МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.17

О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩИХ ОРГРАФОВ РЕГИСТРОВ СДВИГА С ДВУМЯ ОБРАТНЫМИ СВЯЗЯМИ

А. М. Коренева

Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

С помощью матрично-графового подхода исследуются перемешивающие свойства преобразований регистров сдвига с двумя обратными связями над множеством V_r двоичных r-мерных векторов, $r > 1$. Под перемешивающими свойствами понимается существенная зависимость координатных булевых функций различных степеней регистровых преобразований от знаков начального состояния регистра, рассматриваемых как независимые переменные. Для перемешивающих орграфов подстановок регистров сдвига с двумя обратными связями, построенных на основе модифицированных аддитивных генераторов, доказан критерий примитивности и получены достижимые верхние оценки экспонента, которые существенно улучшают все другие известные оценки экспонентов для тех же орграфов.

Ключевые слова: *матрично-графовый подход, модифицированный аддитивный генератор, перемешивающий орграф, примитивность, регистр сдвига, экспонент.*

DOI 10.17223/20710410/37/3

ON PRIMITIVITY OF MIXING DIGRAPHS ASSOCIATED WITH 2-FEEDBACKS SHIFT REGISTERS

A. M. Koreneva

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

E-mail: alisa.koreneva@gmail.com

Analysis of mixing properties of round transformations is an important issue in the theory of symmetric iterative block ciphers. For researching this subject, a matrix-digraph approach is widely used in cryptography. This approach allows to characterize the required properties in terms of primitivity and exponent of a matrix (or a digraph) related to the transformations concerned. This paper is devoted to such a characterization of mixing properties of transformations fulfilled by 2-feedback shift registers. For naturals n, m, and r, let $n > 1$, $r > 1$, $0 \leqslant m \leqslant n-2$, $V_r = (\mathrm{GF}(2))^r$; $f_m : V_r^n \to V_r$ and $f_{n-1} : V_r^n \to V_r$ are some feedback functions; $\mu : V_r \to V_r$ and $g : V_r \to V_r$ are some permutations over V_r used to modify feedbacks f_m and f_{n-1} respectively; $x_{\delta_0}, x_{\delta_1}, \ldots, x_{\delta_p}$ are all essential variables of the function $f_m(x_0, x_1, \ldots, x_{n-1})$, $\delta_0 = m+1$, $0 < \delta_1 < \ldots < \delta_p < n$, $p > 0$; $x_{d_0}, x_{d_1}, \ldots, x_{dq}$ are all essential variables of the function $f_{n-1}(x_0, x_1, \ldots, x_{n-1})$,

$d_0 = 0$, $d_1 < \ldots < d_q < n$, $q > 0$; $\varphi^{g,\mu} : V_r^n \to V_r^n$, $\varphi^{g,\mu}(x_0, x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{m-1}, \mu(f_m(x_0, \ldots, x_{n-1})), x_{m+1}, \ldots, x_{n-2}, g(f_{n-1}(x_0, \ldots, x_{n-1})))$. In fact, $\varphi^{g,\mu}$ is the transition function of a shift register of the length n over V_r with two feedback functions $\mu(f_m(x))$ and $g(f_{n-1}(x))$, $x = x_0x_1 \ldots x_{n-1}$. Let $M(\varphi^{g,\mu}) = M$ be a Boolean matrix (m_{ij}) (called the mixing matrix of the map $\varphi^{g,\mu}$), where $m_{ij} = 1$ iff the j-th coordinate function of the map $\varphi^{g,\mu}$ essentially depends on the variable x_i $(i, j \in \{0, 1, \ldots, n-1\})$. The matrix M is said to be primitive if there is a power $M^e = \left(m_{ij}^{(e)}\right)$ of its mixing matrix M such that $m_{ij}^{(e)} > 0$ for all i and j; in this case, the least power e is called an exponent of M and is denoted by $\exp M$. The conceptions of the primitiveness and exponent of the matrix $M(\varphi^{g,\mu})$ expend to the digraph $\Gamma(\varphi^{g,\mu})$ with the adjacency matrix M — the mixing graph associated with $\varphi^{g,\mu}$. The main results of the paper are the following: 1) it is proved that the strongly connected digraph $\Gamma(\varphi^{g,\mu})$ is primitive iff $\delta_1 > m$ and the numbers in the set $L' = \{n - d_i, n + m + 1 - d_j - \delta_k : i = 0, \ldots, q, j = 0, \ldots, t, k = 1, \ldots, p\}$ are relatively prime or $\delta_1 \leqslant m$ and the numbers in the set $L = \{n - d_i, n + m + 1 - d_j - \delta_k, m + 1 - \delta_l : i = 0, \ldots, q, j = 0, \ldots, t, k = \tau + 1, \ldots, p, l = 1, \ldots, \tau\}$ are relatively prime, where t and τ are determined by the conditions: d_t and δ_τ are the largest numbers in $D = \{d_0, \ldots, d_q\}$ and $\Delta = \{\delta_0, \ldots, \delta_p\}$ with the properties $d_t \leqslant m$ and $\delta_\tau \leqslant m$ respectively; 2) for $\exp \Gamma(\varphi^{g,\mu})$, some attainable upper bounds depending on m and other parameters in D and Δ are obtained, improving all the known exponent estimates for the same digraphs. Particularly, if $(n-1) \in D$ and $m \in \Delta$, then $\exp \Gamma(\varphi^{g,\mu}) \leqslant \min\{\rho(D) + \varepsilon, \rho(\Delta) + \varepsilon'\}$, where $\rho(D) = \max\{n - d_q, d_q - d_{q-1}, \ldots, d_1 - d_0\}$, $\rho(\Delta) = \max\{\delta_1 + n - \delta_p, \delta_p - \delta_{p-1}, \ldots, \delta_0 - \delta_r, \ldots, \delta_2 - \delta_1\}$, $\varepsilon = \max\{2n - m - 2 - d_q, n + m - \max\{\delta_0, \delta_p\}\}$, and $\varepsilon' = \max\{2m + 1 - \delta_\tau, n - 1 - d_t\}$. These results can be successfully used in construction of iterative cryptographic algorithms based on $\varphi^{g,\mu}$ with the rapid input data mixing.

Keywords: *primitive digraph, exponent, mixing digraph, multi-feedback shift register, modified additive generator.*

Введение

Введём основные обозначения:

- V_n — n-мерное пространство двоичных векторов, $n \in \mathbb{N}$, $n > 1$;
- $\mathbb{Z}_n$ — кольцо вычетов по модулю n, $n > 1$;
- $E(\varphi)$ — множество номеров существенных переменных дискретной функции φ;
- $\exp \Gamma$ — экспонент орграфа Γ;
- (i, j) — дуга в орграфе, инцидентная вершинам i и j;
- $w(i_0, i_1, \ldots, i_k)$ — путь в орграфе, последовательно проходящий через вершины $i_0, i_1, \ldots, i_k$, $k \in \mathbb{N}$;
- $w[i, j]$ — путь $w(i_0, i_1, \ldots, i_k)$, где $i = i_0$ и $j = i_k$;
- $c(i_0, i_1, \ldots, i_k)$ — контур в орграфе, последовательно проходящий через вершины $i_0, i_1, \ldots, i_k$, $k \in \mathbb{N}$;
- $w \cdot w'$ — конкатенация путей w и w' в орграфе (определена, если и только если конечная вершина пути w совпадает с начальной вершиной пути w');
- $tC(i)$ — t-кратно пройденный контур C, начиная из вершины i;
- $\operatorname{len} w$ ($\operatorname{len} c$) — длина пути w (контура c), равная числу дуг пути (контура);
- $\langle L \rangle$ — аддитивная полугруппа, порождённая множеством L, где $L \subset \mathbb{N}$;
- МАГ — модифицированный аддитивный генератор.

Точное определение существенных переменных для степеней преобразования $\varphi : X^n \to X^n$, где X — векторное пространство над конечным полем, связано, как правило, с кратным просмотром таблиц координатных функций, т. е. вычислительная сложность задачи зависит от n экспоненциально. Поэтому для исследования перемешивающих свойств таких преобразований применяется оценочный матрично-графовый подход, при реализации которого существенная зависимость координат выходных векторов от координат входных кодируется 0,1-матрицей $M(\varphi) = (m_{ij})$ порядка n: $m_{ij} = 1 \Leftrightarrow i \in E(\varphi_j), i, j \in \{0, \ldots, n-1\}$, где $\varphi_0, \ldots, \varphi_{n-1}$ — координатные функции преобразования φ. Матрица $M(\varphi)$ называется перемешивающей матрицей преобразования φ. Равносильно для исследования перемешивающих свойств рассматривается n-вершинный перемешивающий орграф $\Gamma(\varphi)$, матрица смежности вершин которого совпадает с $M(\varphi)$. Важными характеристиками перемешивающей матрицы (орграфа) является примитивность, т. е. положительность матрицы $M(\varphi)$ в некоторой степени, и экспонент примитивной матрицы $M(\varphi)$ (орграфа $\Gamma(\varphi)$): $\exp \Gamma(\varphi) = \exp M(\varphi) = \min\{\gamma \in \mathbb{N} : M(\varphi)^\gamma > 0\}$. Значение экспонента есть нижняя оценка числа итераций преобразования, после которых достигается полное перемешивание входных данных, т. е. зависимость каждой выходной координаты от всех входных координат.

В работе исследуется примитивность перемешивающих орграфов преобразований некоторых классов регистров сдвига длины n над множеством V_r с двумя обратными связями, оцениваются их экспоненты. Полученные выводы развивают результаты работ [1, 2] для регистров сдвига длины n над V_r с одной обратной связью.

В п. 1 доказан критерий биективности регистровых преобразований с произвольным числом обратных связей. В п. 2 исследованы множества простых путей и контуров перемешивающего орграфа регистра с двумя обратными связями. В п. 3 описан частный класс регистров сдвига с двумя обратными связями, построенных на основе модифицированных аддитивных генераторов. В п. 4 доказан критерий примитивности и получены оценки экспонента перемешивающего орграфа для частного класса регистров сдвига с двумя обратными связями.

1. Биективность регистровых преобразований из класса $R(n, X, t)$

При $n, r, t \in \mathbb{N}$, где $n > t \geqslant 1, r > 1$, обозначим: $R(n, X, t)$ — класс регистров сдвига длины n над множеством X с t обратными связями; $\varphi^X : X^n \to X^n$ — преобразование конечного множества X, реализуемое регистром из класса $R(n, X, t)$.

Рассмотрим функции $f_i(x_0, \ldots, x_{n-1}) : X^n \to X, i = 1, \ldots, t$, где $t < n$; X — векторное пространство над конечным полем; $x_0, \ldots, x_{n-1} \in X$. Пусть $Y \subset \{x_0, \ldots, x_{n-1}\}$, $|Y| = t$.

Система функций $F_t = \{f_1(x_0, \ldots, x_{n-1}), \ldots, f_t(x_0, \ldots, x_{n-1})\}$ называется биективной по множеству переменных Y, если F_t реализует подстановку множества X^t при любой фиксации переменных из множества $\{x_0, \ldots, x_{n-1}\} \setminus Y$.

