

ПЕРЕМЕШИВАЮЩИЕ СВОЙСТВА МОДИФИЦИРОВАННЫХ АДДИТИВНЫХ ГЕНЕРАТОРОВ *)

А. М. Коренева^{1,a}, В. М. Фомичёв^{1,2,3,b}

¹Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, 115409 Москва, Россия

²Финансовый университет при Правительстве РФ,
пр. Ленинградский, 49, 125993 Москва, Россия

³Институт проблем информатики ФИЦ ИУ РАН,
ул. Вавилова, 44, корп. 2, 119333 Москва, Россия

E-mail: ^aalisa.koreneva@gmail.com, ^bfomichev@nm.ru

Аннотация. В статье развивается матрично-графовый подход к оценке перемешивающих свойств биективных преобразований регистров сдвига над множеством двоичных векторов. Такие регистры сдвига обобщают, с одной стороны, класс шифров, основанных на сети Фейстеля, а с другой стороны, — класс преобразований множеств состояний аддитивных генераторов (на основе аддитивных генераторов построены алгоритмы Fish, Pike, Mush). Примечательно, что оригинальные схемы аддитивных генераторов признаны нестойкими, в том числе из-за слабых перемешивающих свойств. В статье приведены результаты исследования перемешивающих свойств модифицированных аддитивных генераторов. Для перемешивающего ориентированного графа преобразования множества состояний модифицированного аддитивного генератора определены множества дуг и контуров, получены условия примитивности и дана оценка экспонента. Показано, что при определённых параметрах модифицированного аддитивного генератора полное перемешивание может быть достигнуто за число итераций, существенно меньшее числа вершин перемешивающего орграфа. Табл. 1, ил. 1, библиогр. 13.

Ключевые слова: аддитивный генератор, модифицированный аддитивный генератор, перемешивающий орграф, примитивный орграф, регистр сдвига, экспонент орграфа.

*) Работа второго автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 16-01-00226).

Основные обозначения

В настоящей статье используются следующие обозначения: \mathbb{N} — множество натуральных чисел, $n \in \mathbb{N}$; V_n — n -мерное пространство двоичных векторов, $n > 1$; Z_n — кольцо вычетов по модулю n , $n > 1$; $\gcd(l_1, \dots, l_n)$ — наибольший общий делитель чисел $l_1, \dots, l_n \in \mathbb{N}$; 0,1-матрица — матрица над множеством $\{0,1\}$; $\exp \Gamma$ — экспонент орграфа Γ ; (i, j) — дуга в орграфе из вершины i и в j ; $w[i_0, i_1, \dots, i_k]$ — путь в орграфе, последовательно проходящий через вершины i_0, i_1, \dots, i_k ; $w[i_0, i_1, \dots, i_k] = w[i, j]$, если $i = i_0$ и $j = i_k$; $c(i_0, i_1, \dots, i_k)$ — контур в орграфе, последовательно проходящий через вершины i_0, i_1, \dots, i_k ; $\text{len } w$ ($\text{len } c$) — длина пути w (контура c), равная числу дуг пути (контура); $\Gamma(\varphi)$ — перемешивающий орграф преобразования φ ; \bullet — операция конкатенации путей в орграфе.

Введение

Важным свойством функций векторных пространств, реализуемых криптографическими системами, является перемешивание информации. Под полным перемешиванием информации понимается зависимость каждого знака выхода от всех знаков ключа (или входа). Функции с полным перемешиванием называют *совершенными*. Обобщениями свойства совершенности функций являются такие свойства, как строгий лавинный критерий, критерии распространения, свойство «бент» [6].

Принцип перемешивания (построения совершенных функций), получивший широкое практическое воплощение в эпоху синтеза электронных шифров, теоретически обоснован Шенноном в известном докладе в 1946 г. В дальнейшем детализация принципа перемешивания привела к различным исследованиям характеристик систем функций. Перемешивающие свойства функций обуславливают распространение функциями искажений (такие функции применяются в системах аутентификации) и важны для анализа симметричных криптосистем в связи с криптоаналитическими атаками на основе метода последовательного опробования частей ключа.

