

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

DOI 10.17223/20710410/23/9

УДК 519.6

УТОЧНЁННЫЕ ОЦЕНКИ ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ
ГРАФОВ БИЕКТИВНЫХ РЕГИСТРОВ СДВИГА
НАД МНОЖЕСТВОМ ДВОИЧНЫХ ВЕКТОРОВ

А. М. Дорохова*, В. М. Фомичев**

*Национальный исследовательский ядерный университет (МИФИ), г. Москва, Россия,

**Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия

E-mail: alisa.koreneva@gmail.com, fomichev@nm.ru

Для перемешивающего графа Γ подстановочного преобразования регистра сдвига длины n над множеством r -мерных двоичных векторов получены новые оценки длин простых путей и циклов, доказаны достаточные условия примитивности графа Γ , понижена полученная ранее верхняя оценка значения экспонента.

Ключевые слова: перемешивающий граф преобразования, диаметр графа, экспонент графа.

Введение

Раундовая подстановка алгоритмов шифрования, использующих конструкцию Фейстеля, построена на основе подстановки регистра сдвига длины 2 над множеством V_r двоичных r -мерных векторов. В [1] в порядке обобщения рассмотрена подстановка φ регистра сдвига длины $n \geq 2$ над V_r , получены в различных условиях верхние оценки диаметра и экспонента перемешивающего графа $\Gamma(\varphi)$ подстановки φ . В настоящей работе получены новые достаточные условия примитивности перемешивающего графа $\Gamma(\varphi)$, улучшена оценка [1, теорема 3] экспонента графа $\Gamma(\varphi)$.

1. Определяющие свойства перемешивающего графа

Используем обозначения работы [1]. Обозначим φ подстановку множества V_{rn} , реализующую регистром сдвига длины $n > 1$ над пространством V_r двоичных r -мерных векторов, где $r > 1$ — длина в битах двоичных слов, записанных в ячейках регистра сдвига. Состояние регистра в текущий момент времени представим двоичной матрицей размера $r \times n$, считая при этом, что $(k+1)$ -й столбец матрицы, обозначаемый $y_{k+1} = (x_{1+rk}, \dots, x_{r+rk})^T$, записан в k -й ячейке регистра сдвига, $k = 0, 1, \dots, n-1$.

Пусть подстановка φ определена равенством

$$\varphi(y_1, \dots, y_n) = (y_2, \dots, y_n, y_1 \oplus \psi(y_2, \dots, y_n)), \quad (1)$$

где $\oplus$ — операция XOR в пространстве V_r и функция $\psi : V_{r(n-1)} \rightarrow V_r$ отлична от константы. Условие $\psi \neq \text{const}$ означает, что подстановка φ не есть циклический сдвиг столбцов двоичной матрицы размера $r \times n$.

Подстановка φ задается системой rn булевых координатных функций

$$\{\varphi_1(x_1, \dots, x_{rn}), \dots, \varphi_{rn}(x_1, \dots, x_{rn})\},$$

где функция $\varphi_{v+rk}(x_1, \dots, x_{rn})$ вычисляет v -й бит x_{v+rk} вектора y_{k+1} , $v = 1, \dots, r$, $k = 0, 1, \dots, n-1$.

Обозначим $S(\varphi_j)$ множество номеров существенных булевых переменных функции $\varphi_j(x_1, \dots, x_{rn})$, $j = 1, \dots, rn$. Отметим свойства множеств $S(\varphi_j)$, вытекающие из (1):

- а) $S(\varphi_{v+rk}(x_1, \dots, x_{rn})) = \{v + r(k+1)\}$, $k = 0, 1, \dots, n-2$, $v = 1, \dots, r$;
- б) $v \in S(\varphi_{u+r(n-1)}(x_1, \dots, x_{rn}))$, где $u, v \in \{1, \dots, r\}$, если и только если $u = v$;
- в) $(S(\varphi_{1+r(n-1)}(x_1, \dots, x_{rn})) \cup \dots \cup S(\varphi_{r+r(n-1)}(x_1, \dots, x_{rn}))) \setminus \{1, \dots, r\} \neq \emptyset$.

