),j} \geqslant b_{r(s),s}a_{s,j} = 2$, а значит, $d_{i,j} = 2$ при некотором $i \in \{0, \ldots, n-1\}$, $j = 0, \ldots, n-1$. Тем самым $\mathbb{M}_n^{\langle 2c\rangle}$ — правый идеал.

Для остальных значений α соотношения доказываются аналогично. Утверждение 1 доказано.

Следствие 1. *Если в алфавите $\widehat{M}$ слово w принадлежит $\mathbb{M}_n^{\langle\alpha\rangle}$, то любое продолжение слова w также принадлежит $\mathbb{M}_n^{\langle\alpha\rangle}$, $\alpha \in Z(2)$.*

Далее $\widehat{M} = \{M_1, \dots, M_p\}$ — множество неособенных троичных матриц, $p \in \mathbb{N}$. Обозначим через $w = (i_1, \dots, i_t)$ слово в алфавите $\{1, \dots, p\}$. Ему соответствует слово $M(w) = (M_{i_1}, \dots, M_{i_t})$ в алфавите $\widehat{M}$. *Значением* слова $M(w)$ назовём элемент моноида $\mathbb{M}_n^{0,1,2}$, равный произведению матриц $M_{i_1} \dots M_{i_t}$. Множество значений всех слов полугруппы $\langle\widehat{M}\rangle$ обозначим через $S(\langle\widehat{M}\rangle)$.

Множество $\widehat{M}$ назовём *α-примитивным*, $\alpha \in Z(2)$, если $S(\langle\widehat{M}\rangle) \cap \mathbb{M}_n^{\langle\alpha\rangle} \neq \varnothing$, при этом наименьшая длина слова в алфавите $\widehat{M}$, имеющего значение в $\mathbb{M}_n^{\langle\alpha\rangle}$, называется *$\alpha$-экспонентом* множества $\widehat{M}$ и обозначается через $\langle\alpha\rangle\text{-exp}\,\widehat{M}$. В частности, матрица M *α-примитивна,* если $M^t \in \mathbb{M}_n^{\langle\alpha\rangle}$ при некотором $t \in \mathbb{N}$; наименьшее такое t равно $\langle\alpha\rangle\text{-exp}\,M$. Если множество $\widehat{M}$ не α-примитивное, то положим $\langle\alpha\rangle\text{-exp}\,\widehat{M} = \infty$.

Для любой $\langle 2\rangle$-примитивной матрицы M в силу определений верно

$$\langle 2\rangle\text{-exp}\,M \geqslant \langle 2sc\rangle\text{-exp}\,M = \max\{\langle 2c\rangle\text{-exp}\,M, \langle 2s\rangle\text{-exp}\,M\}, \tag{2}$$

$$\langle 2\rangle\text{-exp}\,M \geqslant \exp M. \tag{3}$$

Утверждение 2 (свойства изотонности)**.** *Пусть $A, B \in \mathbb{M}_n^{0,1,2}$, $A \leqslant B$ и $\alpha \in Z(2)$. Тогда*

(а) *если $A \in \mathbb{M}_n^{\langle\alpha\rangle}$, то $B \in \mathbb{M}_n^{\langle\alpha\rangle}$;*

(б) *если A α-примитивна, то B также α-примитивна и*

$$\langle\alpha\rangle\text{-exp}\,A \geqslant \langle\alpha\rangle\text{-exp}\,B.$$

Доказательство. (а) Пусть $\alpha = 2c$. Из того, что $A \leqslant B$ и $A \in \mathbb{M}_n^{\langle 2c\rangle}$, следует, что A и, следовательно, B имеют элемент 2 в каждом столбце. Значит, $B \in \mathbb{M}_n^{\langle 2c\rangle}$. Рассуждения верны при всех $\alpha \in Z(2)$.

(б) Из неравенства $A \leqslant B$ в силу (1) следует $A^t \leqslant B^t$, $t \in \mathbb{N}$. При $t = \langle\alpha\rangle\text{-exp}\,A$ матрица A^t принадлежит $\mathbb{M}_n^{\langle\alpha\rangle}$, тогда $B^t \in \mathbb{M}_n^{\langle\alpha\rangle}$ по утверждению 2(а). Отсюда B α-примитивна и $\langle\alpha\rangle\text{-exp}\,B \leqslant t$, $\alpha \in Z(2)$. Утверждение 2 доказано.

Пример 1. Вычисление $\exp M$ и $\langle\alpha\rangle\text{-exp}\,M$ для троичной матрицы

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \end{pmatrix}, \quad \alpha \in Z(2).$$

Вычисляем

$$M^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix},$$

$$M^4 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \\ 2 & 2 & 0 & 1 \end{pmatrix}, \quad \ldots, \quad M^9 = \begin{pmatrix} 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 \\ 1 & 2 & 2 & 2 \end{pmatrix},$$

$$M^{10} = \begin{pmatrix} 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 \\ 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad \ldots, \quad M^{12} = \begin{pmatrix} 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad M^{13} = (2)_n.$$

Отсюда

$$\langle 2c\rangle\text{-exp}\, M = \langle 2s\rangle\text{-exp}\, M = \langle 2sc\rangle\text{-exp}\, M = 4,$$
$$\exp M = 10, \quad \langle 2\rangle\text{-exp}\, M = 13.$$

Сложение троичных матриц $A = (a_{i,j})$ и $B = (b_{i,j})$ порядка n определим формулой $A + B = C = (c_{i,j})$, где $c_{i,j} = \max\{a_{i,j}, b_{i,j}\}$, $0 \leqslant i, j < n$.