Аппаратная и/или программная реализация многих совершенных преобразований векторного пространства P^n над полем P затруднена необходимостью реализации большой системы функциональных связей, поэтому хорошее перемешивание часто достигается с помощью итераций удобно реализуемых преобразований с относительно слабыми перемешивающими свойствами. Точное определение множеств существенных переменных функций, как правило, трудоёмко, так как требует просмотра

таблиц функций. Поэтому для преобразования пространства V_n перемешивание оценивается с помощью матрично-графового подхода, при котором существенная зависимость координат выходных векторов от координат входных векторов кодируется 0,1-матрицей M порядка n (имеется или нет зависимость j -й координаты выхода от i -й координаты входа). Матрица M называется *перемешивающей*. Равносильным образом рассматривается n -вершинный перемешивающий орграф Γ преобразования, матрица смежности вершин которого совпадает с M [6, гл. 10].

Для итеративных преобразований пространства P^n оценка перемешивающих свойств состоит в изучении примитивности 0,1-матрицы M или орграфа Γ и определении их экспонентов. Матрица M *примитивна*, если некоторая её степень не содержит нулевых элементов. Орграф Γ *примитивен*, если некоторая его степень является полным орграфом. Наименьшая из таких степеней называется *экспонентом матрицы (орграфа)*. Экспоненты матрицы M и орграфа Γ совпадают, их величина позволяет оценить число необходимых итераций преобразования для достижения хорошего перемешивания информации.

Многие результаты по изучению примитивности и экспонентов матриц (графов), полученные до 2012 г., отражены в обзоре [2]; эта тематика активно разрабатывалась в [5, 7–9, 11–13]. Данная работа продолжает начатые в [1, 3] исследования экспонентов перемешивающих орграфов преобразований регистров сдвига над V_r , $r > 1$.

Любой примитивный орграф Γ является сильно связным. Универсальный критерий примитивности орграфа определяется длинами его контуров. Если l_1, \dots, l_m суть длины контуров орграфа Γ (достаточно рассматривать простые контуры), то орграф Γ примитивен тогда и только тогда, когда $\gcd(l_1, \dots, l_m) = 1$.

Приведём некоторые известные оценки экспонентов примитивных n -вершинных орграфов при $n > 1$, которые потребуются далее. Абсолютная достижимая оценка Виландта [13] имеет вид

$$\exp \Gamma \leq n^2 - 2n + 2. \quad (1)$$

При известной длине l контура в примитивном орграфе Γ оценка более точная [5]:

$$\exp \Gamma \leq n + l(n - 2). \quad (2)$$

В частности, $\exp \Gamma \leq 2n - 2$ для сильно связного орграфа Γ с петлёй.

Статья посвящена получению условий примитивности и оценке экспонентов перемешивающих орграфов биективных преобразований регистров сдвига над пространством V_r двоичных r -мерных векторов. Такие

регистры сдвига обобщают, с одной стороны, некоторый класс шифров, основанных на сети Фейстеля, а с другой стороны, — класс преобразований множеств состояний аддитивных генераторов. На основе аддитивных генераторов, известных также как «запаздывающие генераторы Фибоначчи», построены алгоритмы Fish, Pike, Mush [10]. Вместе с тем, несмотря на удобную реализацию, аддитивные генераторы плохо перемешивают входные данные. В связи с этим представляет интерес изучение перемешивающих свойств модификаций аддитивных генераторов по модулю 2^r с помощью преобразования, применяемого к значениям функции обратной связи.

Статья состоит из трёх разделов. В разд. 1 приведены результаты исследования примитивности и экспонентов перемешивающих графов преобразований биективных регистров сдвига над векторным пространством V_r . В разд. 2 описаны модифицированные аддитивные генераторы и их свойства, получен критерий биективности преобразования множества состояний модифицированного генератора. В разд. 3 описаны свойства перемешивающего орграфа преобразования множества состояний модифицированного аддитивного генератора, определены множества дуг и контуров, получены условия примитивности и дана оценка экспонента перемешивающего орграфа модификации.

1. Перемешивающие свойства биективных регистров сдвига над двоичным векторным пространством

По определению преобразование регистра сдвига длины n над пространством V_r двоичных r -мерных векторов есть преобразование φ множества $V_{nr} = \{(z_0, \dots, z_{n-1}) \mid z_0, \dots, z_{n-1} \in V_r\}$:

$$\varphi(z_0, \dots, z_{n-1}) = (z_1, \dots, z_{n-1}, f(z_0, \dots, z_{n-1})),$$

функция $f: V_{nr} \rightarrow V_r$ называется *функцией обратной связи регистра*. Известно, что φ — подстановка тогда и только тогда, когда функция f биективна по переменной z_0 [6, теорема 5.5].