Множество $S(\varphi_{u+r(n-1)}(x_1, \dots, x_{rn}))$ зададим таблицей T_u , состоящей из r строк, где v -я строка состоит из номеров существенных переменных функции $\varphi_{u+r(n-1)}(x_1, \dots, x_{rn})$, взятых из множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$; наибольшее из чисел v -й строки таблицы T_u обозначим $m(v, u)$, $v, u = 1, \dots, r$.

Перемешивающий граф $\Gamma(\varphi)$ подстановки φ есть rn -вершинный орграф, в котором есть дуга (i, j) тогда и только тогда, когда $i \in S(\varphi_j)$, $i, j \in \{1, \dots, rn\}$. При рассмотрении диаметра графа расстояние от i до j положим равным длине кратчайшего из циклов, проходящих через вершину i .

Обозначим ϑ функцию отождествления вершин графа $\Gamma(\varphi)$: для любого $v = 1, \dots, r$ положим $\vartheta(v + rk) = v$, $k = 0, 1, \dots, n-1$. Функция ϑ индуцирует функцию Θ , отображающую rn -вершинный орграф $\Gamma(\varphi)$ в r -вершинный орграф $\Gamma(\psi)$, где пара (v, u) образует дугу графа $\Gamma(\psi)$ тогда и только тогда, когда функция $\varphi_{u+r(n-1)}$ зависит существенно хотя бы от одной из переменных множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$, $v, u \in \{1, \dots, r\}$ (записывается $\Theta(\Gamma(\varphi)) = \Gamma(\psi)$).

Отметим свойства орграфов $\Gamma(\varphi)$ и $\Gamma(\psi)$, некоторые из них приведены в [1].

1) В силу свойств а и б множеств $S(\varphi_j)$ орграф $\Gamma(\varphi)$ содержит r независимых циклов $C_1, \dots, C_r$ длины n , где $C_v = (v + r(n-1), v + r(n-2), \dots, v + r, v)$, $v = 1, \dots, r$.

2) Вершина j достижима из вершины i в орграфе $\Gamma(\psi)$, если и только если в орграфе $\Gamma(\varphi)$ любая вершина, принадлежащая циклу C_j , достижима из любой вершины, принадлежащей циклу C_i при $i \neq j$, где $i, j \in \{1, \dots, r\}$.

3) Орграф $\Gamma(\varphi)$ сильносвязный, если и только если орграф $\Gamma(\psi)$ сильносвязный.

4) Простой путь из вершины $v + ri$ в вершину $v + rj$ в цикле C_v (обозначим его $[i, j]_v$) имеет длину $L(i, j)$, где $L(i, j) = i - j$, если $i \geq j$, и $L(i, j) = n - j + i$, если $i < j$.

На рис. 1 изображена часть перемешивающего графа $\Gamma(\varphi)$ подстановки φ , содержащая циклы C_v и C_u , которая при отождествлении вершин преобразуется в дугу (v, u) орграфа $\Gamma(\psi)$. Здесь координатная функция $\varphi_{u+r(n-1)}$ подстановки φ зависит существенно от некоторых переменных множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$.

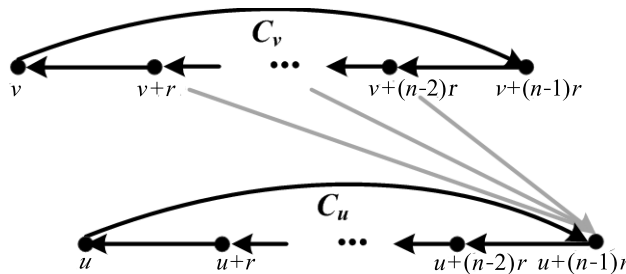


Рис. 1. Часть орграфа $\Gamma(\varphi)$

2. Простые пути и циклы в перемешивающем графе

Функция Θ отображает путь $z = (i_0, \dots, i_t)$ длины t в графе $\Gamma(\varphi)$ в путь $\Theta(z)$ длины $\tau \leq t$ в графе $\Gamma(\psi)$, который получается с помощью замены числом i в последовательности $(\vartheta(i_0), \dots, \vartheta(i_t))$ каждой серии $i, \dots, i$ одинаковых чисел.