Утверждение 3. *Если $\widehat{M}$ — α-примитивное множество, $\alpha \in Z(2)$, то матрица $M = M_1 + \cdots + M_p$ также α-примитивна и верны неравенства*

$$\langle\alpha\rangle\text{-exp}\, M \leqslant \langle\alpha\rangle\text{-exp}\, \widehat{M} \leqslant \min\{\langle\alpha\rangle\text{-exp}\, M_1, \ldots, \langle\alpha\rangle\text{-exp}\, M_p\}.$$

Доказательство. Пусть $\langle\alpha\rangle\text{-exp}\, \widehat{M} = t$. Тогда в алфавите $\widehat{M}$ есть слово $M(w) = (M_{i_1}, \ldots, M_{i_t})$, имеющее значение в множестве $\mathbb{M}_n^{\langle\alpha\rangle}$. Так как $M_{i_j} \leqslant M$, $j = 1, \ldots, t$, в силу (1) $S(M(w)) \leqslant M^t$. Тем самым нижняя оценка $\langle\alpha\rangle\text{-exp}\, \widehat{M}$ верна по утверждению 2(б).

Верхняя оценка следует из определения $\langle\alpha\rangle\text{-exp}\, \widehat{M}$. Утверждение 3 доказано.

3. Свойства мультипликативных моноидов помеченных орграфов

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. Матрицу M над полугруппой G назовём *матрицей меток* орграфа Γ и обозначим через $M(\Gamma)$, если следует подчеркнуть её связь с орграфом.

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

Неособенный орграф необходимо содержит контуры. Орграф Γ называется *примитивным,* если Γ^t — полный орграф с петлями при некотором $t \in \mathbb{N}$, наименьшее такое t называется *экспонентом* орграфа Γ и обозначается через $\exp\Gamma$.

Далее $\Gamma \in \mathbb{\Gamma}_n$. При биекции $\mathbb{\Gamma}_n \leftrightarrow \mathbb{M}_n^{0,1,2}$ дуге $(i, m_{i,j}, j)$ орграфа Γ соответствует элемент $m_{i,j}$ в i-й строке и j-м столбце матрицы M (неособенной троичной матрице взаимно однозначно соответствует неособенный помеченный орграф). Умножение орграфов есть умножение бинарных отношений, и правило (1) согласовано с указанной биекцией. Таким образом, $\mathbb{\Gamma}_n$ — мультипликативный моноид всех неособенных помеченных орграфов: если $\Gamma, \Gamma' \in \mathbb{\Gamma}_n$, в Γ имеется дуга $(i, m_{i,s}, s)$ и в Γ' имеется дуга $(s, \mu_{s,j}, j)$, то в орграфе $\Gamma\Gamma'$ имеется дуга $(i, m_{i,s}\mu_{s,j}, j)$, где умножение меток выполнено в полугруппе G.

В соответствии с данными определениями путь $(v_0, \ldots, v_t)$ длины t из вершины v_0 в вершину v_t помечен словом $(m_1, \ldots, m_t)$, где m_s — метка дуги (v_{s-1}, v_s), $s = 1, \ldots, t$. Произведение $m^{(t)} = m_1 \ldots m_t$, вычисляемое в полугруппе G, назовём значением метки $m_1 \ldots m_t$ пути $(v_0, \ldots, v_t)$. Значение метки любого не существующего в Γ пути равно 0. Значение метки любого существующего пути в Γ равно наибольшей метке дуг пути, следовательно, равно 1 или 2. Путь (контур) в Γ из вершины i в вершину j со значением метки 2 назовём 2-*путём* (2-*контуром*) и обозначим через $w^{[2]}(i, j)$.

Теорема 1. *Пусть* $\Gamma \in \mathbb{\Gamma}_n$, $M(\Gamma) = M = (m_{i,j})$. *Тогда* $M^t = \left(m_{i,j}^{(t)}\right)$, *где* $m_{i,j}^{(t)}$ — *наибольшее значение меток всех путей в* Γ *из* i *в* j *длины* t, $t \in \mathbb{N}$.

Доказательство. Индукция по t. При $t = 1$ утверждение тривиально и $m_{i,j}^{(1)} = m_{i,j}$ для всех пар (i, j).

Пусть утверждение верно при любом $k < t$, где $t \geqslant 2$. Покажем, что оно верно при $k = t$.

Обозначим через $E(j)$ множество всех вершин, из которых исходят дуги в вершину j, $j = 1, \ldots, n$. Без ограничения общности положим $E(j) = \{1, \ldots, r\}$ для фиксированного j. Тогда $m_{i,j} = 0$ при $i > r$ и из равенства $M^t = M^{t-1}M$ в соответствии с (1) следует, что

$$m_{i,j}^{(t)} = \max\left\{m_{i,1}^{(t-1)} m_{1,j}, \ldots, m_{i,r}^{(t-1)} m_{r,j}\right\}.$$

По предположению индукции $m_{i,s}^{(t-1)}$ равно наибольшему значению меток всех путей длины $t-1$ из i в s. Значит, произведение $m_{i,s}^{(t-1)} m_{s,j}$ равно наибольшему значению меток всех путей из i в j длины t при условии, что

вершине j предшествует вершина s, $s = 1, \dots, r$. Тогда $m_{i,j}^{(t)}$ — наибольшее значение меток всех путей длины t из i в j. Теорема 1 доказана.