Отметим некоторые важные для сравнительного анализа результаты работ [1, 3], относящиеся к подстановкам φ с функциями обратной связи вида $f = z_0 \oplus \psi(z_1, \dots, z_{n-1})$ при $n \geq 2$, где $\psi: V_{(n-1)r} \rightarrow V_r$, $\psi \neq \text{const}$ и \oplus — XOR-суммирование векторов из V_r .

Состояние регистра сдвига в текущий момент времени описывается двоичной матрицей размера $r \times n$, где k -й столбец матрицы, обозначаемый через z_k , определён равенством $z_k = (x_{rk}, \dots, x_{r-1+rk})^T$ (T — транспонирование) и записан в k -й ячейке регистра, $k = 0, \dots, n-1$.

Подстановка φ задаётся системой булевых координатных функций

$$\{\varphi_0(x_0, \dots, x_{nr-1}), \dots, \varphi_{nr-1}(x_0, \dots, x_{nr-1})\},$$

где функция $\varphi_{u+rk}(x_0, \dots, x_{nr-1})$ вычисляет u -й бит x_{u+rk} вектора z_k , $u = 0, \dots, r-1$, $k = 0, \dots, n-1$. Перемешивающие свойства подстановки φ определены системой $\{E(\varphi_0), \dots, E(\varphi_{nr-1})\}$, где $E(\varphi_j)$ — множество номеров существенных переменных функции φ_j , $j = 0, \dots, nr-1$. Отметим некоторые свойства:

- 1°. $E(\varphi_{u+rk}) = \{u + r(k+1)\}$, $k = 0, \dots, n-2$, $u = 0, \dots, r-1$;
- 2°. $E(\varphi_{u+r(n-1)}) \cap \{0, \dots, nr-1\} = \{u\}$;
- 3°. $E(\varphi_{r(n-1)}) \cup \dots \cup E(\varphi_{nr-1}) \setminus \{0, \dots, nr-1\} \neq \emptyset$ при $\psi \neq \text{const}$.

Подстановке φ ставится в соответствие nr -вершинный перемешивающий орграф $\Gamma(\varphi)$, в котором имеется дуга (i, j) тогда и только тогда, когда $i \in E(\varphi_j)$, $i, j \in \{0, \dots, nr-1\}$. Таким образом, дуги орграфа $\Gamma(\varphi)$ определяются свойствами 1°, 2° и существенными переменными функциями ψ . Для орграфа $\Gamma(\varphi)$ выполнены следующие свойства [1, 3]:

- 1) орграф $\Gamma(\varphi)$ содержит r независимых контуров c_0, \dots, c_{r-1} длины n , где $c_u = c(u + r(n-1), u + r(n-2), \dots, u + r, u)$, $u = 0, \dots, r-1$;
- 2) при $u = 0, \dots, r-1$ простой путь $w[u + ri, u + rj]$ в контуре c_u имеет длину $i - j$, если $i \geq j$, и $n - j + i$, если $i < j$, $i, j \in \{0, \dots, n-1\}$.

Для примитивного перемешивающего орграфа $\Gamma(\varphi)$ при любых натуральных $n > 1$, $r > 1$ [3, теорема 3] имеем

$$\exp \Gamma(\varphi) \leq n^2 r + nr - 2n. \quad (3)$$

Если, в частности, известна длина $l_1 < n$ контура в $\Gamma(\varphi)$ (т. е. некоторого контура, отличного от c_0, \dots, c_{r-1}), то

$$\exp \Gamma(\varphi) \leq (l_1 + 1)nr - 2l_1. \quad (4)$$

2. Свойства модифицированных аддитивных генераторов

В данном разделе описываются модифицированные аддитивные генераторы и их свойства, приводится критерий биективности преобразования множества состояний модифицированного аддитивного генератора.

2.1. Определяющие функции аддитивных генераторов и модификаций. Опишем аддитивные генераторы и их модификации, образующие частный класс рассмотренных в разд. 1 регистров длины n , ячейки которых занумерованы числами $0, \dots, n-1$.