Пусть $t > 1$ и $j_1, \ldots, j_t$ — номера ячеек регистра сдвига из класса $R(n, X, t)$, в которые записываются в каждом такте значения функций обратной связи. Преобразование $\varphi^X(x_0, \ldots, x_{n-1})$ регистра сдвига с функциями обратной связи $f_{j_s}(x_0, \ldots, x_{n-1}) : X^n \to X$, $s = 1, \ldots, t$, $j_1, \ldots, j_{t-1} \in \{0, \ldots, n-2\}$, $j_t = n-1$, определим системой координатных функций $\{\varphi_0^X(x_0, \ldots, x_{n-1}), \ldots, \varphi_{n-1}^X(x_0, \ldots, x_{n-1})\}$ в соответствии с формулами

$$\varphi_i^X(x_0,\dots,x_{n-1}) = x_{i+1} + \xi_i(x_0,\dots,x_i,x_{i+2},\dots,x_{n-1}),\ i=0,\dots,n-3; \quad (1)$$

$$\varphi_{n-2}^X(x_0,\dots,x_{n-1}) = x_{n-1} + \xi_{n-2}(x_0,\dots,x_{n-2}); \quad (2)$$

$$\varphi_{n-1}^X(x_0,\dots,x_{n-1}) = x_0 + \xi_{n-1}(x_1,\dots,x_{n-1}), \quad (3)$$

где $\xi_i(x_0,\dots,x_i,x_{i+2},\dots,x_{n-1}) = 0$ для всех $i \in \{0,\dots,n-3\} \setminus \{j_1,\dots,j_{t-1}\}$; $\xi_{n-2}(x_0, \dots,x_{n-2}) = 0$, если $j_{t-1} \neq n-2$, и $\xi_{n-1}(x_1,\dots,x_{n-1}) \neq 0$.

Обозначим: $F_t = \{f_{j_s}(x_0,\dots,x_{n-1}) : s = 1,\dots,t\}$ — система функций обратных связей регистра из класса $R(n,X,t)$; Z — множество переменных $\{x_0, x_{j_1+1},\dots,x_{j_{t-1}+1}\}$.

Теорема 1. Преобразование φ^X регистра сдвига из класса $R(n,X,t)$ биективно, если и только если система функций F_t биективна по множеству переменных Z.

Доказательство. Пусть преобразование φ^X регистра сдвига небиективно. Тогда в множестве X^n найдутся наборы $\alpha = (\alpha_0,\dots,\alpha_{n-1})$ и $\beta = (\beta_0,\dots,\beta_{n-1}), \alpha \neq \beta$, такие, что $\varphi^X(\alpha) = \varphi^X(\beta)$, то есть $\varphi_i^X(\alpha_0,\dots,\alpha_{n-1}) = \varphi_i^X(\beta_0,\dots,\beta_{n-1})$, $i = 0,\dots,n-1$. Из (1)–(3) получаем $\alpha_k = \beta_k$ для всех $k \in \{1,\dots,n-1\} \setminus \{j_1+1,\dots,j_{t-1}+1\}$. Так как $\alpha \neq \beta$, то $(\alpha_0,\alpha_{j_1+1},\dots,\alpha_{j_{t-1}+1}) \neq (\beta_0,\beta_{j_1+1},\dots,\beta_{j_{t-1}+1})$. Вместе с тем из равенства $\varphi^X(\alpha) = \varphi^X(\beta)$ следует, что $(f_{j_1}(\alpha),\dots,f_{j_t}(\alpha)) = (f_{j_1}(\beta),\dots,f_{j_t}(\beta))$. Значит, система функций F_t при некоторой фиксации переменных $\{x_0,\dots,x_{n-1}\} \setminus Z$ реализует неинъективное и, следовательно, небиективное преобразование множества X^t.

В обратную сторону. Если φ^X — подстановка, то $\varphi^X(\alpha) \neq \varphi^X(\beta)$ для любых $\alpha = (\alpha_0,\dots,\alpha_{n-1})$ и $\beta = (\beta_0,\dots,\beta_{n-1}), \alpha \neq \beta$. Возьмём α и β такие, что $\alpha_k = \beta_k$ для всех $k \in \{0,\dots,n-1\} \setminus \{0, j_1+1,\dots,j_{t-1}+1\}$. Из (1)–(3) следует, что при таких α и β неравенство $\varphi^X(\alpha) \neq \varphi^X(\beta)$ выполнено, только если $(f_{j_1}(\alpha),\dots,f_{j_t}(\alpha)) \neq$ $\neq (f_{j_1}(\beta),\dots,f_{j_t}(\beta))$. В силу произвольности выбора элементов α_k получаем для $k = \{0,\dots,n-1\} \setminus \{0, j_1+1,\dots,j_{t-1}+1\}$, что при любой фиксации переменных $\{x_0,\dots,x_{n-1}\} \setminus Z$ система функций F_t задаёт инъективное преобразование, то есть подстановку множества X^t. ■

Обозначим через $R(n,r,t)$ класс регистров сдвига $R(n,X,t)$ при $X = V_r$. Преобразование $\varphi(z_0,\dots,z_{n-1})$ из $R(n,r,t)$ есть преобразование множества $V_{nr} = \{(z_0,\dots,z_{n-1}) : z_0,\dots,z_{n-1} \in V_r\}$, где $z_k = (x_{rk},\dots,x_{r-1+rk})^{\mathrm{T}}$ есть k-й столбец двоичной матрицы, определяющей состояние регистра, $k = 0,\dots,n-1$.

2. Перемешивающие свойства регистровых подстановок из $R(n,r,2)$

Рассмотрим регистровую подстановку $\varphi(z_0,\dots,z_{n-1}) \in R(n,r,2)$ с обратными связями f_{n-1} и f_m, $0 \leqslant m < n-1$, определённую формулой

$$\varphi(z_0,\dots,z_{n-1}) = \begin{cases} (f_m, z_2,\dots,z_{n-1},f_{n-1}), & \text{если } m=0,\\ (z_1,\dots,f_m,\dots,z_{n-1},f_{n-1}), & \text{если } 0<m<n-2,\\ (z_1,\dots,z_{n-2},f_m,f_{n-1}), & \text{если } m=n-2, \end{cases} \quad (4)$$

где $z_0,\dots,z_{n-1} \in V_r$; $f_{n-1} = z_0 \oplus \psi_1$ и $f_m = z_{m+1} \oplus \psi_2$; функции $\psi_1 : V_{r(n-1)} \to V_r$ и $\psi_2 : V_{r(n-2)} \to V_r$ отличны от констант (вместо операции суммирования векторов из V_r может быть рассмотрена любая бинарная операция на V_r, биективная по обеим переменным). Заметим, что в соответствии с теоремой 1 система функций $\{f_m(z_0,\dots,z_{n-1}), f_{n-1}(z_0,\dots,z_{n-1})\}$ биективна по множеству переменных $\{z_0, z_{m+1}\}$.

Для исследования перемешивающих свойств подстановки φ используем оценочный матрично-графовый подход. В перемешивающем nr-вершинном орграфе $\Gamma(\varphi)$ подстановки φ обозначим вершины числами $u+ri$, координатные булевы функции — φ_{u+ri},

$u = 0, \ldots, r-1$, $i = 0, \ldots, n-1$. В $\Gamma(\varphi)$ пара $(v+ri, u+rj)$ есть дуга, если и только если $(v + ri) \in E(\varphi_{u+rj})$, $v, u \in \{0, \ldots, r-1\}$, $i, j \in \{0, \ldots, n-1\}$. Для описания множества дуг орграфа $\Gamma(\varphi)$ достаточно в силу (4) описать множество существенных переменных координатных функций $\varphi_{u+r(n-1)}$ и φ_{u+rm}.

Из (4) следует, что орграф $\Gamma(\varphi)$ содержит независимые простые контуры c_u длины n, $u = 0, \ldots, r-1$, где $c_u = c(u + r(n-1), u + r(n-2), \ldots, u + r, u)$.

Пусть θ — функция отождествления вершин орграфа $\Gamma(\varphi)$: при $u = 0, \ldots, r-1$ и любом $i = 0, \ldots, n-1$ положим $\theta(u + ri) = u$. Функция θ индуцирует функцию Θ, отображающую nr-вершинный орграф $\Gamma(\varphi)$ в r-вершинный орграф $\Gamma(\psi) = \Gamma(\psi_1) \cup \cup \Gamma(\psi_2)$, где пара (v, u) образует дугу орграфа $\Gamma(\psi_1)$ (орграфа $\Gamma(\psi_2)$), если и только если функция $\varphi_{u+r(n-1)}$ (функция φ_{u+rm}) зависит существенно хотя бы от одной из переменных $x_v, x_{v+r}, \ldots, x_{v+r(n-1)}$, $v, u \in \{0, \ldots, r-1\}$. На рис. 1 изображена часть перемешивающего орграфа $\Gamma(\varphi)$ подстановки φ, содержащая контуры c_v и c_u при $v \neq u$, которая при отождествлении вершин преобразуется в дугу (v, u) орграфа $\Gamma(\psi)$. Здесь координатные функции φ_{u+rm} и $\varphi_{u+r(n-1)}$ зависят существенно от некоторых из переменных $x_v, x_{v+r}, \ldots, x_{v+r(n-1)}$, $v, u \in \{0, \ldots, r-1\}$, что соответствует светлым дугам на рис. 1.

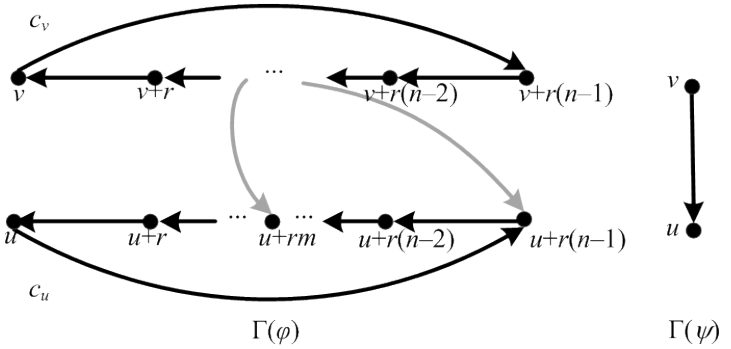

Рис. 1. Часть орграфа $\Gamma(\varphi)$ и соответствующая ей дуга в $\Gamma(\psi)$

Обозначим через Γ_0 орграф $\Gamma(\varphi)$ при функциях $\psi_1 \equiv \psi_2 \equiv 0$, то есть Γ_0 состоит из независимых простых контуров $c_0, \ldots, c_{r-1}$ длины n.

Теорема 2. Перемешивающий орграф $\Gamma(\varphi)$ сильносвязный, если и только если орграф $\Gamma(\psi)$ сильносвязный.