Следствие 2. *При $t \geqslant 1$ в орграфе Γ^t дуга (i, j) имеет метку*

(а) 0 *тогда и только тогда, когда в орграфе* Γ *вершина j не достижима из вершины i за t шагов;*

(б) 1 *тогда и только тогда, когда в орграфе* Γ *значение метки любого пути длины t из i в j равно* 1;

(в) 2 *тогда и только тогда, когда в орграфе* Γ *существует* 2*-путь длины t из i в j.*

Помеченный орграф Γ назовём *α-графом,* $\alpha \in Z(2)$, если

а) при $\alpha = 2c$ в каждую вершину орграфа Γ заходит дуга с меткой 2;

б) при $\alpha = 2s$ из каждой вершины орграфа Γ исходит дуга с меткой 2;

в) при $\alpha = 2sc$ орграф Γ является $2c$- и $2s$-графом;

г) при $\alpha = 2$ орграф Γ полный и каждая его дуга имеет метку 2.

Обозначим через $\mathbb{\Gamma}_n^{\langle\alpha\rangle}$ множество всех α-графов, $\alpha \in Z(2)$. В силу определения

$$\mathbb{\Gamma}_n^{\langle 2\rangle} \subseteq \mathbb{\Gamma}_n^{\langle 2sc\rangle} = \mathbb{\Gamma}_n^{\langle 2c\rangle} \cap \mathbb{\Gamma}_n^{\langle 2s\rangle}.$$

Далее $\widehat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$ — множество неособенных помеченных орграфов, $p \in \mathbb{N}$. Слову $w \in \mathbb{N}_p^*$ соответствует слово $\Gamma(w) = (\Gamma_{i_1}, \dots, \Gamma_{i_t})$ в алфавите $\widehat{\Gamma}$. *Значением* слова $\Gamma(w)$ назовём элемент моноида $\mathbb{\Gamma}_n$, равный произведению орграфов $\Gamma_{i_1} \dots \Gamma_{i_t}$. Множество значений всех слов полугруппы $\langle\widehat{\Gamma}\rangle$ обозначим через $S(\langle\widehat{\Gamma}\rangle)$.

Множество орграфов $\widehat{\Gamma}$ называется *α-примитивным,* $\alpha \in Z(2)$, если $S(\langle\widehat{\Gamma}\rangle) \cap \mathbb{\Gamma}_n^{\langle\alpha\rangle} \neq \varnothing$, а наименьшая длина слова в алфавите $\widehat{\Gamma}$, имеющего значение в $\mathbb{\Gamma}_n^{\langle\alpha\rangle}$, называется *$\alpha$-экспонентом* множества $\widehat{\Gamma}$ и обозначается через $\langle\alpha\rangle\text{-}\exp\widehat{\Gamma}$ (кратко γ_α). В частности, помеченный орграф Γ *α-примитивный,* если $\Gamma^t \in \mathbb{\Gamma}_n^{\langle\alpha\rangle}$ при некотором $t \in \mathbb{N}$, а наименьшее такое t равно $\langle\alpha\rangle\text{-}\exp\Gamma$. Если множество $\widehat{\Gamma}$ не $\langle\alpha\rangle$-примитивное, то положим $\langle\alpha\rangle\text{-}\exp\widehat{\Gamma} = \infty$.

В силу биекции $\mathbb{\Gamma}_n \leftrightarrow \mathbb{M}_n^{0,1,2}$ и утверждения 1 $\mathbb{\Gamma}_n^{\langle\alpha\rangle}$ есть двусторонний идеал моноида $\mathbb{\Gamma}_n$, $\alpha \in Z(2)$, при этом Γ α-примитивен тогда и только тогда, когда матрица $M(\Gamma)$ α-примитивна, и $\langle\alpha\rangle\text{-}\exp\Gamma = \langle\alpha\rangle\text{-}\exp M(\Gamma)$.

4. Критерии α-примитивности и оценки α-экспонентов помеченных орграфов из различных классов

В орграфе Γ обозначим через V_C множество циклических вершин (вершина циклическая, если через неё проходит некоторый контур); $C(\varepsilon)$ — контур C, пройденный из вершины ε; $w^{[2]}(i, j)$ — 2-путь из i в j;

$w^{[2]}(i, V_C)$ — кратчайший 2-путь из i в некоторую циклическую вершину; $w^{[2]}(V_C, j)$ — кратчайший 2-путь из некоторой циклической вершины в j; $w^{[2]}(i, *)$ — кратчайший 2-путь из i в некоторую вершину; $w^{[2]}(*, j)$ — кратчайший 2-путь из некоторой вершины в j, $0 \leqslant i, j < n$. Положим также

$$d = \max\{\operatorname{len} w^{[2]}(0, *), \ldots, \operatorname{len} w^{[2]}(n-1, *)\},$$
$$\delta = \max\{\operatorname{len} w^{[2]}(*, 0), \ldots, \operatorname{len} w^{[2]}(*, n-1)\}.$$

Теорема 2 (критерий α-примитивности орграфа)**.** *Помеченный орграф $\Gamma \in \mathbb{\Gamma}_n$ α-примитивен тогда и только тогда, когда*