Функция Θ определяет отношение эквивалентности $\cong$ на множестве путей (циклов) графа $\Gamma(\varphi)$: если z и z' — пути в графе $\Gamma(\varphi)$, то $z \cong z'$, если и только если $\Theta(z) = \Theta(z')$. Класс эквивалентных путей (циклов) z в графе $\Gamma(\varphi)$, которым при отождествлении вершин соответствует путь (цикл) w в графе $\Gamma(\psi)$, то есть $\Theta(z) = w$, обозначим $[w]$.

Для последовательности из $m > 1$ путей определена операция конкатенации (обозначим символом $\cdot$), если конечная вершина предыдущего пути совпадает с начальной вершиной следующего пути; записывается $z = z_0 \cdot z_1 \cdot \dots \cdot z_m$.

Теорема 1.

а) Если путь z в графе $\Gamma(\varphi)$, начинающийся с вершины $v_0 + r(n-1)$ (цикл z , проходящий через вершину $v_0 + r(n-1)$), простой, где $v_0 \in \{1, \dots, r\}$, то и путь (цикл) $\Theta(z)$ в графе $\Gamma(\psi)$ простой.

б) Для любого простого пути w длины $\tau > 0$ (цикла w длины $\tau > 1$) в графе $\Gamma(\psi)$ класс $[w]$ содержит непустое множество простых путей (простых циклов) графа $\Gamma(\varphi)$.

Доказательство.

а) Простой путь (цикл) z не содержит одинаковых вершин, в частности, не содержит более одного раза вершину $v_0 + (n-1)r$. Если путь (цикл) z целиком состоит из вершин цикла C_{v_0} , то $\Theta(z)$ есть путь (цикл длины 1), состоящий из единственной вершины v_0 , то есть $\Theta(z)$ простой.

В противном случае путь (цикл) z представляется с помощью конкатенации путей, составленной из вершин различных циклов $C_{v_0}, \dots, C_{v_\tau}$, где $\tau \geq 1$, при этом путь z и цикл z имеют соответствующий вид:

- $z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z'_\tau$ — путь,
- $z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z_\tau \cdot \delta_\tau$ — цикл,

где z_j — путь в цикле C_{v_j} с начальной вершиной $v_j + r(n-1)$ и с конечной вершиной $v_j + rk_j$, взятой из строки с номером v_j таблицы $T_{v_{j+1}}$; $v_{\tau+1} = v_0$ (длина пути z_j не более n , иначе путь z не простой); z'_τ — путь в цикле C_{v_τ} длины менее n с начальной вершиной $v_\tau + r(n-1)$; $\delta_j = (v_j + rk_j, v_{j+1} + r(n-1))$ — дуги графа $\Gamma(\varphi)$, $j = 0, \dots, \tau$.

Осталось заметить, что $\Theta(z) = (v_0, v_1, \dots, v_\tau)$ и числа $v_0, v_1, \dots, v_\tau$ попарно различные. Действительно, если $v_i = v_j$, где $i, j \in \{0, 1, \dots, \tau\}$, $i \neq j$, то совпадают начальные вершины путей z_i и z_j (z_i и z'_τ), это противоречит тому, что путь (цикл) z простой.

б) Дадим конструктивное описание всех эквивалентных простых путей (циклов) в графе $\Gamma(\varphi)$, которым в графе $\Gamma(\psi)$ соответствует простой путь (цикл) $\Theta(z)$, а именно: если $w = (v_0, v_1, \dots, v_\tau)$ — простой путь (цикл) в графе $\Gamma(\psi)$, то простой путь (цикл) z в графе $\Gamma(\varphi)$, для которого $\Theta(z) = w$, является конкатенацией путей

$$z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z'_\tau \quad (z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z_\tau \cdot \delta_\tau).$$

Перебирая все возможные комбинации вершин в строках с номерами v_j таблиц $T_{v_{j+1}}$, $j = 0, \dots, \tau$, получаем требуемое множество эквивалентных путей из класса $[w]$. ■

Обозначим: $L_\psi(w)$ — длина пути w в графе $\Gamma(\psi)$; $L_\varphi(z)$ — длина пути z в графе $\Gamma(\varphi)$.