Пусть X_0, X_1, \dots, X_{n-1} — числа из Z_{2^r} , составляющие начальное состояние генератора. В аддитивном генераторе знак X_i при $i \geq n$ образуется в соответствии с законом рекурсии:

$$X_i = \left(\sum_{j=0}^{n-1} a_j X_{j+i-n} \right) \bmod 2^r, \quad (5)$$

где $a_1, \dots, a_{n-1} \in \{0, 1\}$ и $a_0 = 1$ (в противном случае реальная длина регистра меньше n).

Пусть $b: Z_{2^r} \rightarrow V_r$ — биекция, сопоставляющая числу $X_i \in Z_{2^r}$ его двоичное представление. Формально, если $X = 2^{r-1}x_0 + \dots + 2x_{r-2} + x_{r-1} \in Z_{2^r}$, то

$$b(X) = (x_0, \dots, x_{r-1}) \in V_r.$$

Положим $\bar{X} = b(X)$. Тогда в соответствии с (5) аддитивный генератор есть регистр сдвига длины n с функцией обратной связи $f: V_{nr} \rightarrow V_r$, где

$$f(\bar{X}_0, \dots, \bar{X}_{n-1}) = b \left(\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r \right).$$

Функция $f(\bar{X}_0, \dots, \bar{X}_{n-1})$ биективна по переменной \bar{X}_0 , значит, регистр реализует подстановку φ множества состояний генератора

$$\varphi(\bar{X}_0, \dots, \bar{X}_{n-1}) = (\bar{X}_1, \dots, \bar{X}_{n-1}, f(\bar{X}_0, \dots, \bar{X}_{n-1})).$$

Обозначим через $\varphi_{u+rk}(x_0, \dots, x_{nr-1})$ координатные функции подстановки φ , где $u = 0, \dots, r-1$, $k = 0, \dots, n-1$.

Далее $\Gamma(\varphi)$ — перемешивающий nr -вершинный орграф подстановки φ множества состояний аддитивного генератора.

Из закона рекурсии (5) следует, что i -е разряды двоичного представления каждого из чисел X_0, X_1, \dots, X_{n-1} текущего состояния зависят только от $(r-1)$ -го, \dots , i -го разрядов чисел предыдущего состояния, $i = 0, \dots, r-1$. Следовательно, орграф $\Gamma(\varphi)$ не сильно связный, что исключает хорошие перемешивающие свойства преобразования множества состояний аддитивного генератора. Для достижения хорошего перемешивания необходима сильная связность орграфа $\Gamma(\varphi)$. В связи с этим модифицируем аддитивные генераторы с помощью преобразования g множества V_r , такие генераторы назовём *g-модификациями аддитивных генераторов*.

Для g -модификации аддитивного генератора при $i \geq n$ закон рекурсии имеет вид

$$X_i = b \cdot g \cdot b^{-1} \left(\left(\sum_{j=0}^{n-1} a_j X_{j+i-n} \right) \bmod 2^r \right), \quad (6)$$

где « \cdot » — операция произведения функций, при этом последовательность применения функций выполняется слева направо.

Обозначим через φ^g преобразование множества V_{nr} , которое реализуется g -модификацией:

$$\varphi^g(\overline{X}_0, \dots, \overline{X}_{n-1}) = (\overline{X}_1, \dots, \overline{X}_{n-1}, f^g(\overline{X}_0, \dots, \overline{X}_{n-1})). \quad (7)$$

В этом случае φ^g есть преобразование регистра сдвига с обратной связью $f^g: V_{nr} \rightarrow V_r$, где

$$\begin{aligned} f^g(\overline{X}_0, \dots, \overline{X}_{n-1}) &= f \cdot g(\overline{X}_0, \dots, \overline{X}_{n-1}) \\ &= b \cdot g \left(\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r \right). \end{aligned} \quad (8)$$

2.2. Критерий биективности преобразования множества состояний модифицированного генератора.

Теорема 1. Преобразование φ^g является подстановкой пространства V_{nr} тогда и только тогда, когда g — подстановка пространства V_r .

ДОКАЗАТЕЛЬСТВО. Пусть g есть подстановка V_{nr} , а (X_0, \dots, X_{n-1}) и (Y_0, \dots, Y_{n-1}) суть различные состояния g -модификации аддитивного генератора. Возможны два случая.