• *в случае $\alpha = 2c$ имеется 2-путь из некоторой циклической вершины в вершину j, $0 \leqslant j < n$, при этом*

$$\gamma_{2c} = \max_{0 \leqslant j < n} \operatorname{len} w^{[2]}(V_C, j) \leqslant n;$$

в частности, если Γ сильно связный, то $\gamma_{2c} = \delta$;

• *в случае $\alpha = 2s$ имеется 2-путь из вершины i в некоторую циклическую вершину, $0 \leqslant i < n$, при этом*

$$\gamma_{2s} = \max_{0 \leqslant i < n} \operatorname{len} w^{[2]}(i, V_C) \leqslant n;$$

в частности, если Γ сильно связный, то $\gamma_{2s} = d$;

• *в случае $\alpha = 2sc$ орграф Γ $2c$-примитивен и $2s$-примитивен, при этом*

$$\gamma_{2sc} = \max\{\gamma_{2c}, \gamma_{2s}\} \leqslant n;$$

• *в случае $\alpha = 2$ орграф Γ примитивен и имеет дугу с меткой 2, при этом*

$$\gamma_2 \leqslant \min\{d, \delta\} + \exp\Gamma \leqslant n^2 - n + 2.$$

Доказательство. Если помеченный орграф Γ α-примитивен, по определению Γ^t — α-граф при $t = \langle\alpha\rangle\text{-}\exp\Gamma$. Так как $\mathbb{\Gamma}_n^{\langle\alpha\rangle}$ есть идеал моноида $\mathbb{\Gamma}_n$, то α-графом является орграф Γ^τ при любом $\tau \geqslant t$, $\alpha \in Z(2)$.

Пусть $\alpha = 2c$. По условию $2c$-примитивности существует $t \in \mathbb{N}$ такое, что при любом $\tau \geqslant t$ в вершину j орграфа Γ^τ заходит дуга с меткой 2, $0 \leqslant j < n$. Значит, в орграфе Γ при любом $\tau \geqslant t$ имеется 2-путь длины τ в вершину j, и при $\tau \geqslant \max\{t, n\}$ этот 2-путь обходит целиком некоторый контур. Следовательно, в Γ имеется 2-путь длины $\tau \geqslant \max\{t, n\}$ из некоторой циклической вершины в j, $0 \leqslant j < n$.

В обратную сторону. Если имеется 2-путь длины $t(j)$ из некоторой циклической вершины в j, то при любом $\tau \geqslant t(j)$ имеется 2-путь длины τ из некоторой вершины того же контура в j. Следовательно, в вершину j орграфа Γ^τ заходит дуга с меткой 2 при любом $\tau \geqslant \max\{t(0), \ldots, t(n-1)\}$, $0 \leqslant j < n$. Значит, орграф Γ будет $2c$-примитивным.

Оценим величину γ_{2c}. В силу доказанного критерия вершина j достижима из вершины некоторого контура посредством некоторого 2-пути. Если вершина j принадлежит простому 2-контуру C, то $w^{[2]}(V_C, j)$ есть часть контура C и $\operatorname{len} w^{[2]}(V_C, j) \leqslant \operatorname{len} C \leqslant n$.

Пусть j не принадлежит простому 2-контуру C, дуга (μ, ν) контура C имеет метку 2 и ε — вершина контура C, ближайшая к вершине j, $\varepsilon \neq j$. Тогда вершина j достижима с помощью 2-пути $w^{[2]}(\mu, j)$, являющегося конкатенацией путей $w(\mu, \varepsilon) \bullet w(\varepsilon, j)$, где $w(\mu, \varepsilon)$ — часть контура C. Заметим, что $w(\varepsilon, j)$ можно построить как кратчайший простой путь, не проходящий через вершины пути $w(\mu, \varepsilon)$ за исключением, быть может, вершины μ (иначе путь $w(\varepsilon, j)$ не кратчайший). Тогда

$$\operatorname{len} w^{[2]}(\mu, j) = w(\mu, \varepsilon) + w(\varepsilon, j) \leqslant n.$$

Отсюда

$$\gamma_{2c} = \max_{0 \leqslant j < n} \operatorname{len} w^{[2]}(V_C, j) \leqslant n.$$

Если орграф Γ сильно связный, то все его вершины циклические, поэтому пути $w^{[2]}(V_C, j)$ и $w^{[2]}(*, j)$ совпадают и $\gamma_{2c} = \delta$.

При $\alpha = 2s$ доказательство аналогично.

При $\alpha = 2sc$ теорема верна в силу определения $2sc$-примитивности.

При $\alpha = 2$ из определения следует [1)], что 2-примитивный орграф Γ сильно связный и существует $t \in \mathbb{N}$ такое, что при любом $\tau \geqslant t$ в вершину j орграфа Γ^τ заходит дуга с меткой 2, $0 \leqslant j < n$. Значит, Γ примитивен и имеет дугу с меткой 2.

В обратную сторону. Пусть Γ примитивный, имеет дугу с меткой 2 и $t = \exp \Gamma$. В орграфе Γ все вершины циклические, отсюда

$$w^{[2]}(i, V_C) = w^{[2]}(i, *), \quad w^{[2]}(V_C, j) = w^{[2]}(*, j).$$

Обозначим через $(\xi(i), \eta(i))$ дугу с меткой 2 такую, что вершина $\xi(i)$ ближайшая к i ($\xi(i) = i$ не исключено). Определим 2-путь $w(i, j)$:

$$w(i, j) = w(i, \xi(i)) \bullet (\xi(i), \eta(i)) \bullet w(\eta(i), j),$$

где путь $w(i, \xi(i))$ кратчайший, а путь $w(\eta(i), j)$ любой не меньшей t длины имеется, так как $t = \exp \Gamma$. По построению $\operatorname{len} w(i, j) \leqslant d + t$ для всех i, j. Следовательно, $\gamma_2 \leqslant d + \exp \Gamma$.