Доказательство. Множества вершин орграфов Γ_0 и $\Gamma(\varphi)$ совпадают и Γ_0 является частью орграфа $\Gamma(\varphi)$. Значит, если обе вершины орграфа $\Gamma(\varphi)$ принадлежат контуру c_u, то они взаимно достижимы, $u = 0, \ldots, r-1$. Следовательно, в орграфе $\Gamma(\varphi)$ при $u \neq v$, $u, v \in \{0, \ldots, r-1\}$, вершина $u+rj$ контура c_u достижима из вершины $v+ri$ контура c_v, если и только если u достижима из v в орграфе $\Gamma(\psi)$. ■

Используя индуктивный метод, опишем множество простых путей орграфа $\Gamma(\varphi)$.

При $v, u = 0, \ldots, r-1$ обозначим: $D(v, u)$ и $\Delta(v, u)$ — множества номеров переменных из множества $\{v, v + r, \ldots, v + r(n-1)\}$, существенных для координатных функций $\varphi_{u+r(n-1)}$ и φ_{u+rm} соответственно; $w[u + ri, u + rj]$ — путь в орграфе $\Gamma(\varphi)$, $i, j \in \{0, \ldots, n-1\}$. Так как простой путь $w[u+ri, u+rj]$ является частью контура c_u, его длина равна $i - j$, если $i \geqslant j$, и $n - j + i$, если $i < j$.

Пусть в орграфе $\Gamma(\psi)$ имеется дуга (v, u) (простой путь длины 1). Тогда в орграфе $\Gamma(\varphi)$ при любых $i, j \in \{0, \ldots, n-1\}$ имеются пути $w[v + ri, u + rj]$ (рис. 2) двух видов:

$$w[v+ri, v+ra]\cdot(v+ra, u+r(n-1))\cdot w[u+r(n-1), u+rj],$$
$$w[v+ri, v+rb]\cdot(v+rb, u+rm)\cdot w[u+rm, u+rj],$$

где $v+ra \in D(v,u)$, $v+rb \in \Delta(v,u)$. Заметим, что множество данных путей есть полный прообраз $\Theta^{-1}(v,u)$.

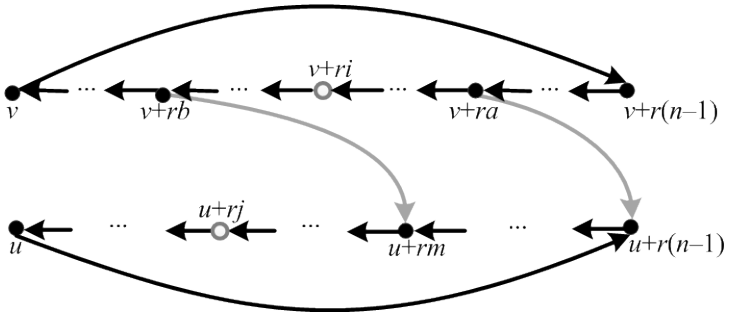

Рис. 2. Пути в орграфе $\Gamma(\varphi)$

Теперь, используя индукцию, опишем все прообразы относительно Θ для любого простого пути $w(u_1,\ldots,u_l)$ длины $l-1$ в $\Gamma(\psi)$, $l>2$. Пусть $w(u_1,\ldots,u_l) = w(u_1, \ldots, u_{l-1})\cdot(u_{l-1},u_l)$ и описаны все пути из множества $\Theta^{-1}(w(u_1,\ldots,u_{l-1}))$. В частности, описаны пути видов $w' = w[u_1{+}ri, u_{l-1}{+}ra]$ и $w'' = w[u_1{+}ri, u_{l-1}{+}rb]$ при $i=0,\ldots,n{-}1$ и любых a,b, таких, что $u_{l-1}+ra \in D(u_{l-1},u_l)$, $u_{l-1}+rb \in \Delta(u_{l-1},u_l)$. Тогда любой путь $w[u_1+ri, u_l+rj]$ из $\Theta^{-1}(w(u_1,\ldots,u_{l-1}))$ при любых $i,j \in \{0,\ldots,n-1\}$ есть конкатенация путей двух видов:

$$w[u_1+ri, u_l+rj] = w'\cdot(u_{l-1}+ra, u_l+r(n-1))\cdot w[u_l+r(n-1), u_l+rj],$$
$$w[u_1+ri, u_l+rj] = w''\cdot(u_{l-1}+rb, u_l+rm)\cdot w[u_l+rm, u_l+rj].$$

3. Регистровые преобразования на основе модифицированных аддитивных генераторов

В общем случае множества $D(v,u)$ и $\Delta(v,u)$ зависят от пары (v,u), $v,u=0,\ldots r-1$, следовательно, в орграфе $\Gamma(\varphi)$ описание путей и контуров большой длины является громоздким (см. п. 2). Опишем пути в важном для криптографических приложений случае, когда $D(v,u)=D$, $\Delta(v,u)=\Delta$ (множества $D(v,u)$ и $\Delta(v,u)$ одинаковы для всех пар (v,u)). В частности, таким свойством обладает преобразование множеств состояний аддитивных генераторов и некоторых их модификаций. Рассмотрим модификации, заключающиеся в применении преобразования к множеству значений функции обратной связи [3, 4]. При итерациях преобразования в некоторых таких модификациях достигается полное перемешивание входных данных, в то время как преобразования аддитивных генераторов плохо перемешивают входные данные. Определим аддитивные генераторы и их модификации.

Пусть b_r — биекция $\mathbb{Z}_{2^r} \leftrightarrow V_r$, определяющая двоичное r-разрядное представление числа $X \in \mathbb{Z}_{2^r}$ по правилу: если $X = 2^{r-1}x_0 + \ldots + 2x_{r-2} + x_{r-1}$, то $b_r(X) = \overline{X} = (x_0,\ldots,x_{r-1}) \in V_r$; b_r^{-1} — обратная к b_r функция. Аддитивный генератор есть регистр сдвига длины n над $\mathbb{Z}_{2^r}$ с функцией обратной связи $f: V_{nr} \to V_r$ следующего вида:

$$f(\overline{X}_0,\ldots,\overline{X}_{n-1}) = b_r\left(\left(\sum_{k\in D} X_k\right) \bmod 2^r\right),$$

где $D = \{d_0, \ldots, d_q\}$ — множество номеров существенных переменных функции f; $0 < q$; $0 = d_0 < \ldots < d_q < n$. Модифицированный аддитивный генератор (МАГ) есть регистр сдвига длины n с функцией обратной связи f^g:

$$f^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = g(f(\overline{X}_0, \ldots, \overline{X}_{n-1})) = b_r g\left(\left(\sum_{k\in D} X_k\right) \bmod 2^r\right),$$

то есть к значениям функции f применяется преобразование g множества V_r (в записи вида $b_r g(\cdot)$ умножение функций выполняется слева направо).

Преобразование φ^g множества состояний МАГ имеет вид

$$\varphi^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, \overline{X}_{n-1}, f^g(\overline{X}_0, \ldots, \overline{X}_{n-1})),$$

при этом φ^g — подстановка множества V_{nr}, если и только если g — подстановка множества V_r [4, теорема 1]. Перемешивающие свойства преобразования φ^g описаны в [4].

Актуальной задачей является улучшение перемешивающих свойств регистров, построенных на основе МАГ, то есть построение преобразований, перемешивающий орграф которых имеет более низкую оценку экспонента. Один из способов решения задачи — увеличение числа обратных связей в регистровом преобразовании. Исследуем перемешивающие свойства регистровых преобразований $\varphi^{g,\mu}$ с двумя обратными связями, построенных на основе МАГ (класс таких преобразований обозначим МАГ$(n, r, 2)$), где модификация выполнена с помощью преобразований g и μ множества V_r. В соответствии с (4) регистровое преобразование $\varphi^{g,\mu}$ с использованием преобразований g и μ при $0 \leqslant m < n-1$ задано одним из следующих равенств:

$$\varphi^{g,\mu}(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (f_m, \overline{X}_2, \ldots, \overline{X}_{n-1}, f_{n-1}),\ m = 0; \tag{5}$$

$$\varphi^{g,\mu}(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, f_m, \ldots, \overline{X}_{n-1}, f_{n-1}),\ 0 < m < n-2; \tag{6}$$

$$\varphi^{g,\mu}(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, \overline{X}_{n-2}, f_m, f_{n-1}),\ m = n-2. \tag{7}$$

Функции обратных связей f_{n-1} и f_m определены равенствами

$$f_{n-1} = b_r g\left(\left(\sum_{k\in D} X_k\right) \bmod 2^r\right); \tag{8}$$

$$f_m = b_r \mu\left(\left(\sum_{k\in \Delta} X_k\right) \bmod 2^r\right), \tag{9}$$

где $D, \Delta \subseteq \{0, \ldots, n-1\}$ — непустые множества номеров тех из чисел $X_0, \ldots, X_{n-1}$, которые суммируются в формулах (8) и (9) соответственно.

По теореме 1 преобразование $\varphi^{g,\mu}$ биективное, если и только если система функций обратной связи $\{f_m(X_0, \ldots, X_{n-1}), f_{n-1}(X_0, \ldots, X_{n-1})\}$ биективна по множеству переменных $\{X_0, X_{m+1}\}$. В частности, $\varphi^{g,\mu}$ является подстановкой, если $0 \in D \setminus \Delta$, $(m+1) \in \Delta$ и каждая координатная функция преобразований g и μ отлична от константы.

4. Примитивность и оценки экспонента перемешивающего орграфа МАГ$(n, r, 2)$

Получим критерий примитивности перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ и оценим его экспонент при $0 < m < n-2$ (при $m = n-2$ и 0 результаты получаются аналогично). Обозначим: $D = \{d_0, \ldots, d_q\}$, $\Delta = \{\delta_0, \ldots, \delta_p\}$, где $q, p > 0$; $0 = d_0 < \ldots < d_q < n$; $\delta_0 = m+1$; $0 < \delta_1 < \ldots < \delta_p < n$.

В [4] с использованием комбинаторных свойств биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$ описано множество существенных переменных функции обратной связи f^g, что позволило исследовать примитивность перемешивающего орграфа $\Gamma(\varphi^g)$ и оценить его экспонент. Описание множества существенных переменных функции f^g [4, теорема 2] справедливо для функций вида $b_r g\left(\left(\sum\limits_{k\in D} X_k\right) \bmod 2^r\right)$ при любом подмножестве $D \subseteq \{0,\dots,n-1\}$ порядка не менее 2. Воспользуемся данным описанием для исследования перемешивающих свойств регистровых преобразований $\varphi^{g,\mu}$ из МАГ$(n,r,2)$.

Опишем множество дуг перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$. Обозначим при $u = 0,\dots,r-1$: $\varphi^{g,\mu}_{u+rk}(\overline{X}_0,\dots,\overline{X}_{n-1})$ — координатная булева функция преобразования $\varphi^{g,\mu}$, $k = 0,\dots,n-1$; $g_u(y_0,\dots,y_{r-1})$ и $\mu_u(y_0,\dots,y_{r-1})$ — координатные булевы функции преобразований g и μ соответственно.

