ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О неабелевых группах наложения ключа и марковости алгоритмов блочного шифрования // Прикладная дискретная математика. Приложение. 2018. № 11. С. 79–81.
2. *Холл М.* Теория групп. М.: ИЛ, 1962. 468 с.
3. *Погорелов Б. А., Пудовкина М. А.* Вариации ортоморфизмов и псевдоадамаровых преобразований на неабелевой группе // Прикладная дискретная математика. Приложение. 2019. № 12. С. 24–27.

УДК 519.1 DOI 10.17223/2226308X/12/8

ТОЧНАЯ ФОРМУЛА ЭКСПОНЕНТА ПЕРЕМЕШИВАЮЩЕГО ОРГРАФА РЕГИСТРОВОГО ПРЕОБРАЗОВАНИЯ

В. М. Фомичев, Я. Э. Авезова

Для примитивного перемешивающего n-вершинного орграфа $\Gamma(g)$ преобразования g двоичного регистра сдвига длины n, где обратная связь $f(x_0, \ldots, x_{n-1})$ имеет m существенных переменных с множеством номеров $D(g) = \{d_1, \ldots, d_m\}$, $n \geqslant 3$, $2 \leqslant m \leqslant n$, $0 = d_1 < \ldots < d_m$, при $d_m \in \{n-1, n-2\}$ получена точная формула экспонента $\exp \Gamma(g)$ и элементарных локальных экспонентов $\gamma_{u,v}$, $0 \leqslant u, v < n$.

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

Введение

Изучение экспонентов примитивных матриц и графов началось в 1912 г. с работы Фробениуса [1]. Основные понятия и научные достижения отражены в обзоре [2] и ряде других работ. Получение точной аналитической формулы экспонента для того или иного класса матриц и орграфов — сложная комбинаторная задача, в связи с чем большинство работ в этой области посвящены верхним оценкам экспонентов, важным для приложений.

Исследован класс преобразований g пространства n-мерных векторов, реализуемых регистром левого сдвига с нелинейной обратной связью $f(x_0, \ldots, x_{n-1})$, имеющей m существенных переменных, в том числе x_0 (иначе реальная длина регистра меньше n), $n \geqslant 3$, $2 \leqslant m \leqslant n$. Анализ перемешивающих свойств преобразований данного класса имеет прикладное значение для ряда систем защиты информации.

Пусть множество вершин перемешивающего орграфа $\Gamma(g)$, соответствующих номерам входных переменных преобразования g, есть $\{0, \ldots, n-1\}$. Получены точные формулы экспонентов и локальных экспонентов двух частных классов перемешивающих орграфов регистровых преобразований. Первый класс орграфов имеет петлю в вершине $n-1$, второй класс содержит контур $(n-1, n-2)$ длины 2.

1. Структурные свойства перемешивающих орграфов регистровых преобразований

Рассмотрим преобразование g двоичного регистра левого сдвига длины n с нелинейной функцией обратной связи $f(x_0, \ldots, x_{n-1})$. Обозначим $D(g) = \{d_1, \ldots, d_m\}$ множество номеров всех существенных переменных функции f, где $0 = d_1 < \ldots < d_m \leqslant n-1$. Тогда преобразованию g соответствует n-вершинный перемешивающий орграф $\Gamma(g)$, имеющий $n+m-1$ дуг, где n дуг составляют гамильтонов контур $(n-1, \ldots, 0)$ и остальные дуги суть $(d_2, n-1), \ldots, (d_m, n-1)$. Таким образом, связный орграф $\Gamma(g)$ есть объ-

единение простых контуров $C_1, \ldots, C_m$, где $C_t = (n-1, n-2, \ldots, d_t)$, $t = 1, \ldots, m-1$, $C_m = (n-1, n-2, \ldots, d_m)$ при $d_m < n-1$ и C_m есть петля в вершине $n-1$ при $d_m = n-1$. Вершины $d_m, \ldots, n-1$ являются общими для всех простых контуров.