Обозначим через $(\xi(j), \eta(j))$ дугу с меткой 2 такую, что вершина $\eta(j)$ ближайшая к j. Рассуждая аналогично о конкатенации путей $w(i, \xi(j)) \bullet (\xi(j), \eta(j)) \bullet w(\eta(j), j)$, получаем $\operatorname{len} w(i, j) \leqslant \delta + t$ для всех i, j. При совмещении обеих оценок имеем $\gamma_2 \leqslant \min\{d, \delta\} + \exp \Gamma$. Так как $\min\{d, \delta\} < n$,

[1)] Доказательства, относящиеся к критерию и оценкам показателя $\langle 2 \rangle$-примитивности орграфов, даны в [18], здесь приведены некоторые из них для удобства русскоязычного читателя.

с учётом оценки Виландта для $\exp\Gamma$ выводим $\gamma_2 \leqslant n^2 - n + 2$. Теорема 2 доказана.

Замечание 1. Сильная связность и связность орграфа Γ не являются необходимыми условиями его α-примитивности при $\alpha \in \{2c, 2s, 2sc\}$.

Для некоторых орграфов доказаны следующие оценки $\langle 2\rangle$-экспонентов [18].

Теорема 3. *Если $\langle 2\rangle$-примитивный орграф Γ имеет контур длины l, то*

$$\gamma_2 \leqslant 2n + l(n-2).$$

В частности, если C есть 2-контур, то $\langle 2\rangle$-$\exp\Gamma \leqslant n + l(n-1)$.

Теорема 4. *Если $\langle 2\rangle$-примитивный орграф Γ имеет $p > 0$ петель, то*

$$\gamma_2 \leqslant 3n - p - 1.$$

В частности, если m петель имеют метку 2, где $0 < m \leqslant p$, то $\gamma_2 \leqslant 2n - m$.

Универсальная оценка экспонента n-вершинных орграфов [6], равная $n^2 - 2n + 2$, достигается на множестве орграфов, являющихся объединением гамильтонова контура и контура длины $n-1$ (и только на них), $n \geqslant 3$. Такие орграфы называют графами Виландта.

Пусть Γ — орграф Виландта с помеченными дугами и указанные контуры суть $C_0 = (0, 1, \ldots, n-1)$ и $C_1 = (1, 2, \ldots, n-1)$.

Теорема 5 (универсальная оценка)**.** *Если помеченный n-вершинный орграф Γ имеет дугу с меткой 2, то*

$$\gamma_2 = \begin{cases} n^2 - n + 1, & \text{если метка 2 только у одной из дуг } (0,1),\\ & (n-1,0),\ (n-1,1);\\ n^2 - n, & \text{если метка 2 только у дуг } (0,1) \text{ и } (n-1,0);\\ n^2 - 2n + 2 & \text{в остальных случаях.} \end{cases}$$

Следствие 3. *Пусть n-вершинный орграф Γ имеет дуги с меткой 2, $n \geqslant 3$. Тогда если Γ — помеченный орграф Виландта, то*

$$n^2 - 2n + 2 \leqslant \gamma_2 \leqslant n^2 - n + 1;$$

в противном случае $\gamma_2 \leqslant n^2 - 2n + 4$.

5. Признаки в полугруппах преобразований векторных пространств

МГП применяется для оценки множеств существенных и нелинейных переменных координатных функций композиций преобразований пространства P^n, где P — поле, $n \in \mathbb{N}$. Преобразование $g^{(t)}$ пространства P^n зададим системой координатных функций $\{g_0^{(t)}(x), \ldots, g_{n-1}^{(t)}(x)\}$, где $x = (x_0, \ldots, x_{n-1})$, $t \geqslant 1$.

5.1. Существенные переменные. Обозначим через $\Gamma(g)$ *перемешивающий орграф* преобразования g с множеством вершин $\{0,\dots,n-1\}$, т. е. (i,j) является дугой тогда и только тогда, когда x_i — существенная переменная функции $g_j(x)$, $0 \leqslant i,j < n$. Двоичная матрица $M(g)$ смежности вершин графа $\Gamma(g)$ называется *перемешивающей матрицей* преобразования g.

Преобразование g называется *вполне перемешивающим,* если $M(g) = (1)_n$. Множество вполне перемешивающих преобразований назовём *признаком полного перемешивания* (в общем случае он не наследственный и не идеальный), обозначим его $\Pi_n^{\langle 1\rangle}$.

Обозначим через $\widehat{G} = \{g^{(1)},\dots,g^{(p)}\}$ множество преобразований пространства P^n, $p \in \mathbb{N}$, а через $\widehat{M}(\widehat{G})$ — множество перемешивающих матриц всех преобразований из $\widehat{G}$. Множество $\widehat{G}$ назовём *перфективным,* если $\langle\widehat{G}\rangle \cap \Pi_n^{\langle 1\rangle} \neq \varnothing$. Наименьшая длина слова в алфавите $\widehat{G}$, принадлежащего $\Pi_n^{\langle 1\rangle}$, называется *показателем перфективности* множества $\widehat{G}$ и обозначается через $\operatorname{prf}\widehat{G}$. В частности, наименьшее $t \in \mathbb{N}$, при котором $g^t \in \Pi_n^{\langle 1\rangle}$, называется *показателем перфективности* преобразования g и обозначается через $\operatorname{prf} g$.