Из (6) следует, что при $u = 0,\dots,r-1$ и любом $k \in \{0,\dots,n-2\}\setminus\{m\}$ существенные переменные координатных функций $\varphi^{g,\mu}_{u+rk}$ описываются просто:

$$E(\varphi^{g,\mu}_{u+rk}) = \{u + r(k+1)\}. \tag{10}$$

То есть задача состоит в описании существенных переменных функций при $k = n-1$ и $k = m$. Из (6) следует также, что в орграфе $\Gamma(\varphi^{g,\mu})$ имеется контур $c_u = (u + r(n-1), u + r(n-2),\dots,u)$, если и только если в $\Gamma(\varphi^{g,\mu})$ имеются дуги $(u + r(m+1), u + rm)$ и $(u, u + r(n-1))$, $u = 0,\dots,r-1$. Из (8), (9) следует:

$$\varphi^{g,\mu}_{u+r(n-1)}(\overline{X}_0,\dots,\overline{X}_{n-1}) = g_u\left(b_r\left(\left(\sum_{k\in D} X_k\right) \bmod 2^r\right)\right),$$
$$\varphi^{g,\mu}_{u+rm}(\overline{X}_0,\dots,\overline{X}_{n-1}) = \mu_u\left(b_r\left(\left(\sum_{k\in \Delta} X_k\right) \bmod 2^r\right)\right).$$

Обозначим $\xi(u)$ — наименьший номер существенной переменной функции $g_u(y_0,\dots,y_{r-1})$, $0 \leqslant \xi(u) < r$; $\eta(u)$ — наименьший номер существенной переменной функции $\mu_u(y_0,\dots,y_{r-1})$, $0 \leqslant \eta(u) < r$.

Из [4, теорема 2] следует описание множеств существенных переменных функций $\varphi^{g,\mu}_{u+r(n-1)}$ и $\varphi^{g,\mu}_{u+rm}$, $u = 0,\dots,r-1$.

Теорема 3. Переменная x_{v+rk} существенная:

а) для $\varphi^{g,\mu}_{u+r(n-1)}$, если и только если $k \in D$ и $\xi(u) \leqslant v < r$;

б) для $\varphi^{g,\mu}_{u+rm}$, если и только если $k \in \Delta$ и $\eta(u) \leqslant v < r$.

Данное описание множества дуг перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ позволяет исследовать условия его примитивности. Необходимым условием примитивности орграфа является сильная связность. Получим достаточное условие сильной связности орграфа $\Gamma(\varphi^{g,\mu})$.

Из (10) и теоремы 3 следует, что в орграфе $\Gamma(\varphi^{g,\mu})$ имеются пути следующих видов:

1) $w_v^{(n-1,m+1)} = w(v + r(n-1), v + r(n-2),\dots,v + r(m+1))$ и $w_v^{(m,0)} = w(v + rm, v + r(m-1),\dots,v)$ при $0 \leqslant v < \max\{\xi(u),\eta(u)\}$;
2) $w_v^{(m,m+1)} = w_v^{(m,0)} \cdot (v, v + r(n-1)) \cdot w_v^{(n-1,m+1)}$ при $v \geqslant \xi(u)$;
3) $w_v = w_v^{(n-1,m+1)} \cdot (m+1, m) \cdot w_v^{(m,0)} = w(v + r(n-1), v + r(n-2),\dots,v)$ при $v \geqslant \eta(u)$.

При $\max\{\xi(u),\eta(u)\} \leqslant v < r$ в $\Gamma(\varphi^{g,\mu})$ имеются простые контуры

$$c_v = (v + r(n-1), v + r(n-2),\dots,v).$$

Обозначим: $\Gamma(g)$ и $\Gamma(\mu)$ — перемешивающие орграфы преобразований g и μ соответственно; $V(v)$ — множество вершин $\{v + r(n-1), v + r(n-2), \ldots, v\}$ в $\Gamma(\varphi^{g,\mu})$, $v = 0, \ldots, r-1$.

Теорема 4. Орграф $\Gamma(\varphi^{g,\mu})$ сильносвязный, если в каждом из орграфов $\Gamma(g)$ и $\Gamma(\mu)$ имеется дуга $(0, r-1)$ и полустепень захода каждой вершины орграфов $\Gamma(g)$ и $\Gamma(\mu)$ больше нуля.

Доказательство. Наличие в каждом из орграфов $\Gamma(g)$ и $\Gamma(\mu)$ дуги $(0, r-1)$ равносильно тому, что переменная y_0 существенная для координатных функций $g_{r-1}(y_0, \ldots, y_{r-1})$ и $\mu_{r-1}(y_0, \ldots, y_{r-1})$. В силу теоремы 3 это равносильно тому, что переменная x_{j+rk} является существенной для функции $\varphi^{g,\mu}_{u+r(n-1)}$ при любом $k \in D$, $j = 0, \ldots, r-1$, и для функции $\varphi^{g,\mu}_{u+rm}$ при любом $k \in \Delta$, $j = 0, \ldots, r-1$. Следовательно, с использованием пути w_{r-1} и контура c_{r-1} любая вершина из $V(r-1)$ достижима из любой вершины множества $\bigcup\limits_{j=0}^{r-1} V(j)$, то есть из любой вершины орграфа $\Gamma(\varphi^{g,\mu})$.

Вместе с тем по условию в любую вершину j каждого из орграфов $\Gamma(g)$ и $\Gamma(\mu)$ заходит дуга, значит, по теореме 3 и с использованием путей вида $w_v^{(n-1,m+1)}$ и $w_v^{(m,0)}$ любая вершина орграфа $\Gamma(\varphi^{g,\mu})$ достижима из множества $V(r-1)$. Значит, орграф $\Gamma(\varphi^{g,\mu})$ сильносвязный. ■

В частности, условиям теоремы 4 удовлетворяют следующие модифицирующие преобразования:

— сдвиг $R(y_0, \ldots, y_{r-1}) = (y_1, y_2, \ldots, y_{r-1}, y_0)$ координат векторов из V_r;
— инволютивная перестановка $I(y_0, \ldots, y_{r-1}) = (y_{r-1}, \ldots, y_0)$ координат векторов из V_r;
— треугольная подстановка T множества V_r с координатными функциями $t_i(y_0, \ldots, y_{r-1}) = y_0 \oplus \ldots \oplus y_i$, $i = 0, \ldots, r-1$;
— совершенные преобразования (s-боксы множества V_r, в которых каждая координатная функция существенно зависит от всех входных переменных).

Докажем критерий примитивности орграфа $\Gamma(\varphi^{g,\mu})$. Напомним [5], что множество контуров $C = \{C_1, \ldots, C_s\}$ длин $l_1, \ldots, l_s$ соответственно называется примитивным, если числа $l_1, \ldots, l_s$ взаимно простые.

Обозначим: $d^{(\zeta)}$ — наибольшее число из D, не превышающее ζ, где $\zeta = 0, \ldots, n-1$; $\delta^{(\zeta)}$ — наибольшее число из Δ, не превышающее ζ, в случае $\delta_1 \leqslant \zeta$, где $\zeta = 1, \ldots, n-1$ в силу свойства $0 \in D \setminus \Delta$. Отсюда $d^{(n-1)} = d_q$, $\delta^{(n-1)} = \max\{\delta_0, \delta_p\}$. Пусть $d^{(m)} = d_t$, где $t \in \{0, \ldots, q\}$, и $\delta^{(m)} = \delta_\tau$ при $\delta_1 \leqslant m$, где $\tau \in \{0, \ldots, p\}$.

Определим множества чисел L (при $\delta_1 \leqslant m$) и L' (при $\delta_1 > m$):

$$L = \{n - d_i, n + m + 1 - d_j - \delta_k, m + 1 - \delta_l : i = 0, \ldots, q,\ j = 0, \ldots, t,$$
$$k = \tau + 1, \ldots, p,\ l = 1, \ldots, \tau\},$$
$$L' = \{n - d_i, n + m + 1 - d_j - \delta_k : i = 0, \ldots, q,\ j = 0, \ldots, t,\ k = 1, \ldots, p\}.$$

Теорема 5 (критерий примитивности орграфа $\Gamma(\varphi^{g,\mu})$). Сильносвязный орграф $\Gamma(\varphi^{g,\mu})$ примитивный, если и только если либо $\delta_1 \leqslant m$ и L — множество взаимно простых чисел, либо $\delta_1 > m$ и L' — множество взаимно простых чисел.

Доказательство. Напомним, что в соответствии с универсальным критерием примитивности [6, ч. 1, разд. 11.3] сильносвязный орграф примитивный, если и только если он содержит примитивную систему простых контуров (иначе говоря, длины всех простых контуров образуют множество взаимно простых чисел).

Обозначим: $B_i = \{v + ri : v = 0, \ldots, r-1\}$ — множество вершин, $i = 0, \ldots, n-1$; $C^{(v)}$ — множество простых контуров сильносвязного орграфа $\Gamma(\varphi^{g,\mu})$, все вершины которых принадлежат множеству $V(v)$ вершин контура c_v, где $v \in \{0, \ldots, r-1\}$. В соответствии с теоремой 3 $C^{(v)} \neq \varnothing$, если $\max\{\xi(u), \eta(u)\} \leqslant v < r$ (в частности, $C^{(v)} \neq \varnothing$, если отлична от константы каждая координатная функция преобразований g и μ).

Из (6) следует, что каждый контур орграфа $\Gamma(\varphi^{g,\mu})$ проходит хотя бы через одну из вершин множества $B_{n-1} \cup B_m$. В частности, каждый контур из $C^{(v)}$ проходит хотя бы через одну из двух вершин $v + r(n-1)$ и $v + rm$. Из (8) и (9) следует, что $C^{(v)}$ есть объединение трёх множеств:

$$C^{(v)} = \{c_v^D(d) : d \in D\} \cup \{c_v^{\Delta,D}(\delta, d) : d \in D, \delta \in \Delta, d \leqslant m < \delta\} \cup \{c_v^{\Delta}(\delta) : \delta \in \Delta, \delta \leqslant m\},$$

где

$$\begin{gathered} c_v^D(d) = w(v + r(n-1), v + r(n-2), \ldots, v + rd) \cdot (v + rd, v + r(n-1)), \\ c_v^{\Delta}(\delta) = w(v + rm, v + r(m-1), \ldots, v + r\delta) \cdot (v + r\delta, v + rm), \\ c_v^{\Delta,D}(\delta, d) = w(v + r(n-1), v + r(n-2), \ldots, v + r\delta) \cdot (v + r\delta, v + rm) \cdot \\ \cdot w(v + rm, v + r(m-1), \ldots, v + rd) \cdot (v + rd, v + r(n-1)). \end{gathered}$$

Длины этих контуров равны

$$\operatorname{len} c_v^D(d) = n - d, \ \operatorname{len} c_v^{\Delta}(\delta) = m + 1 - \delta, \ \operatorname{len} c_v^{\Delta,D}(\delta, d) = n + m + 1 - \delta - d.$$

Следовательно, множество длин контуров из $C^{(v)}$ совпадает при $\delta_1 \leqslant m$ с множеством L и при $\delta_1 > m$ — с множеством L'. Тогда в соответствии с универсальным критерием примитивности взаимная простота либо множества L при $\delta_1 \leqslant m$, либо множества L' при $\delta_1 > m$ достаточна для примитивности сильносвязного орграфа $\Gamma(\varphi^{g,\mu})$.