СЛУЧАЙ 1. Пусть $(X_1, \dots, X_{n-1}) \neq (Y_1, \dots, Y_{n-1})$. Тогда в соответствии с (7) имеем

$$\varphi^g(\overline{X}_0, \dots, \overline{X}_{n-1}) \neq \varphi^g(\overline{Y}_0, \dots, \overline{Y}_{n-1}).$$

СЛУЧАЙ 2. Пусть $(X_1, \dots, X_{n-1}) = (Y_1, \dots, Y_{n-1})$ и $X_0 \neq Y_0$. Тогда

$$f(\overline{X}_0, \dots, \overline{X}_{n-1}) \neq f(\overline{Y}_0, \dots, \overline{Y}_{n-1}),$$

так как при $a_0 = 1$ функция $f(\overline{X}_0, \dots, \overline{X}_{n-1})$ биективна по переменной \overline{X}_0 . Отсюда в соответствии с (8) выводим

$$f^g(\overline{X}_0, \dots, \overline{X}_{n-1}) \neq f^g(\overline{Y}_0, \dots, \overline{Y}_{n-1}),$$

поскольку g и b — биекции. Следовательно, в соответствии с (7) получаем

$$\varphi^g(\overline{X}_0, \dots, \overline{X}_{n-1}) \neq \varphi^g(\overline{Y}_0, \dots, \overline{Y}_{n-1}).$$

Значит, в любом случае функция φ^g инъективная и тем самым биективная.

Обратно, пусть g — не подстановка. Тогда $g(b(\alpha)) = g(b(\beta))$ для некоторых $\alpha, \beta \in Z_{2^r}$, где $\alpha \neq \beta$ и $b(\alpha) \neq b(\beta)$, в силу биективности функции b . Для различных состояний $(\alpha, \mathbf{0}, \dots, \mathbf{0})$ и $(\beta, \mathbf{0}, \dots, \mathbf{0})$ g -модификации аддитивного генератора в силу (5) выполнено

$$f(b(\alpha), \mathbf{0}, \dots, \mathbf{0}) = b(\alpha) \neq b(\beta) = f(b(\beta), \mathbf{0}, \dots, \mathbf{0}),$$

где $\mathbf{0} \in Z_{2^r}$, $b(\mathbf{0}) = \overline{0}$. Тогда из (8) следует

$$f^g(b(\alpha), \overline{0}, \dots, \overline{0}) = g(b(\alpha)) = g(b(\beta)) = f^g(b(\beta), \overline{0}, \dots, \overline{0}).$$

Отсюда с учётом (7) получаем, что φ^g не является подстановкой множества V_r . Теорема 1 доказана.

3. Свойства перемешивающего орграфа преобразования множества состояний модифицированного аддитивного генератора

В данном разделе описываются свойства перемешивающего орграфа преобразования множества состояний модифицированного аддитивного генератора, определяются множества дуг и контуров, даются условия примитивности и оценка экспонента перемешивающего орграфа модификации.

Для каждого $u = 0, \dots, r-1$ введём следующие обозначения: $\varphi_{u+rk}^g(\overline{X}_0, \dots, \overline{X}_{n-1})$, $k = 0, \dots, n-1$, — координатные булевы функции преобразования φ^g ; $g_u(y_0, \dots, y_{r-1})$ — координатные булевы функции преобразования g ; $\Gamma(g)$ — перемешивающий r -вершинный орграф преобразования g ; $\Gamma(\varphi^g)$ — перемешивающий nr -вершинный орграф преобразования φ^g ; $D = \{d_0, \dots, d_q\}$ — множество точек съёма регистра φ^g (т. е. множество номеров существенных переменных функции обратной связи регистра), где $0 < q$, $0 = d_0 < \dots < d_q < n$. Множество D не зависит от g и в соответствии с (8) $j \in D$ тогда и только тогда, когда $a_j = 1$.

3.1. Определение множества дуг перемешивающего орграфа. В силу (7) при описании множеств существенных переменных координатных функций φ_j^g , $j = 0, \dots, nr-1$, достаточно ограничиться координатными функциями $\varphi_{u+r(n-1)}^g$ обратной связи f^g , $u = 0, \dots, r-1$.