Для оценки множеств существенных переменных координатных функций любого произведения $g^{(1)}\dots g^{(t)}$ из полугруппы $\langle\widehat{G}\rangle$ применяется МГП, в соответствии с которым выполнено неравенство [3, с. 183]

$$M(g^{(1)}\dots g^{(t)}) \leqslant M(g^{(1)})\dots M(g^{(t)}), \quad t \geqslant 1. \tag{4}$$

Утверждение 4. *Если множество $\widehat{G}$ перфективное, то*

$$\operatorname{prf}\widehat{G} \geqslant \exp\widehat{M}(\widehat{G}).$$

Доказательство. Пусть $\operatorname{prf}\widehat{G} = t$. Тогда существует слово $(g^{(i_1)},\dots,g^{(i_t)})$ длины t в алфавите $\widehat{G}$ такое, что соответствующее произведение $g^{(i_1)}\dots g^{(i_t)}$ принадлежит $\Pi_n^{\langle 1\rangle}$. Значит, $M(g^{(i_1)}\dots g^{(i_t)}) = (1)_n$. Отсюда $M(g^{(i_1)})\dots M(g^{(i_t)}) = (1)_n$ в силу (4). Тем самым в алфавите $\widehat{M}(\widehat{G})$ имеется слово длины t, соответствующее матрице $(1)_n$. Следовательно, $\exp\widehat{M}(\widehat{G}) \leqslant t$. Утверждение 4 доказано.

Следствие 4. *Если преобразование g перфективное, то*

$$\operatorname{prf} g \geqslant \exp M(g).$$

5.2. Нелинейные переменные. Определим матрицу характеристик нелинейности $M_\Theta(g)$ порядка n (кратко — матрицу нелинейности) для преобразования g пространства P^n. Определим *матрицу нелинейности* $\mathrm{M}_\Theta(g) = (m_{i,j})$ как троичную матрицу, где элемент $m_{i,j}$ равен 0, 1 или 2

тогда и только тогда, когда $g_j(x)$ зависит от x_i фиктивно, линейно или нелинейно соответственно, $0 \leqslant i, j < n$. Помеченный орграф, в который матрица $M_\Theta(g)$ отображается биекцией $\mathbb{\Gamma}_n \leftrightarrow \mathbb{M}_n$, назовём *орграфом нелинейности* преобразования g и обозначим через $\Gamma_\Theta(g)$.

Преобразование g называется *α-нелинейным,* $\alpha \in Z(2)$ (более детально, *нелинейным по выходу* при $\alpha = 2c$, *нелинейным по входу* при $\alpha = 2s$, *строго нелинейным* при $\alpha = 2sc$, *вполне нелинейным* при $\alpha = 2$), если $M_\Theta(g)$ есть α-матрица ($\Gamma_\Theta(g)$ — α-граф). Множество α-нелинейных преобразований обозначим через $\Pi_n^{\langle\alpha\rangle}$, $\alpha \in Z(2)$. Признак α-нелинейности в полугруппе $\mathbb{\Pi}(P^n)$ в общем случае не наследственный и не идеальный.

Заметим, что преобразование, удовлетворяющее строгому лавинному критерию, вполне нелинейно [3, с. 182]. Класс вполне нелинейных булевых функций содержит не только все максимально нелинейные функции, но и некоторые равновероятные функции, что представляет его перспективным для использования в криптографических приложениях.

Характеристики нелинейности координатных функций произведения $g^{(1)} \dots g^{(t)}$ любых преобразований пространства P^n оцениваются с помощью неравенства [18]

$$M_\Theta(g^{(1)} \dots g^{(t)}) \leqslant M_\Theta(g^{(1)}) \dots M_\Theta(g^{(t)}), \quad t \geqslant 1. \tag{5}$$

В частности, $M_\Theta(g^t) \leqslant (M_\Theta(g))^t$ для любого преобразования g пространства P^n.

Множество преобразований $\widehat{G}$ назовём *α-перфективным,* если $\langle\widehat{G}\rangle \cap \Pi_n^{\langle\alpha\rangle} \neq \varnothing$. Наименьшая длина слова в алфавите $\widehat{G}$, принадлежащего $\Pi_n^{\langle\alpha\rangle}$, называется *$\alpha$-экспонентом* множества $\widehat{G}$ и обозначается через $\langle\alpha\rangle\text{-}\exp\widehat{G}$, $\alpha \in Z(2)$. В частности, преобразование g является *α-перфективным,* если циклическая полугруппа $\langle g\rangle$ содержит α-нелинейное преобразование, а наименьшее $t \in \mathbb{N}$, при котором $g^t \in \Pi_n^{\langle\alpha\rangle}$, называется α-экспонентом преобразования g и обозначается через $\langle\alpha\rangle\text{-}\exp g$.

Обозначим через $\widehat{M}_\Theta(\widehat{G})$ множество матриц нелинейности преобразований из $\widehat{G}$.