Докажем необходимость. Пусть $d, d' \in D$; $\delta, \delta' \in \Delta$.

С л у ч а й 1. $\delta_1 \leqslant m$.

В $\Gamma(\varphi^{g,\mu})$ при $v, u \in \{0, \ldots, r-1\}$ элементарным путём назовём любой путь вида

$$w_{v,u}^{(n-1,n-1)}(d) = w(v + r(n-1), \ldots, v + rd) \cdot (v + rd, u + r(n-1)), \ m + 1 \leqslant d < n; \quad (11)$$

$$w_{v,u}^{(m,m)}(\delta) = w(v + rm, \ldots, v + r\delta) \cdot (v + r\delta, u + rm), \ 0 \leqslant \delta \leqslant m; \quad (12)$$

$$w_{v,u}^{(n-1,m)}(\delta) = w(v + r(n-1), \ldots, v + r\delta) \cdot (v + r\delta, u + rm), \ m + 1 \leqslant \delta < n; \quad (13)$$

$$w_{v,u}^{(m,n-1)}(d) = w(v + rm, \ldots, v + rd) \cdot (v + rd, u + r(n-1)), \ 0 \leqslant d \leqslant m. \quad (14)$$

Элементарные пути $w_{v,u}^{(n-1,n-1)}(d)$, $w_{v,u}^{(m,m)}(\delta)$, $w_{v,u}^{(n-1,m)}(\delta)$ и $w_{v,u}^{(m,n-1)}(d)$ изображены светлым цветом на рис. 3 и 4. Заметим, что при $v = u$ элементарные пути вида (11) и (12) являются контурами.

Каждый контур орграфа $\Gamma(\varphi^{g,\mu})$ проходит через некоторую вершину множества $B_{n-1} \cup B_m$, поэтому он однозначно представляется конкатенацией элементарных путей при фиксированной начальной вершине из множества $B_{n-1} \cup B_m$. Рангом контура в орграфе $\Gamma(\varphi^{g,\mu})$ назовём число составляющих его элементарных путей.

Докажем с помощью индукции по рангу контура промежуточное утверждение: длина любого контура орграфа $\Gamma(\varphi^{g,\mu})$ содержится в полугруппе $\langle L \rangle$.

Если утверждение верно и орграф $\Gamma(\varphi^{g,\mu})$ примитивный, то числа множества L взаимно простые, иначе у длин всех контуров орграфа $\Gamma(\varphi^{g,\mu})$ имеется общий делитель.

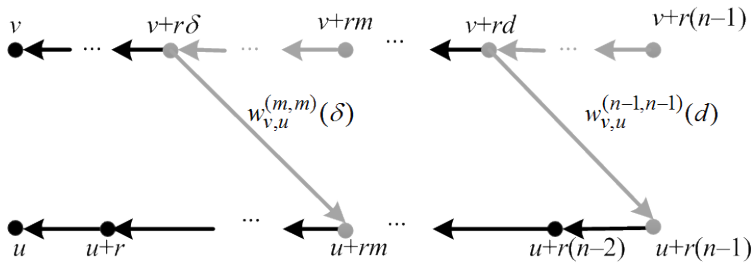

Рис. 3. Элементарные пути $w_{v,u}^{(n-1,n-1)}(d)$ и $w_{v,u}^{(m,m)}(\delta)$

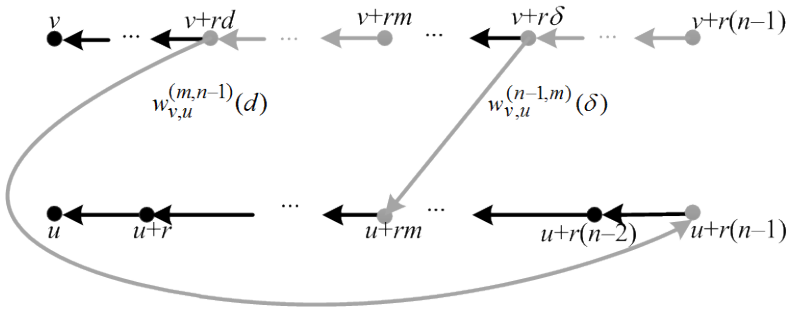

Рис. 4. Элементарные пути $w_{v,u}^{(n-1,m)}(\delta)$ и $w_{v,u}^{(m,n-1)}(d)$

В соответствии с теоремой 3 любой контур ранга 1 имеет при $v = u$ вид (11), где $\xi(u) \leqslant v < r$, или вид (12), где $\eta(u) \leqslant v < r$. Длина его равна соответственно $n - d$ и $m + 1 - \delta$. Следовательно, для простых контуров ранга 1 утверждение верно.

Любой контур ранга 2 есть конкатенация двух элементарных путей и при $v, u \in \{0, \ldots, r-1\}$ имеет вид либо $w_{v,u}^{(n-1,n-1)}(d) \cdot w_{u,v}^{(n-1,n-1)}(d')$, если $m + 1 \leqslant d < n$ и $m + 1 \leqslant d' < n$, либо $w_{v,u}^{(m,m)}(\delta) \cdot w_{u,v}^{(m,m)}(\delta')$, если $0 \leqslant \delta \leqslant m$ и $0 \leqslant \delta' \leqslant m$, либо $w_{v,u}^{(n-1,m)}(\delta) \cdot w_{u,v}^{(m,n-1)}(d)$ или $w_{v,u}^{(m,n-1)}(d) \cdot w_{u,v}^{(n-1,m)}(\delta)$, если $0 \leqslant d \leqslant m$ и $m + 1 \leqslant \delta < n$. Длины таких контуров равны $n - d + n - d'$, $m + 1 - \delta + m + 1 - \delta'$ и $n + m + 1 - d - \delta$ соответственно. Следовательно, для контуров ранга 2 утверждение также верно.

Пусть утверждение верно для всех контуров рангов $k-1$ и $k-2$, где $k > 2$. Докажем, что утверждение верно для любого контура ранга k.

Любой контур ранга k является конкатенацией k элементарных путей и при $v, u, z \in \{0, \ldots, r-1\}$ имеет одно из следующих строений:

$$w_1 \cdot w_{u,v}^{(n-1,n-1)}(d), \text{ если } m + 1 \leqslant d < n;$$
$$w_2 \cdot w_{u,v}^{(m,m)}(\delta), \text{ если } 0 \leqslant \delta \leqslant m;$$
$$w_3 \cdot w_{z,u}^{(n-1,m)}(\delta) \cdot w_{u,v}^{(m,n-1)}(d),$$
$$w_4 \cdot w_{z,u}^{(m,n-1)}(d) \cdot w_{u,v}^{(n-1,m)}(\delta), \text{ если } 0 \leqslant d \leqslant m \text{ и } m + 1 \leqslant \delta < n,$$

где $w_1 = w[v+r(n-1), u+r(n-1)]$, $w_2 = w[v+rm, u+rm]$, $w_3 = w[v+r(n-1), z+r(n-1)]$, $w_4 = w[v + rm, z + rm]$ — пути в $\Gamma(\varphi^{g,\mu})$. В соответствии с равенствами (11)–(14)

$$\operatorname{len} w_{u,v}^{(n-1,n-1)}(d) = n - d, \quad \operatorname{len} w_{u,v}^{(m,m)}(\delta) = m + 1 - \delta,$$
$$\operatorname{len}(w_{z,u}^{(n-1,m)}(\delta) \cdot w_{u,v}^{(m,n-1)}(d)) = \operatorname{len}(w_{z,u}^{(m,n-1)}(d) \cdot w_{u,v}^{(n-1,m)}(\delta)) = n + m + 1 - d - \delta.$$

Следовательно, осталось показать, что длины путей w_1, w_2, w_3 и w_4 содержатся в $\langle L\rangle$. Длины путей w_1 и w_2 совпадают с длинами контуров ранга $k-1$, полученными из этих путей заменой последних дуг. Длины путей w_3 и w_4 совпадают с длинами контуров ранга $k-2$, полученными из этих путей заменой последних дуг. По предположению индукции длины контуров рангов $k-1$ и $k-2$ содержатся в $\langle L\rangle$, значит, длины путей w_1, w_2, w_3 и w_4 также содержатся в $\langle L\rangle$. Следовательно, длина любого контура ранга k содержится в $\langle L\rangle$.

С л у ч а й 2. $\delta_1 > m$.

В этом случае в $\Gamma(\varphi^{g,\mu})$ имеются элементарные пути трёх видов $w_{v,u}^{(n-1,n-1)}(d)$, $w_{v,u}^{(n-1,m)(\delta)}$ и $w_{v,u}^{(m,n-1)}(d)$, которые определены равенствами (11), (13) и (14) соответственно.

С помощью индукции по рангу контура докажем промежуточное утверждение: длина любого контура орграфа $\Gamma(\varphi^{g,\mu})$ содержится в полугруппе $\langle L'\rangle$. В этом случае из примитивности орграфа $\Gamma(\varphi^{g,\mu})$ следует взаимная простота чисел множества L'.

В соответствии с теоремой 3 любой контур ранга 1 имеет вид (11) при $v = u$, где $\xi(u) \leqslant v < r$. Длина его равна $n - d$. Следовательно, для простых контуров ранга 1 утверждение верно.

Любой контур ранга 2 есть конкатенация двух элементарных путей и при $v, u \in \{0, \ldots, r-1\}$ имеет вид либо $w_{v,u}^{(n-1,n-1)}(d) \cdot w_{u,v}^{(n-1,n-1)}(d')$, если $m+1 \leqslant d < n$ и $m+1 \leqslant d' < n$, либо $w_{v,u}^{(n-1,m)}(\delta) \cdot w_{u,v}^{(m,n-1)}(d)$ или $w_{v,u}^{(m,n-1)}(d) \cdot w_{u,v}^{(n-1,m)}(\delta)$, если $0 \leqslant d \leqslant m$ и $m+1 \leqslant \delta < n$. Длины таких контуров равны $n-d+n-d'$ и $n+m+1-d-\delta$ соответственно. Отсюда утверждение верно для контуров ранга 2.