Обозначим: $n - D(g) = \{n - d_i : i = 1, \ldots, m\}$; $\Lambda W(u,v)$ — множество длин всех путей из вершины u в вершину v; $\overline{\Lambda W(u,v)} = \mathbb{N}_0 \backslash \Lambda W(u,v)$, где $\mathbb{N}_0$ — множество целых неотрицательных чисел. Определим элементарные локальные экспоненты орграфа $\Gamma(g)$. По определению локальный экспонент (обозначается $\gamma_{u,v}$) есть наименьшее натуральное число γ, такое, что из u в v есть путь длины t при любом $t \geqslant \gamma$ [3]. В соответствии с определением

$$\gamma_{u,v} = 1 + \max \overline{\Lambda W(u,v)}, \quad 0 \leqslant u, v < n,$$
$$\exp \Gamma(g) = \max_{0 \leqslant u,v < n} \gamma_{u,v}.$$

2. Формулы экспонента и локальных экспонентов при $d_m = n-1$

При $0 \leqslant u, v < n$ и $d_m \in \{n-1, n-2\}$ обозначим:

- $\tau(u)$ — наибольшее число множества $\{1, \ldots, m\}$, такое, что $d_{\tau(u)} \leqslant u$;
- $l_t(u,v) = u - d_t + n - v$, $t = 1, \ldots, \tau(u)$, $u < n-1$;
- $L(u,v) = \{l_1(u,v), \ldots, l_{\tau(u)}(u,v)\}$, $u < n-1$;
- $\Delta(D) = \max\{d_2 - d_1, \ldots, d_m - d_{m-1}\}$.

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

Теорема 1. Если орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, то при $d_m = n-1$

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

Приведём формулу экспонента орграфа $\Gamma(g)$.

Теорема 2. Пусть орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, тогда при $d_m = n-1$

$$\exp \Gamma(g) = n + \Delta(D) - 1.$$

Пример 1. $n = 5$, $D(g) = \{0, 2, 4\}$. Вычисляем $\Delta(D) = 2$, тогда в соответствии с теоремой 2 $\exp \Gamma(g) = 5 + 2 - 1 = 6$. Локальные экспоненты $\gamma_{u,v}$ приведены в таблице.

u	v				
	0	1	2	3	4
0	5	4	3	2	1
1	6	5	4	3	2
2	5	4	3	2	1
3	6	5	4	3	2
4	4	3	2	1	1

3. Формулы экспонента и локальных экспонентов при $d_m = n-2$

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

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

Введём следующие обозначения:

— $I(L(u,v))$ и $J(L(u,v))$ — множества нечётных и чётных чисел множества $L(u,v)$ соответственно;
— $l^0(u,v) = \min J(L(u,v))$, если $J(L(u,v)) \neq \varnothing$;
— $l^1(u,v) = \min I(L(u,v))$, если $I(L(u,v)) \neq \varnothing$;
— $\chi(u,v) = |l^1(u,v) - l^0(u,v)|$;
— d_μ — наибольшее число множества $D(g)$, чётность которого не совпадает с чётностью числа n;
— d_λ — наименьшее нечётное число множества $D(g)$.

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

1) величины $l^0(u,v)$ и $l^1(u,v)$ существуют и $l_{\tau(u)} = \min\{l^0(u,v), l^1(u,v)\}$;
2) величина $\chi(u,v)$ существует и не зависит от v, $\chi(u,v) = \chi(u) = |\mu(u) - \eta(u)|$, где $\mu(u)$ и $\eta(u)$ — наибольшие числа различной чётности множества $\{d_1, \ldots, d_{\tau(u)}\}$.

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

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

Приведём формулу экспонента орграфа $\Gamma(g)$.

Теорема 4. Пусть орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, тогда при $d_m = n-2$

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

где $\Delta(D_{[\lambda]}) = \max\{d_2 - d_1, \ldots, d_\lambda - d_{\lambda-1}\}$, $p_s = d_{s+1} - d_s + \min\{0, \chi(d_s) - n + d_\mu\}$, $s = \lambda, \ldots, m-1$.

Пример 2. $n = 8$, $D(g) = \{0,2,5,6\}$. Найдём $\exp\Gamma(g)$, используя теорему 4. Вычисляем: $d_\mu = d_\lambda = 5$, $d_m = 6$. Тогда при $d_\lambda < d_m$ находим: $\Delta(D_{[\lambda]}) = \max\{2,3\} = 3$, $\chi(d_2) = 1$, $p_3 = 6 - 5 + \min\{0, 1 - 8 + 5\} = -1$. Следовательно, $\exp\Gamma(g) = 16 - 5 - 2 + {} + \max\{3, -1\} = 12$.

ЛИТЕРАТУРА

1. *Frobenius G.* Über Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss. 1912. P. 456–477.
2. *Fomichev V. M., Avezova Ya. E., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Fomichev V. M. and Kyazhin S. N.* Local primitivity of matrices and graphs // J. Appl. Industr. Math. 2017. V. 11. No. 1. P. 26–39.