Теорема 2.

а) Если в графе $\Gamma(\psi)$ имеется простой путь $w = (v_0, v_1, \dots, v_\tau)$ длины $\tau > 0$, то при любых $\lambda, \mu \in \{0, \dots, n-1\}$ в графе $\Gamma(\varphi)$ имеется принадлежащий классу $[w]$ простой

путь $z(w, \lambda, \mu)$ из вершины $v_0 + r\lambda$ в вершину $v_\tau + r\mu$, длина которого

$$L_\varphi(z(w, \lambda, \mu)) = n\tau + L(\lambda, m(v_0, v_1)) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau) - \mu.$$

б) Если в графе $\Gamma(\psi)$ имеется простой цикл $w = (v_0, v_1, \dots, v_{\tau-1})$ длины $\tau > 1$, то в $\Gamma(\varphi)$ имеется принадлежащий классу $[w]$ простой цикл $z(w)$, длина которого

$$L_\varphi(z(w)) = n\tau + L(\lambda, m(v_0, v_1)) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau).$$

Доказательство.

а) В соответствии с теоремой 1б путь $z(w, \lambda, \mu) \in [w]$ имеет вид (номера существенных переменных в строках таблиц T_u взяты наибольшие)

$$z(w, \lambda, \mu) = [\lambda, m(v_0, v_1)]_{v_0} \cdot \delta_0 \cdot [n-1, m(v_1, v_2)]_{v_1} \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot [n-1, \mu]_{v_\tau}.$$

Длины путей $[\lambda, m(v_0, v_1)]_{v_0}$, $[n-1, m(v_s, v_{s+1})]_{v_s}$ и $[n-1, \mu]_{v_\tau}$ в соответствии со свойством 4 равны соответственно $L(\lambda, m(v_0, v_1))$, $n-1-m(v_s, v_{s+1})$ и $n-1-\mu$, $s = 1, \dots, \tau-1$. В пути $z(w, \lambda, \mu)$ имеются также дуги $\delta_0, \dots, \delta_{\tau-1}$. Следовательно,

$$L_\varphi(z(w, \lambda, \mu)) = L(\lambda, m(v_0, v_1)) + (\tau-1)(n-1) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau) + (n-1) - \mu + \tau = n\tau + L(\lambda, m(v_0, v_1)) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau) - \mu.$$

б) В соответствии с теоремой 1б проходящий через вершину $v_0 + r(n-1)$ цикл $z(w) \in [w]$ имеет вид

$$z(w) = [n-1, m(v_0, v_1)]_{v_0} \cdot \delta_0 \cdot [n-1, m(v_1, v_2)]_{v_1} \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-2} \cdot [n-1, m(v_{\tau-1}, v_0)]_{v_{\tau-1}} \cdot \delta_{\tau-1}.$$

В соответствии со свойством 4 длины путей $[n-1, m(v_s, v_{s+1})]$ равны $n-1-m(v_s, v_{s+1})$, $s = 0, \dots, \tau-1$, $v_\tau = v_0$. В цикле $z(w)$ имеются также дуги $\delta_0, \dots, \delta_{\tau-1}$. Следовательно,

$$\begin{aligned} L_\varphi(z(w)) &= \tau(n-1) - m(v_0, v_1) - \dots - m(v_{\tau-2}, v_{\tau-1}) - m(v_{\tau-1}, v_0) + \tau = \\ &= n\tau - m(v_0, v_1) - \dots - m(v_{\tau-2}, v_{\tau-1}) - m(v_{\tau-1}, v_0). \end{aligned}$$

Теорема доказана. ■

Следствие 1. В условиях теоремы имеют место следующие неравенства:

$$\text{а) } \tau \leq L_\varphi(z(w, \lambda, \mu)) \leq n\tau + n - \tau;$$

$$\text{б) } \tau \leq L_\varphi(z(w)) \leq n\tau - \tau.$$

Доказательство. Вытекает из оценок $1 \leq m(v_1, v_2) \leq n-1, \dots, 1 \leq m(v_{\tau-1}, v_\tau) \leq n-1$, $0 \leq L(\lambda, m(v_0, v_1)) \leq n-1$, $0 \leq \mu \leq n-1$. ■

Обозначим через d_ψ и d_φ диаметры графов $\Gamma(\varphi)$ и $\Gamma(\psi)$ соответственно.