Пусть утверждение верно для всех контуров рангов $k-1$ и $k-2$, где $k > 2$. Докажем, что утверждение верно для любого контура ранга k. Любой контур ранга k является конкатенацией k элементарных путей и при $v, u, z \in \{0, \ldots, r-1\}$ имеет одно из следующих строений:

$$w_1 \cdot w_{u,v}^{(n-1,n-1)}(d), \text{ если } m+1 \leqslant d < n;$$
$$w_2 \cdot w_{z,u}^{(n-1,m)}(\delta) \cdot w_{u,v}^{(m,n-1)}(d),$$
$$w_3 \cdot w_{z,u}^{(m,n-1)}(d) \cdot w_{u,v}^{(n-1,m)}(\delta), \text{ если } 0 \leqslant d \leqslant m \text{ и } m+1 \leqslant \delta < n,$$

где $w_1 = w[v+r(n-1), u+r(n-1)]$, $w_2 = w[v+r(n-1), z+r(n-1)]$, $w_3 = w[v+rm, z+rm]$ — пути в $\Gamma(\varphi^{g,\mu})$. В соответствии с равенствами (11), (13), (14)

$$\operatorname{len} w_{u,v}^{(n-1,n-1)}(d) = n-d,$$
$$\operatorname{len}(w_{z,u}^{(n-1,m)}(\delta) \cdot w_{u,v}^{(m,n-1)}(d)) = \operatorname{len}(w_{z,u}^{(m,n-1)}(d) \cdot w_{u,v}^{(n-1,m)}(\delta)) = n+m+1-d-\delta.$$

Следовательно, осталось показать, что длины путей w_1, w_2 и w_3 содержатся в $\langle L'\rangle$. Длина пути w_1 равна длине контура ранга $k-1$, полученного из w_1 заменой последней дуги. Длины путей w_2 и w_3 равны длинам контуров ранга $k-2$, полученным из этих путей заменой последних дуг. По предположению индукции длины контуров рангов $k-1$ и $k-2$ содержатся в $\langle L'\rangle$, следовательно, длины путей w_1, w_2 и w_3 также содержатся в $\langle L'\rangle$. Следовательно, длина любого контура ранга k содержится в $\langle L'\rangle$. Теорема доказана. ■

Получим оценки экспонента орграфа $\Gamma(\varphi^{g,\mu})$. Обозначим:

— $\rho(D) = \max\{n-d_q, d_q-d_{q-1}, \ldots, d_1-d_0\}$ при $d_q > m$;
— $\rho(\Delta, D) = \max\{\max\{n-\delta_p, \delta_p-\delta_{p-1}, \ldots, \delta_{\tau+2}-\delta_0\}+m-d_q+1, \max\{m-d_q+1, d_q-d_{q-1}, \ldots, d_1-d_0\}\}$ при $d_q \leqslant m$;

— $\rho(\Delta) = \max\{\delta_1 + n - \delta_p, \delta_p - \delta_{p-1}, \ldots, \delta_0 - \delta_\tau, \ldots, \delta_2 - \delta_1\}$ при $\delta_1 \leqslant m$;
— $\rho'(\Delta, D) = \max\{\max\{n - \delta_p, \delta_p - \delta_{p-1}, \ldots, \delta_1 - \delta_0\}, \max\{m - d_t + 1, d_t - d_{t-1}, \ldots, d_1 - d_0\} + n - \delta_p\}$ при $\delta_1 > m$;
— $\varepsilon = \max\{2n - m - 2 - d_q, n + m - \max\{\delta_0, \delta_p\}\}$;
— $\varepsilon' = \max\{2m + 1 - \delta_\tau, n - 1 - d_t\}$.

Лемма 1. Пусть $0 \leqslant v < r$, $0 \leqslant u < r$, $i, j \in \{0, \ldots, n-1\}$. Тогда в орграфе $\Gamma(\phi^{g,\mu})$ длины кратчайших путей:

а) из вершины $v + ri$ в вершину $nr - 1$ — не превышает $\rho(D)$ при $d_q > m$; $\rho(\Delta, D)$ при $d_q < m$;
б) из вершины $v + ri$ в вершину $r - 1 + rm$ — не превышает $\rho(\Delta)$ при $\delta_1 \leqslant m$; $\rho'(\Delta, D)$ при $d_q < m$;
в) из вершины $nr - 1$ в вершину $u + rj$ — не превышает ε;
г) из вершины $r - 1 + rm$ в вершину $u + rj$ — не превышает ε'.

Доказательство.

а) При $d_q > m$ и любом v кратчайший путь $w[v + ri, nr - 1]$ имеет строение

$$w[v + ri, nr - 1] = w(v + ri, v + r(i-1), \ldots, v + rd^{(i)}) \cdot (v + rd^{(i)}, nr - 1),$$

его длина равна $i - d^{(i)} + 1$. Отсюда $\operatorname{len}[v + ri, nr - 1] \leqslant \rho(D)$. При $d_q \leqslant m$ кратчайший путь $w[v + ri, nr - 1]$ имеет одно из двух строений:

$$w(v + ri, v + r(i-1), \ldots, v + r\delta^{(i)}) \cdot (v + r\delta^{(i)}, r - 1 + rm) \cdot w^{(m,n-1)}_{r-1,r-1}(d^{(m)}) \text{ при } m < i \leqslant n - 1,$$
$$w(v + ri, v + r(i-1), \ldots, v + rd^{(i)}) \cdot (v + rd^{(i)}, nr - 1) \text{ при } 0 \leqslant i \leqslant m,$$

где элементарный путь $w^{(m,n-1)}_{r-1,r-1}(d^{(m)})$ определён равенством (14). Длина пути $w[v + ri, nr - 1]$ равна $i - \delta^{(i)} + 1 + m - d^m$ в первом случае и $i - d^{(i)} + 1$ во втором. С учётом равенства $d^{(m)} = d_t = d_q$ получаем

$$\max_{i \in \{0,\ldots,n-1\}} \operatorname{len} w[v + ri, nr - 1] \leqslant \rho(\Delta, D).$$

б) При $\delta_1 \leqslant m$ кратчайший путь $w[v + ri, r - 1 + rm]$ имеет строение

$$w[v + ri, r - 1 + rm] = w(v + ri, v + r(i-1), \ldots, v + r\delta^{(i)}) \cdot (v + r\delta^{(i)}, r - 1 + rm),$$

его длина равна $i - \delta^{(i)} + 1$. Отсюда

$$\max_{i \in \{0,\ldots,n-1\}} \operatorname{len} w[v + ri, r - 1 + rm] \leqslant \rho(\Delta).$$

При $\delta_1 > m$ кратчайший путь $w[v + ri, r - 1 + rm]$ имеет одно из двух строений:

$$w(v + ri, v + r(i-1), \ldots, v + r\delta^{(i)}) \cdot (v + r\delta^{(i)}, r - 1 + rm) \text{ при } m < i \leqslant n - 1,$$
$$w(v + ri, v + r(i-1), \ldots, v + rd^{(i)}) \cdot (v + rd^{(i)}, nr - 1) \cdot w^{(n-1,m)}_{r-1,r-1}(\delta^{(n-1)}) \text{ при } 0 \leqslant i \leqslant m,$$

где элементарный путь $w^{(n-1,m)}_{r-1,r-1}(\delta^{(n-1)})$ определён равенством (13). Длина пути $w[v + ri, r - 1 + rm]$ в первом случае равна $i - \delta^{(i)} + 1$ и во втором случае равна $i - d^{(i)} + 1 + n - \delta^{(n-1)}$. С учётом равенства $\delta^{(n-1)} = d_p$ получаем

$$\max_{i \in \{0,\ldots,n-1\}} \operatorname{len} w[v + ri, r - 1 + rm] \leqslant \rho'(\Delta, D).$$

в) Кратчайший путь $w[nr-1, u+rj]$ имеет одно из двух строений:

$$w[nr-1,u+rj] = w_{r-1,u}^{(n-1,n-1)}(d^{(n-1)}) \cdot w(u+r(n-1), u+r(n-2), \ldots, u+rj)$$
$$\text{при } m < j \leqslant n-1,$$
$$w[nr-1,u+rj] = w_{r-1,u}^{(n-1,m)}(\delta^{(n-1)}) \cdot w(u+rm, u+r(m-1), \ldots, u+rj) \text{ при } 0 \leqslant j \leqslant m,$$

где элементарные пути $w_{r-1,u}^{(n-1,n-1)}(d^{(n-1)})$ и $w_{r-1,u}^{(n-1,m)}(\delta^{(n-1)})$ определены равенствами (11) и (13) соответственно. Длина пути $w[nr-1, u+rj]$ равна $2n-1-d^{(n-1)}-j$ при $m < j \leqslant n-1$ и $n+m-\delta^{(n-1)}-j$ при $0 \leqslant j \leqslant m$. С учётом равенств $d^{(n-1)} = d_q$ и $\delta^{(n-1)} = \max\{\delta_0, \delta_p\}$ получаем

$$\max_{j\in\{0,\ldots n-1\}} \operatorname{len} w[nr-1, u+rj] \leqslant \varepsilon.$$

г) Кратчайший путь $w[r-1+rm, u+rj]$ имеет одно из двух строений:

$$w_{r-1,u}^{(m,m)}(\delta^{(m)}) \cdot w(u+rm, u+r(m-1), \ldots, u+rj) \text{ при } 0 \leqslant j \leqslant m,$$
$$w_{r-1,u}^{(m,n-1)}(d^{(m)}) w(u+r(n-1), u+r(n-2), \ldots, u+rj) \text{ при } m < j \leqslant n-1,$$

где элементарные пути $w_{r-1,u}^{(m,m)}(\delta^{(m)})$ и $w_{r-1,u}^{(m,n-1)}(d^{(m)})$ определены равенствами (12) и (14) соответственно. Длина пути $w[r-1+rm, u+rj]$ равна $2m+1-\delta^{(m)}-j$ при $0 \leqslant j \leqslant m$ и $n+m-d^{(m)}-j$ при $m < j \leqslant n-1$. С учётом равенств $\delta^{(m)} = \delta_\tau$ и $d^{(m)} = d_t$ получаем оценку

$$\max_{i\in\{0,\ldots,n-1\}} \operatorname{len} w[r-1+rm, u+rj] \leqslant \varepsilon'.$$

Лемма доказана. ■

Для оценки экспонента орграфа $\Gamma(\varphi^{g,\mu})$ используются числа Фробениуса. Числом Фробениуса $\Phi(\Lambda)$ называется наибольшее число, не принадлежащее аддитивной полугруппе $\langle\Lambda\rangle$, где Λ — множество взаимно простых чисел; $\Phi(\{1\}) = \Phi(\{1, l_2, \ldots, l_s\}) = -1$ при любых $l_2, \ldots, l_s$. Известно, что при $s = 2$ выполнено равенство $\Phi(\{l_1, l_2\}) = l_1 l_2 - l_1 - l_2$.