Утверждение 5. *Если множество $\widehat{G}$ α-перфективно, $\alpha \in Z(2)$, то*

$$\langle\alpha\rangle \exp\widehat{G} \geqslant \langle\alpha\rangle\text{-}\exp\widehat{M}_\Theta(\widehat{G}).$$

Доказательство. Пусть $\langle\alpha\rangle\text{-}\exp\widehat{G} = t$. Тогда в алфавите $\widehat{G}$ имеется слово $(g^{(i_1)}, \dots, g^{(i_t)})$ длины t такое, что соответствующее произведение $g^{(i_1)} \dots g^{(i_t)} \in \Pi_n^{\langle\alpha\rangle}$. Значит, $M_\Theta(g^{(i_1)} \dots g^{(i_t)}) \in \mathbb{M}_n^{\langle\alpha\rangle}$. Тогда в соответствии с (5) и свойством изотонности выполнено $M_\Theta(g^{(i_1)}) \dots M_\Theta(g^{(i_t)}) \in \mathbb{M}_n^{\langle\alpha\rangle}$. Тем самым в алфавите $\widehat{M}_\Theta(\widehat{G})$ есть слово длины t, принадлежащее $\mathbb{M}_n^{\langle\alpha\rangle}$. Следовательно, $\langle\alpha\rangle\text{-}\exp\widehat{M}_\Theta(\widehat{G}) \leqslant t$. Утверждение 5 доказано.

Следствие 5. *Если преобразование g α-перфективно, $\alpha \in Z(2)$, то*

$$\langle\alpha\rangle\text{-}\exp g \geqslant \langle\alpha\rangle\text{-}\exp M_\Theta(g).$$

Пример 2. Вычисление $\exp M$ и $\langle\alpha\rangle$-$\exp M$ для матрицы нелинейности $M_\Theta(g)$ регистровой подстановки, заданной множеством координатных функций $\{x_1, x_2, x_3, x_0 \oplus x_2x_3\}$, $\alpha \in Z(2)$. Найдём ряд степеней матрицы нелинейности

$$M = M_\Theta(g) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix}:$$

$$M^2 = \begin{pmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 2 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 \end{pmatrix},$$

$$M^4 = \begin{pmatrix} 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad M^5 = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad M^6 = (2)_n.$$

Отсюда

$$\langle 2s\rangle\text{-}\exp M = 3, \quad \langle 2c\rangle\text{-}\exp M = \langle 2sc\rangle\text{-}\exp M = 4,$$
$$\exp M = 5, \quad \langle 2\rangle\text{-}\exp M = 6.$$

6. Оценка числа раундов при синтезе итеративного блочного шифра

Пусть $f^{(s)}$ — подстановка s-го раунда t-раундового блочного шифра. Если матрицы $M_\Theta(f^{(s)})$ равны M, т. е. одинаковы при $s = 1, \ldots, t$ (это выполнено, например, при «подмешивании» раундового ключа с помощью операции XOR), то $\exp M$ и $\langle 2\rangle$-$\exp M$ следует рассматривать как нижние оценки числа раундов, необходимого для полного перемешивания и полной нелинейности соответственно. Точность оценки с помощью $\langle 2\rangle$-$\exp M$ в любом случае не ниже, так как $\exp M \leqslant \langle 2\rangle$-$\exp M$.

Для раундовых подстановок g и h блочных шифров DES и «Магма» соответственно выполнены вычислительные эксперименты (ВКР Сапегиной М. Д., 2019 г., НИЯУ МИФИ). С помощью техники МГП определены экспоненты и $\langle 2\rangle$-экспоненты троичных матриц нелинейности $M(g)$ и $M(h)$ раундовых подстановок. Получены следующие результаты: $\exp M(g) = \langle 2\rangle$-$\exp M(g) = 5$, $\exp M(h) = \langle 2\rangle$-$\exp M(h) = 6$.

Выводы

1. В настоящей работе матрично-графовый подход получил дальнейшее развитие для оценки ряда характеристик нелинейности композиций преобразований векторных пространств.

2. Для различных классов помеченных орграфов получены оценки показателей признаков α-примитивности, $\alpha \in \{2c, 2s, 2sc, 2\}$, связанных с характеристиками нелинейности преобразований векторных пространств, в том числе универсальная оценка $\langle 2 \rangle$-экспонента n-вершинных орграфов, обобщающая универсальную оценку экспонента Виландта.

ЛИТЕРАТУРА

1. **Сачков В. Н., Тараканов В. Е.** Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
2. **Фомичёв В. М.** Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. **Фомичёв В. М., Мельников Д. А.** Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: ЮРАЙТ, 2016. 209 с.
4. **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.
5. **Frobenius G.** Über Matrizen aus nicht negativen Elementen // Berl. Ber. 1912. P. 456–477. [German].
6. **Wielandt H.** Unzerlegbare nicht negative Matrizen // Math. Z. 1950. Bd. 52. S. 642–648. [German].
7. **Perkins P.** A theorem on regular graphs // Pac. J. Math. 1961. Vol. 2. P. 1529–1533.
8. **Dulmage A. L., Mendelsohn N. S.** The exponent of a primitive matrix // Can. Math. Bull. 1962. Vol. 5, No. 3. P. 241–244.
9. **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.
10. **Brualdi R. A., Liu B.** Generalized exponents of primitive directed graphs // J. Graph Theory. 1990. Vol. 14, No. 4. P. 483–499.
11. **Neufeld S. W.** A diameter bound on the exponent of a primitive directed graph // Linear Algebra Appl. 1996. Vol. 245. P. 27–47.
12. **Liu B.** Generalized exponents of Boolean matrices // Linear Algebra Appl. 2003. Vol. 373. P. 169–182.
13. **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).
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. **Fomichev V. M., Koreneva A. M., Miftakhutdinova A. R., Zadorozhny D. I.** Evaluation of the maximum performance of block encryption algorithms // Мат. вопр. криптогр. 2019. Т. 10, № 2. P. 181–190.
18. **Fomichev V. M., Koreneva A. M.** Encryption performance and security of certain wide block ciphers // J. Comput. Virol. Hack. Tech. 2020. Available at `https://link.springer.com/article/10.1007/s11416-020-00351-1` (accessed June 5, 2020).