Теорема 3. Для сильносвязного графа $\Gamma(\psi)$ с диаметром $d_\psi > 1$ верны оценки

$$d_\psi - 1 + n \leq d_\varphi \leq (n-1) \min\{d_\psi, r-1\} + n.$$

Доказательство. Верхняя оценка доказана в [1, теорема 3.1]. Докажем нижнюю оценку. При $r > 1$ в сильносвязном графе $\Gamma(\psi)$ с диаметром $d_\psi > 1$ имеется пара различных вершин (v_0, v_τ) , для которых кратчайший путь $w = (v_0, \dots, v_\tau)$ имеет длину $\tau = d_\psi - 1$. Тогда по теореме 2а в $\Gamma(\varphi)$ при $\lambda = \mu = 0$ и $m(v_{j-1}, v_j) = n-1$, $j = 2, \dots, \tau$, имеется кратчайший путь $z(w, 0, 0) \in [w]$ из вершины v_0 в вершину v_τ вида

$$z(w, 0, 0) = [0, m(v_0, v_1)]_{v_0} \cdot \delta_0 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot [n-1, 0]_{v_\tau},$$

где $\delta_j = (v_j + r(n-1), v_{j+1} + r(n-1))$ — дуги графа $\Gamma(\varphi)$, $j = 0, \dots, \tau-1$. С учётом оценок $L(0, m(v_0, v_1)) \geq 1$ и $L(n-1, 0) = n-1$ получаем отсюда длину пути $z(w, 0, 0)$ равную $\tau + n$. Длина пути $z(w, 0, 0)$ является нижней оценкой для d_φ , так как пути w и $z(w, 0, 0)$ кратчайшие. ■

3. Примитивность и экспонент перемешивающего графа

Пусть U_ψ — множество дуг (v, u) графа $\Gamma(\psi)$, таких, что координатная функция $\varphi_{u+(n-1)r}$ подстановки φ зависит существенно от переменных x_{v+tr} не менее чем при двух различных значениях t , где $t \in \{1, \dots, n-1\}$ (в v -й строке таблицы T_u записано не менее двух вершин).

Теорема 4 (достаточное условие примитивности сильносвязного орграфа $\Gamma(\varphi)$). Пусть $(v, u) \in U_\psi$ и координатная функция $\varphi_{u+(n-1)r}$ зависит существенно от переменных с номерами $v + r(t - d_j^{(v,u)})$, $j = 0, \dots, h_{v,u}$, где

$$h_{v,u} > 0, \quad 0 = d_0^{(v,u)} < \dots < d_{h_{v,u}}^{(v,u)} \leq n-2, \quad t \in \{d_{h_{v,u}}^{(v,u)} + 1, \dots, n-1\}.$$

Тогда граф $\Gamma(\varphi)$ примитивен, если $(n, \vartheta) = 1$, где

$$\vartheta = \text{НОД}\{\vartheta_{v,u} : (v, u) \in U_\psi\}, \quad \vartheta_{v,u} = (d_1^{(v,u)}, \dots, d_{h_{v,u}}^{(v,u)}).$$

Доказательство. По условию граф $\Gamma(\varphi)$ сильносвязный, тогда и $\Gamma(\psi)$ сильносвязный. Обозначим w простой цикл длины $\tau > 1$ в графе $\Gamma(\psi)$, проходящий через дугу (v, u) . Без ограничения общности можно считать, что $w = (1, 2, \dots, \tau)$, $v = \tau$ и $u = 1$, то есть функция $\varphi_{1+(n-1)r}$ зависит существенно от переменных с номерами $\tau + r(t - d_j^{(\tau,1)})$, $j = 0, \dots, h_{\tau,1}$. Следовательно, в сильносвязном графе $\Gamma(\varphi)$ существует простой цикл $z(w)$, проходящий через вершину с номером $\tau + rt$ (в этом случае $j = 0$ и $d_0^{(\tau,1)} = 0$) и представимый конкатенацией следующих путей (при $t = m(\tau, 1)$ данный цикл совпадает с циклом, рассмотренным при доказательстве теоремы 2б):

$$z(w) = [n-1, m(1, 2)]_1 \cdot \delta_1 \cdot \dots \cdot [n-1, m(\tau-1, \tau)]_{\tau-1} \cdot \delta_{\tau-1} \cdot [n-1, t]_\tau \cdot \delta_\tau,$$

где $\delta_\tau = (\tau + rt, 1 + r(n-1))$ и $\delta_s = (s + rm(s, s+1), s+1 + r(n-1))$, $s = 1, \dots, \tau-1$.