Теорема 6. Пусть $C = \{C_1, \ldots, C_s\}$ — примитивное множество контуров в орграфе $\Gamma(\varphi^{g,\mu})$ с множеством длин $\Lambda = \{l_1, \ldots, l_s\}$, где $s \geqslant 1$ и все вершины контуров $C_1, \ldots, C_s$ принадлежат множеству $V(r-1)$. Тогда:

а) если контуры $C_1, \ldots, C_s$ проходят через вершину $nr-1$, то

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \rho(d_q) + \varepsilon, \tag{15}$$

где $\rho(d_q) = \rho(D)$ при $d_q > m$ и $\rho(d_q) = \rho(\Delta, D)$ при $d_q \leqslant m$;

б) если контуры $C_1, \ldots, C_s$ не проходят через вершину $nr-1$, то

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \rho(\Delta) + \varepsilon'; \tag{16}$$

в) если контуры $C_1, \ldots, C_h$ проходят через вершину $nr-1$, $1 \leqslant h < s$, а контуры $C_{h+1}, \ldots, C_s$ проходят через вершину $r-1+rm$ и не проходят через вершину $nr-1$, то

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \rho(d_q) + n - \max\{\delta_0, \delta_p\} + \varepsilon'. \tag{17}$$

Доказательство. Для получения оценок экспонента примитивного орграфа $\Gamma(\varphi^{g,\mu})$ используем утверждение $3, б$ из [7, с. 103]: если в сильносвязном орграфе Γ при некотором $l \in \mathbb{N}$ имеется путь длины l из любой вершины в любую, то орграф Γ примитивный и $\exp\Gamma \leqslant l$.

Возьмём в $\Gamma(\varphi^{g,\mu})$ любые вершины $v+ri$ и $u+rj$, $0 \leqslant v < r$, $0 \leqslant u < r$, $i, j \in \in \{0, \ldots, n-1\}$, и оценим длину пути $w[v+ri, u+rj]$, используя подход, изложенный в [5] для получения универсальной оценки экспонента. Для этого рассмотрим следующие случаи.

а) Пусть контуры $C_1, \ldots, C_s$ проходят через вершину $nr-1$. Путь $w[v+ri, u+rj]$ представляется конкатенацией путей

$$w[v+ri, u+rj] = w[v+ri, nr-1] \cdot t_1 C_1(nr-1) \cdot \ldots \cdot t_s C_s(nr-1) \cdot w[nr-1, u+rj],$$

где $t_1, \ldots, t_s$ — целые неотрицательные коэффициенты, равные кратностям обхода контуров $C_1, \ldots, C_s$ соответственно. Варьируя кратности $t_1, \ldots, t_s$, можно (в соответствии с определением числа Фробениуса) построить путь $w[v+ri, u+rj]$ длины t при любом $t > \Phi(\Lambda) + \operatorname{len} w[v+ri, nr-1] + \operatorname{len} w[nr-1, u+rj]$. Отсюда

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \max_{i\in\{0,\ldots,n-1\}} \operatorname{len} w[v+ri, nr-1] + \max_{j\in\{0,\ldots,n-1\}} \operatorname{len}[nr-1, u+rj].$$

В соответствии с леммой 1 (случаи *а* и *в*) получаем оценку

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \rho(d_q) + \varepsilon,$$

где $\rho(d_q) = \rho(D)$ при $d_q > m$ и $\rho(d_q) = \rho(\Delta, D)$ при $d_q \leqslant m$.

б) Пусть контуры $C_1, \ldots, C_s$ не проходят через вершину $nr-1$, то есть $\delta_1 \leqslant m$. Путь $w[v+ri, u+rj]$ представляется конкатенацией путей

$$w[v+ri, u+rj] = w[v+ri, r-1+rm] \cdot t_1 C_1(r-1+rm) \cdot \ldots \cdot t_s C_s(r-1+rm) \cdot w[r-1+rm, u+rj],$$

где $t_1, \ldots, t_s$ — целые неотрицательные коэффициенты, равные кратностям обхода контуров $C_1, \ldots, C_s$ соответственно. Варьируя кратности $t_1, \ldots, t_s$, можно (в соответствии с определением числа Фробениуса) построить путь $w[v+ri, u+rj]$ длины t при любом $t > \Phi(\Lambda) + \operatorname{len} w[v+ri, r-1+rm] + \operatorname{len} w[r-1+rm, u+rj]$. Отсюда

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \max_{i\in\{0,\ldots,n-1\}} \operatorname{len} w[v+ri, r-1+rm] + \max_{j\in\{0,\ldots,n-1\}} \operatorname{len}[r-1+rm, u+rj].$$

В соответствии с леммой 1 (случаи *б* и *г*) получаем оценку

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \rho(\Delta) + \varepsilon'.$$

в) Пусть $C_1, \ldots, C_h$ — контуры, проходящие через вершину $nr-1$, а $C_{h+1}, \ldots, C_s$ — контуры, проходящие через вершину $r-1+rm$ и не проходящие через вершину $nr-1$. Путь $w[v+ri, u+rj]$ представляется конкатенацией путей

$$\begin{gathered} w[v+ri, u+rj] = w[v+ri, nr-1] \cdot t_1 C_1(nr-1) \cdot \ldots \cdot t_h C_h(nr-1) \cdot \\ \cdot w(r-1+n(r-1), r-1+n(r-2), \ldots, r-1+rm) \cdot t_{h+1} C_{h+1}(r-1+rm) \cdot \ldots \\ \ldots \cdot t_s C_s(r-1+rm) \cdot w[r-1+rm, u+rj], \end{gathered}$$

где $t_1, \ldots, t_s$ — целые неотрицательные коэффициенты, определяющие кратности обхода контуров $C_1, \ldots, C_s$ соответственно. Варьируя кратности $t_1, \ldots, t_s$, можно (в соответствии с определением числа Фробениуса) построить путь $w[v + ri, u + rj]$ длины t при любом $t > \Phi(\Lambda) + \operatorname{len} w[v+ri, nr-1] + \operatorname{len} w[nr-1, r-1+rm] + \operatorname{len} w[r-1+rm, u+rj]$. Отсюда

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \max_{i\in\{0,\ldots,n-1\}} \operatorname{len} w[v + ri, nr - 1] + n - \max\{\delta_0, \delta_p\} + \\ + \max_{j\in\{0,\ldots,n-1\}} \operatorname{len}[r - 1 + rm, u + rj].$$

В соответствии с леммой 1 (случаи *а* и *г*) получаем оценку

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda) + 1 + \rho(d_q) + n - \max\{\delta_0, \delta_p\} + \varepsilon'.$$

Теорема доказана. ■

Из теоремы 6 следует, что оценка $\exp\Gamma(\varphi^{g,\mu})$ зависит от выбора параметров, в частности от значения параметра m второй обратной связи и точек съёма: $d^{(n-1)} = d_q$ и $d^{(m)} = d_t$ из множества D, $\delta^{(m)} = \delta_\tau$ и $\delta^{(n-1)} = \max\{\delta_0, \delta_p\}$ из множества Δ. Известно, что оценка экспонента понижается при наличии петель в примитивном орграфе. Уточним оценку $\exp\Gamma(\varphi^{g,\mu})$ для случая, когда $(n-1) \in D$, $m \in \Delta$.

Следствие 1. Если выполнено условие $(n-1) \in D$, $m \in \Delta$, то сильносвязный орграф $\Gamma(\varphi^{g,\mu})$ является примитивным и справедлива оценка

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \min\{\rho(D) + \varepsilon, \rho(\Delta) + \varepsilon'\}. \tag{18}$$

Доказательство. Если $(n-1) \in D$, $m \in \Delta$, то в орграфе $\Gamma(\varphi^{g,\mu})$ есть петли в вершинах $nr - 1$ и $r - 1 + rm$, следовательно, $\Gamma(\varphi^{g,\mu})$ примитивен и $\Phi(\Lambda) = -1$. Так как $d_q = n - 1$, $\delta_\tau = m$, то выполняются условия $d_q > m$, $\delta_1 \leqslant m$, следовательно, $\rho(d_q) = \rho(D)$. Из случаев *а* и *б* теоремы 6 получаем оценку следствия. ■

В [4, теорема 5] получены оценки экспонента перемешивающего орграфа $\Gamma(\varphi^g)$ регистрового преобразования на основе МАГ с одной обратной связью:

$$\exp\Gamma(\varphi^g) \leqslant \Phi(\Lambda) + \rho(D) + 2n - d_q; \tag{19}$$

$$\exp\Gamma(\varphi^g) \leqslant \rho(D) + n, \text{ при} (n-1) \in D. \tag{20}$$

Проиллюстрируем полученные результаты на примерах.

Пример 1.

а) Рассмотрим перемешивающий орграф $\Gamma(\varphi^g)$ регистра сдвига с одной обратной связью при $n = 8$, $r = 32$, $D = \{0, 2, 4, 5\}$. Оценим $\exp\Gamma(\varphi^g)$. В орграфе $\Gamma(\varphi^g)$ множество длин контуров $L = \{8, 6, 4, 3\}$ (рис. 5). Орграф $\Gamma(\varphi^g)$ примитивный, так как НОД$(8, 6, 4, 3) = 1$. Выберем примитивное подмножество контуров с множеством длин $\Lambda = \{3, 4\}$. С учётом равенств $\Phi(3, 4) = 5$, $\rho(D) = 3$, $d_q = 5$ получаем по формуле (19) оценку $\exp\Gamma(\varphi^g) \leqslant 19$.

б) Оценим $\exp\Gamma(\varphi^{g,\mu})$ перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ регистра с двумя обратными связями при тех же значениях n, r, D. Пусть $m = 3$, $\Delta = \{2, 4, 5\}$. В этом случае

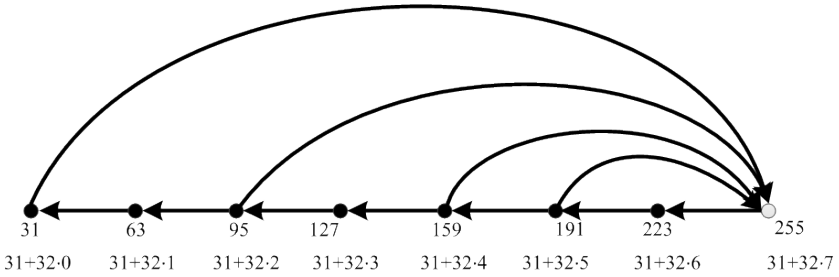

Рис. 5. Часть орграфа $\Gamma(\varphi^{g})$ при $v = 31$

выполняются условия $d_q > m$ ($d_q = 5$) и $\delta_1 \leqslant m$ ($\delta_1 = 2$). В $\Gamma(\varphi^{g,\mu})$ имеется множество $C^{(31)}$ (рис. 6), состоящее из семи простых контуров:

$$c^{D}_{31}(0) = c(255, 223, 191, 159, 127, 95, 63, 31),\ c^{D}_{31}(2) = c(255, 223, 191, 159, 127, 95),$$
$$c^{D}_{31}(4) = c(255, 223, 191, 159),\ c^{D}_{31}(5) = c(255, 223, 191),$$
$$c^{\Delta,D}_{31}(5, 0) = (255, 223, 191, 127, 95, 63, 31),$$
$$c^{\Delta,D}_{31}(5, 2) = (255, 223, 191, 127, 95),\ c^{\Delta}_{31}(2) = (127, 95).$$

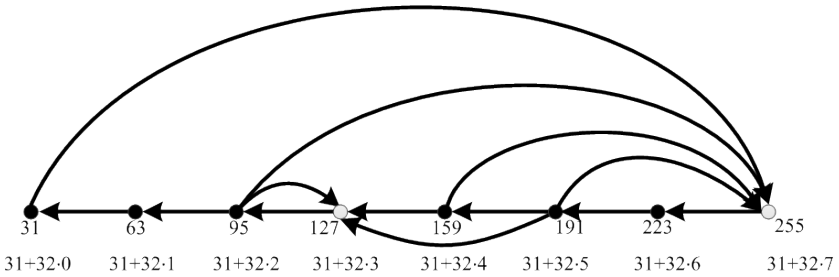

Рис. 6. Часть орграфа $\Gamma(\varphi^{g,\mu})$ при $v = 31$

Множество длин данных контуров есть $L = \{8, 7, 5, 4, 3, 2\}$. В соответствии с теоремой 5 орграф $\Gamma(\varphi^{g,\mu})$ примитивный. В соответствии с теоремой 6 оценим $\exp\Gamma(\varphi^{g,\mu})$ в зависимости от используемого примитивного множества контуров C. Заметим, что $d_t = \delta_\tau = 2$, $\max\{\delta_0, \delta_p\} = 5$. Значения параметров, необходимых для оценки экспонента, даны в табл. 1.