Фомичёв Владимир Михайлович

Статья поступила
5 мая 2020 г.
После доработки —
28 мая 2020 г.
Принята к публикации
2 июня 2020 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
October–December 2020. Vol. 27, No. 4. P. 131–151

UDC 519.17 DOI 10.33048/daio.2020.27.686

ESTIMATING NONLINEARITY CHARACTERISTICS FOR ITERATIVE TRANSFORMATIONS OF A VECTOR SPACE

V. M. Fomichev[1, 2, 3]

[1] Financial University under the Government of Russian Federation,
49 Leningradsky 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

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

Abstract. We present theoretical foundations for the matrix-graphic approach (MGA) to the estimation of characteristics of the sets of essential and nonlinear variables of the composition of transformations of an n-dimensional vector space over a field. The ternary nonlinearity matrix corresponds to a transformation, where the ith row and the jth column of the matrix contain 0, 1, or 2 if and only if the jth coordinate function of the transformation depends on the ith variable fictitiously, or linearly, or nonlinearly, $0 \leqslant i, j < n$. MGA is based on the inequality according to which the nonlinearity matrix of the product of transformations is at most (the inequality is elementwise) the product of the nonlinearity matrices of the transformations.

We define the multiplication for ternary matrices. The properties are studied of the multiplicative monoid of all ternary matrices of order n without zero rows and columns and of the monoid $\mathbb{\Gamma}_n$ bijectively corresponding to it of all n-vertex digraphs with edges labeled with 0, 1, and 2, where each vertex has nonzero indegree and outdegree. The iteration depth (number of multipliers) for transformations is estimated with the use of MGA in which the four types of the nonlinearity of transformations can be achieved, where each or some of the coordinate functions of the product of transformations can depend nonlinearly on all or at least some variables.

We present the results of research on the nonlinearity of iterations of round substitution of the block ciphers DES and "Magma." Bibliogr. 18.

English version: Journal of Applied and Industrial Mathematics **14** (4), 610–622 (2020), DOI 10.1134/S199047892004002X.

Keywords: nonlinearity matrix (digraph) of a transformation, $\langle\alpha\rangle$-primitive matrix (digraph), $\langle\alpha\rangle$-exponent of a matrix (of a digraph), perfective transformation.

REFERENCES

1. **V. N. Sachkov** and **V. E. Tarakanov,** *Combinatorics of Nonnegative Matrices* (TVP, Moscow, 2000 [Russian]; AMS, Providence, 2002).
2. **V. M. Fomichev,** *Methods of Discrete Mathematics in Cryptology* (Dialog-MIFI, Moscow, 2010) [Russian].
3. **V. M. Fomichev** and **D. A. Melnikov,** *Cryptographic Methods of Information Security* (YURAYT, Moscow, 2016) [Russian].
4. **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)].
5. **G. Frobenius,** Über Matrizen aus nicht negativen Elementen, *Berl. Ber.,* 456–477 (1912) [German].
6. **H. Wielandt,** Unzerlegbare, nicht negative Matrizen, *Math. Z.* **52**, 642–648 (1950) [German].
7. **P. Perkins,** A theorem on regular graphs, *Pac. J. Math.* **2**, 1529–1533 (1961).
8. **A. L. Dulmage** and **N. S. Mendelsohn,** The exponent of a primitive matrix, *Canad. Math. Bull.* **5**, 241–244 (1962).
9. **A. L. Dulmage** and **N. S. Mendelsohn,** Gaps in the exponent set of primitive matrices, *Ill. J. Math.* **8** (4), 642–656 (1964).
10. **R. A. Brualdi** and **B. Liu,** Generalized exponents of primitive directed graphs, *J. Graph Theory* **14** (4), 483–499 (1990).
11. **S. W. Neufeld,** A diameter bound on the exponent of a primitive directed graph, *Linear Algebra Appl.* **245**, 27–47 (1996).
12. **B. Liu,** Generalized exponents of Boolean matrices, *Linear Algebra Appl.* **373**, 169–182 (2003).
13. **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).
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. V. M. Fomichev, A. M. Koreneva, A. R. Miftakhutdinova, and **D. I. Zadorozhny,** Evaluation of the maximum performance of block encryption algorithms, *Mat. Vopr. Kriptogr.* **10** (2), 181–190 (2019).

18. V. M. Fomichev and **A. M. Koreneva,** Encryption performance and security of certain wide block ciphers, *J. Comput. Virol. Hack. Tech.* (2020). Available at `https://link.springer.com/article/10.1007/s11416-020-00351-1` (accessed June 5, 2020).

Vladimir M. Fomichev

Received May 5, 2020
Revised May 28, 2020
Accepted June 2, 2020