Так как при $j = 1, \dots, h_{\tau,1}$ переменные с номерами $\tau + r(t - d_j^{(\tau,1)})$ также являются существенными для координатной функции $\varphi_{1+(n-1)r}$, то в сильносвязном графе $\Gamma(\varphi)$ существуют простые циклы $z_j(w)$, каждый из которых проходит через все вершины цикла $z(w)$ и содержит новую вершину с номером $\tau + r(t - d_j^{(\tau,1)})$:

$$z_1(w) = [n-1, m(1, 2)]_1 \cdot \delta_1 \cdot \dots \cdot [n-1, m(\tau-1, \tau)]_{\tau-1} \cdot \delta_{\tau-1} \cdot [n-1, t - d_1^{(\tau,1)}]_\tau \cdot \delta_\tau^1, \dots,$$

$$z_{h_{\tau,1}}(w) = [n-1, m(1, 2)]_1 \cdot \delta_1 \cdot \dots \cdot [n-1, m(\tau-1, \tau)]_{\tau-1} \cdot \delta_{\tau-1} \cdot [n-1, t - d_{h_{\tau,1}}^{(\tau,1)}]_\tau \cdot \delta_\tau^{h_{\tau,1}},$$

где $\delta_\tau^j = (\tau + r(t - d_j^{(\tau,1)}), 1 + r(n-1))$.

При фиксированных τ и t длины циклов $z(w)$, $z_1(w)$, $\dots$, $z_{h_{\tau,1}}(w)$ равны

$$L_\varphi(z(w)) = n\tau - m(1, 2) - m(2, 3) - \dots - m(\tau-1, \tau) - t,$$

$$L_\varphi(z_1(w)) = L_\varphi(z(w)) + d_1^{(\tau,1)}, \quad \dots, \quad L_\varphi(z_{h_{\tau,1}}(w)) = L_\varphi(z(w)) + d_{h_{\tau,1}}^{(\tau,1)}.$$

Таким образом, если для рассмотренной дуги $(\tau, 1)$ обозначить $L_\varphi(z(w)) = \lambda_{\tau,1}$ и распространить аналогичные рассуждения на произвольную дугу $(v, u) \in U_\psi$, то получим, что для любой дуги в графе $\Gamma(\varphi)$ имеются простые циклы длины n , $\lambda_{v,u}$, $\lambda_{v,u} + d_1^{(v,u)}$, $\dots$, $\lambda_{v,u} + d_{h_{v,u}}^{(v,u)}$ при некотором натуральном числе $\lambda_{v,u}$. Если все эти числа имеют делитель $\mu > 1$, то μ делит не только число n , но и разность любой пары из этих чисел, в частности делит числа $d_1^{(v,u)}$, $\dots$, $d_{h_{v,u}}^{(v,u)}$. Отсюда μ делит числа $\vartheta_{v,u}$ для

любой дуги $(v, u) \in U_\psi$ и, следовательно, μ делит ϑ . Имеем противоречие с условием $(n, \vartheta) = 1$. Тогда длины указанных простых циклов взаимно просты, и в соответствии с [2, с. 226] граф $\Gamma(\varphi)$ примитивный. ■

В качестве следствия уточним оценку экспонента, полученную в [1, теорема 3.3].

Следствие 2.