Таблица 1

Значения параметров в зависимости от выбора C

Параметры	Значения параметров (теорема 6, случай *а*)	Значения параметров (теорема 6, случай *в*)
C	$C = \{c^{D}_{31}(5), c^{D}_{31}(4)\}$	$C = \{c^{D}_{31}(5), c^{\Delta}_{31}(2)\}$
Λ, $\Phi(\Lambda)$	$\Lambda = \{3, 4\}$, $\Phi(3, 4) = 5$	$\Lambda = \{2, 3\}$, $\Phi(2, 3) = 1$
$\rho(d_q)$	$\rho(d_q) = \rho(D) = 3$	$\rho(d_q) = \rho(D) = 3$
ε либо ε'	$\varepsilon = 6$	$\varepsilon' = 5$

В случае *а* теоремы 6 (формула (15)) $\exp\Gamma(\varphi^{g,\mu}) \leqslant 15$; в случае *в* теоремы 6 (формула (17)) $\exp\Gamma(\varphi^{g,\mu}) \leqslant 13$.

Таким образом, оценка экспонента перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ регистра с двумя обратными связями может быть понижена по сравнению с оценкой экспонента

перемешивающего орграфа $\Gamma(\varphi^g)$ регистра с одной обратной связью. Величина оценки $\exp\Gamma(\varphi^{g,\mu})$ может быть оптимизирована с помощью выбора примитивного множества контуров.

в) Сравним (табл. 2) при $n = 8$ и $r = 32$ оценку $\exp\Gamma(\varphi^{g,\mu})$ по формулам (15) и (17) с известными оценками [6, ч. 1, разд. 11.3], применёнными к примитивным nr-вершинным орграфам Γ. Абсолютная оценка Виландта имеет вид

$$\exp\Gamma \leqslant (nr)^2 - 2nr + 2.$$

При известной длине l контура в примитивном орграфе Γ оценка более точная:

$$\exp\Gamma \leqslant nr + l(nr - 2).$$

Оценка экспонента уточняется, если в орграфе известны длины l и λ двух простых контуров, где $(l, \lambda) = 1$, $1 < \lambda < l \leqslant nr$. Если эти контуры не имеют общих вершин, то

$$\exp\Gamma \leqslant l\lambda - 2l - 3\lambda + 3nr;$$

если контуры имеют h общих вершин, то

$$\exp\Gamma \leqslant l\lambda - l - 3\lambda + h + 2nr.$$

Таблица 2

Оценки $\exp\Gamma(\varphi^{g,\mu})$, вычисленные по разным формулам

Формула	Значение оценки
$(nr)^2 - 2nr + 2$	65026
$nr + l(nr - 2)$	764 при $l = 2$
$l\lambda - 2l - 3\lambda + 3nr$	762 при $\lambda = 2,\ l = 3$
$l\lambda - l - 3\lambda + h + 2nr$	511 при $\lambda = 3,\ l = 4,\ h = 2$
$\Phi(\Lambda) + 1 + \rho(d_q) + \varepsilon$	15
$\Phi(\Lambda) + 1 + n - \max\{\delta_0, \delta_p\} + \rho(d_q) + \varepsilon'$	13

Табл. 2 показывает, что оценка $\exp\Gamma(\varphi^{g,\mu})$ существенно понижена с использованием полученных в теореме 6 формул.

Пример 2. Рассмотрим перемешивающий орграф $\Gamma(\varphi^{g,\mu})$, содержащий петли (случай $(n-1) \in D$, $m \in \Delta$), при $n = 8$, $r = 32$, $D = \{0, 2, 7\}$, $\Delta = \{m, m+1, 7\}$. В этом случае $\rho(D) = 5$, $d_q = 7$, $\max\{\delta_0, \delta_p\} = 7$. Сравним (табл. 3) оценки $\exp\Gamma(\varphi^g)$ (формула (20)) и $\exp\Gamma(\varphi^{g,\mu})$ (формула (18)) при различных значениях параметра m второй обратной связи.

Таблица 3

Оценки $\exp\Gamma(\varphi^g)$ и $\exp\Gamma(\varphi^{g,\mu})$ при различных значениях параметров

m	$\rho(D)$	$\rho(\delta)$	d_t	δ_τ	ε	ε'	$\exp\Gamma(\varphi^g)$	$\exp\Gamma(\varphi^{g,\mu})$
1	5	5	0	1	6	7	13	11
2	5	4	2	2	5	5	13	9
3	5	4	2	3	4	5	13	9
4	5	5	2	4	5	5	13	10
5	5	6	2	5	6	6	13	11

Пример показывает, что экспонент перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ может иметь более низкую оценку по сравнению с экспонентом перемешивающего орграфа $\Gamma(\varphi^g)$. Наименьшая величина оценки $\exp\Gamma(\varphi^{g,\mu})$ получается при значениях $m \approx \lceil (n-2)/2 \rceil$.

Замечание 1. Полученные оценки (15)–(18) являются достижимыми при оптимальном выборе примитивной системы контуров. Доказательство достижимости получается, например, при $d_q > m$, если рассмотреть пару вершин орграфа $(v+ri, u+rj)$ при $i = d_{k-1}$, где $\max\{n-d_q, d_q-d_{q-1}, \ldots, d_1-d_0\}$ достигается при $q = k$, и при вершине $u+rj$, наиболее удалённой от вершины $u+r(n-1)$ или вершины $u+rm$ (в зависимости от соотношения параметров). В частности, в примере 1, *б* между вершинами 254 и 158 существуют пути длины t при любом $t \geqslant 13$ и в силу свойств чисел Фробениуса не существует пути длины 12. При этом получена оценка $\exp\Gamma(\varphi^{g,\mu}) \leqslant 13$.

Заключение

Установлен ряд свойств преобразований регистров сдвига над пространтсвом V_r двоичных r-мерных векторов. Для регистровых преобразований с произвольным числом обратных связей получен критерий биективности.

С использованием матрично-графового подхода исследованы перемешивающие свойства преобразований регистров сдвига над V_r. Для подстановок φ из класса регистров сдвига с двумя обратными связями описаны множества простых путей и контуров в перемешивающем орграфе $\Gamma(\varphi)$. Для перемешивающих орграфов $\Gamma(\varphi^{g,\mu})$ подстановок регистров сдвига с двумя обратными связями, построенных на основе модифицированных аддитивных генераторов, доказан критерий примитивности, получены достижимые верхние оценки экспонента.

Полученные оценки экспонентов улучшают все другие известные оценки экспонентов для тех же орграфов (табл. 2).

Показано, что оценка экспонента перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ регистра сдвига над V_r с двумя обратными связями при определённых параметрах может быть улучшена по сравнению с оценкой экспонента перемешивающего орграфа $\Gamma(\varphi^g)$ регистра сдвига с одной обратной связью. Примеры показывают, что при одинаковых множествах точек съёма и $m \approx \lceil (n-2)/2 \rceil$ оценка экспонента улучшается до 30 %. Наименьшая величина оценки $\exp\Gamma(\varphi^{g,\mu})$ достигается в случае, если $(n-1)$ и m являются точками съёма, то есть орграф $\Gamma(\varphi^{g,\mu})$ имеет петли.

Полученные результаты могут быть использованы для построения итеративных криптографических алгоритмов на основе МАГ с быстрым перемешиванием входных данных.

ЛИТЕРАТУРА

1. *Коренева А. М., Фомичёв В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
2. *Коренева* (*Дорохова*) *А. М., Фомичёв В. М.* Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикладная дискретная математика. 2014. № 1(23). С. 77–83.
3. *Коренева* (*Дорохова*) *А. М.* Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов // Прикладная дискретная математика. Приложение. 2014. № 7. С. 60–64.
4. *Коренева А. М., Фомичёв В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 2. С. 32–52.
5. *Фомичёв В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.
6. *Фомичёв В. М., Мельников Д. А.* Криптографические методы защиты информации: учебник для академического бакалавриата. М.: ЮРАЙТ, 2016. 454 с.

7. *Фомичёв В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.

REFERENCES

1. *Koreneva A. M. and Fomichev V. M.* Ob odnom obobshchenii blochnykh shifrov Feystelya [About a Feistel block cipher generalization]. Prikladnaya Diskretnaya Matematika, 2012, no. 3(17), pp. 34–40. (in Russian)
2. *Dorokhova A. M. and Fomichev V. M.* Utochnennye otsenki eksponentov peremeshivayushchikh grafov biektivnykh registrov sdviga nad mnozhestvom dvoichnykh vektorov [Improvement of exponent estimates for mixing graphs of bijective shift registers over a set of binary vectors]. Prikladnaya Diskretnaya Matematika, 2014, no. 1(23), pp. 77–83. (in Russian)
3. *Dorokhova A. M.* Otsenki eksponentov peremeshivayushchikh grafov nekotorykh modifikatsiy additivnykh generatorov [Estimates for exponents of mixing graphs relating to some modifications of additive generators]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2014, no. 7, pp. 60–64. (in Russian)
4. *Koreneva A. M. and Fomichev V. M.* Peremeshivayushchie svoystva modifitsirovannykh additivnykh generatorov [The mixing properties of modified additive generators]. Diskretn. Anal. Issled. Oper., 2017, vol. 24, no. 2, pp. 32–52. (in Russian)
5. *Fomichev V. M.* Novaya universal'naya otsenka eksponentov grafov [The new universal estimation for exponents of graphs]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 78–84. (in Russian)
6. *Fomichev V. M. and Mel'nikov D. A.* Kriptograficheskie metody zashchity informatsii: uchebnik dlya akademicheskogo bakalavriata [Cryptographic Methods of Information Security.]. Moscow, YuRAYT Publ., 2016. 454 p. (in Russian)
7. *Fomichev V. M.* Otsenki eksponentov primitivnykh grafov [The estimates of exponents for primitive graphs]. Prikladnaya Diskretnaya Matematika, 2011, no. 2(12), pp. 101–112. (in Russian)