Из (8) следует, что

$$\varphi_{u+r(n-1)}^g(\overline{X}_0, \dots, \overline{X}_{n-1}) = b \cdot g_u \left(\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r \right). \quad (9)$$

Функцию f , определённую на множестве X , назовём *постоянной на подмножестве* $Q \subseteq X$, если ограничение f на Q есть константа. При $\tau = 1, \dots, r-1$ имеют место следующие разбиения:

1) r -мерный куб V_r разбивается на $2^{r-\tau}$ подкубов $Q(c_\tau, \dots, c_{r-1})$ размерности τ вида

$$Q(c_\tau, \dots, c_{r-1}) = \{(y_0, \dots, y_{\tau-1}, c_\tau, \dots, c_{r-1}) \mid y_0, \dots, y_{\tau-1} \in \{0, 1\}\},$$

где $(c_\tau, \dots, c_{r-1}) \in V_{r-\tau}$;

2) аддитивная группа Z_{2^r} разбивается на $2^{r-\tau}$ смежных классов вида $2^{r-\tau}Z_{2^r} + a$ по подгруппе $2^{r-\tau}Z_{2^r}$, где $a \in Z_{2^{r-\tau}}$.

Такие системы подкубов и смежных классов обозначим через Q_r^τ и $Z_{2^r}^\tau$ соответственно. С преобразованием g связано преобразование \hat{g} группы Z_{2^r} :

$$\hat{g}(Y) = b \cdot g \cdot b^{-1}(Y).$$

Из формул (6)–(8) непосредственно следуют леммы 1 и 2.

Лемма 1. Биекция $b: Z_{2^r} \leftrightarrow V_r$ индуцирует биекцию $\xi: Q_r^\tau \leftrightarrow Z_{2^r}^\tau$ со свойством $\xi(Q(c_\tau, \dots, c_{r-1})) = 2^{r-\tau}Z_{2^r} + b^{-1}(0, \dots, 0, c_\tau, \dots, c_{r-1})$.

Лемма 2. Функция $g_u(y_0, \dots, y_{r-1})$ постоянна на любом подкубе из системы Q_r^τ тогда и только тогда, когда $y_0, \dots, y_{\tau-1}$ — фиктивные переменные координатной функции g_u .

Теорема 2. При $u = 0, \dots, r-1$ для множества переменных функции $\varphi_{u+r(n-1)}^g$ верны следующие утверждения:

- 1) x_{v+rk} фиктивна при любом $k \notin D$, $v = 0, \dots, r-1$;
- 2) x_{v+rk} фиктивна при любом $k \in D$, $v = 0, \dots, \tau-1$, если переменные $y_0, \dots, y_{\tau-1}$ фиктивны для функции g_u , $\tau \geq 1$;
- 3) x_{v+rk} существенна при $v = \theta, \dots, r-1$ и при любом $k \in D$, если переменная y_θ существенна для функции g_u , $\theta \geq 0$.

Доказательство. 1) Пусть $(\overline{X}_0, \dots, \overline{X}_{n-1}), (\overline{Y}_0, \dots, \overline{Y}_{n-1}) \in V_{nr}$ — векторы, соседние по $(v+rk)$ -й координате при некотором $k \notin D$. Тогда $X_j = Y_j$ при всех $k \in D$, значит,

$$\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r = \left(\sum_{j=0}^{n-1} a_j Y_j \right) \bmod 2^r.$$

В силу (8) имеем $f^g(\overline{X}_0, \dots, \overline{X}_{n-1}) = f^g(\overline{Y}_0, \dots, \overline{Y}_{n-1})$, откуда

$$\varphi_{u+r(n-1)}^g(\overline{X}_0, \dots, \overline{X}_{n-1}) = \varphi_{u+r(n-1)}^g(\overline{Y}_0, \dots, \overline{Y}_{n-1}).$$

Осталось заметить, что эти рассуждения верны при произвольных $k \notin D$ и $v = 0, \dots, r-1$.

В соответствии с (8) функция $f^g(\overline{X}_0, \dots, \overline{X}_{n-1})$ инвариантна относительно любой перестановки переменных \overline{X}_k , $k \in D$. Следовательно, при любом $v = 0, \dots, r-1$ переменные x_{v+rk} при $k \in D$ существенные или несущественные для $\varphi_{u+r(n-1)}^g$ одновременно. Поэтому 2) и 3) достаточно доказать для переменной x_v (случай $k = 0$).