а) Если w — простой цикл длины $\tau > 1$ в примитивном графе $\Gamma(\psi)$, то

$$\exp \Gamma(\varphi) \leq nr + \min\{n, L_\varphi(z(w))\}(nr - 2).$$

б) Пусть $\tau_{v,u}$ — длина простого цикла $w_{v,u}$ в графе $\Gamma(\psi)$, проходящего через дугу (v, u) , где $\tau_{v,u} > 1$, и функция $\varphi_{u+r(n-1)}$ зависит существенно от x_{v+rt} и $x_{v+r(t-1)}$, $t \in \{2, \dots, n-1\}$. Тогда граф $\Gamma(\varphi)$ примитивный и

$$\exp \Gamma(\varphi) \leq (\lambda_{v,u})^2 - 2\lambda_{v,u} + 2nr - 1,$$

где $\lambda_{v,u}$ — длина простого цикла $z(w_{v,u})$ в графе $\Gamma(\varphi)$, проходящего через дугу $(v + rt, u + (n-1)r)$.

в) Если в графе $\Gamma(\varphi)$ имеется простой цикл H длины L , проходящий через дугу $(v + tr, u + (n-1)r)$, где $(L, n) = 1$, то

$$\exp \Gamma(\varphi) \leq n(L + 2r) - t - L - 2 \min\{L, n\}.$$

Доказательство.

а) Оценка экспонента следует из теоремы [2, с. 227]: для примитивного m -вершинного графа Γ выполняется $\exp \Gamma \leq m + \lambda(m - 2)$, где λ — длина кратчайшего цикла.

б) Граф $\Gamma(\varphi)$ содержит простые циклы $z(w_{v,u})$ и $z_1(w_{v,u})$, их длины равны соответственно $\lambda_{v,u}$ и $\lambda_{v,u} + 1$, отсюда $(\lambda_{v,u}, \lambda_{v,u} + 1) = 1$ и граф $\Gamma(\varphi)$ примитивный. Тогда в соответствии с [3, теорема 1б] для экспонента графа $\Gamma(\varphi)$ верна оценка $\exp \Gamma(\varphi) \leq (\lambda_{v,u})^2 - 2\lambda_{v,u} + 2nr - 1$.

в) Граф $\Gamma(\varphi)$ содержит независимые простые циклы $C_1, \dots, C_r$ длины n . Если $(L, n) = 1$, то граф $\Gamma(\varphi)$ примитивный. По условию цикл H в графе $\Gamma(\varphi)$ проходит через дугу $(v + tr, u + (n-1)r)$, следовательно, он проходит через вершины $v + (n-1)r, v + (n-2)r, \dots, v + tr$, то есть цикл H имеет $n - t$ общих вершин с циклом C_v .

Оценим экспонент графа $\Gamma(\varphi)$. Используя формулу теоремы 1б [3] при $n < L$, получим

$$\exp \Gamma(\varphi) \leq Ln - L - 3n + n - t + 2nr = n(L + 2r) - t - L - 2n,$$

используя формулу теоремы 1б [3] при $L < n$, имеем

$$\exp \Gamma(\varphi) \leq nL - n - 3L + n - t + 2nr = n(L + 2r) - t - L - 2L.$$

Таким образом, в обоих случаях верна оценка

$$\exp \Gamma(\varphi) \leq n(L + 2r) - t - L - 2 \min\{L, n\}.$$

Следствие доказано. ■

Замечание. Оценка следствия а лучше оценки теоремы 3.3 [1] при $L_\varphi(z(w)) < n$, необходимое условие этого $\tau < n$.

Оценка следствия б лучше оценки теоремы 3.3 [1] при $\lambda_{v,u} < \sqrt{n^2r - n(r-2)}$.

Оценка следствия в лучше оценки теоремы 3.3 [1] при $L < r(n-1)$.

Заключение

Для подстановок φ регистров сдвига длины n над множеством r -мерных двоичных векторов с сильносвязным перемешивающим графом $\Gamma(\varphi)$:

- описаны множества простых путей и циклов графа $\Gamma(\varphi)$, оценены их длины;
- получены новые достаточные условия примитивности графа $\Gamma(\varphi)$;
- уточнены верхние оценки экспонента графа $\Gamma(\varphi)$.

ЛИТЕРАТУРА

1. Коренева А. М., Фомичев В. М. Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3 (17). С. 34–40.
2. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
3. Фомичев В. М. Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2 (12). С. 101–112.