2) Пусть $\overline{X}_0, \overline{Y}_0 \in V_r$ — соседние по v -й координате векторы, где $b^{-1}(\overline{X}_0) - b^{-1}(\overline{Y}_0) = 2^{r-v}$. Тогда $(\overline{X}_0, \dots, \overline{X}_{n-1})$ и $(\overline{Y}_0, \dots, \overline{Y}_{n-1})$ суть соседние по v -й координате векторы из V_{nr} при $\overline{X}_i = \overline{Y}_i \in V_r$, где $i = 1, \dots, n-1$. Этим векторам соответствуют состояния g -модификации аддитивного генератора (X_0, \dots, X_{n-1}) и (Y_0, \dots, Y_{n-1}) , для которых

$$\sum_{j=0}^{n-1} a_j Y_j \equiv \sum_{j=0}^{n-1} a_j X_j \pmod{2^{r-v}}. \quad (10)$$

Пусть $v \leq \tau$. Из (10) следует, что числа

$$\left(\sum_{j=0}^{n-1} a_j Y_j \right) \bmod 2^r \quad \text{и} \quad \left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r$$

принадлежат одному смежному классу аддитивной группы Z_{2^r} по подгруппе $2^{r-\tau} Z_{2^r}$. С учётом этого по лемме 1 получаем, что векторы

$$b \left(\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r \right) \quad \text{и} \quad b \left(\left(\sum_{j=0}^{n-1} a_j Y_j \right) \bmod 2^r \right)$$

лежат в некотором подкубе размерности τ . Отсюда по лемме 2 имеем

$$b \cdot g_u \left(\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r \right) = b \cdot g_u \left(\left(\sum_{j=0}^{n-1} a_j Y_j \right) \bmod 2^r \right).$$

Тогда из (9) следует, что

$$\varphi_{u+r(n-1)}^g(\overline{X}_0, \dots, \overline{X}_{n-1}) = \varphi_{u+r(n-1)}^g(\overline{Y}_0, \dots, \overline{Y}_{n-1}).$$

В силу произвольности пары $(\bar{X}_0, \dots, \bar{X}_{n-1})$ и $(\bar{Y}_0, \dots, \bar{Y}_{n-1})$ соседних по v -й координате векторов переменная x_v фиктивная для $\varphi_{u+r(n-1)}^g$.

3) По условию $g_u(\bar{X}_0) \neq g_u(\bar{Y}_0)$ для некоторых соседних по θ -й координате векторов $\bar{X}_0, \bar{Y}_0 \in V_r$. Если $\bar{X}_i = \bar{Y}_i = \bar{0}$, $i = 1, \dots, n-1$, то для соседних по θ -й координате векторов $(\bar{X}_0, \dots, \bar{X}_{n-1})$ и $(\bar{Y}_0, \dots, \bar{Y}_{n-1})$ из V_{nr} выполнено

$$\begin{aligned} b \cdot g_u \left(\left(\sum_{j=0}^{n-1} a_j X_j \right) \bmod 2^r \right) &= g_u(\bar{X}_0) \\ &\neq g_u(\bar{Y}_0) = b \cdot g_u \left(\left(\sum_{j=0}^{n-1} a_j Y_j \right) \bmod 2^r \right). \end{aligned}$$

Тогда переменная x_θ существенна для $\varphi_{u+r(n-1)}^g$, так как в силу (9) имеем

$$\varphi_{u+r(n-1)}^g(\bar{X}_0, \dots, \bar{X}_{n-1}) \neq \varphi_{u+r(n-1)}^g(\bar{Y}_0, \dots, \bar{Y}_{n-1}). \quad (11)$$

Покажем, что при $\theta < r-1$ переменная $x_{\theta+1}$ также существенна для $\varphi_{u+r(n-1)}^g$.

Пусть $\bar{X}_0 = (a_0, \dots, a_{r-1})$, $\bar{Y}_0 = (c_0, \dots, c_{r-1})$, где $a_i = c_i$ при всех $i \in \{0, \dots, r-1\} \setminus \{\theta\}$. Без ограничения общности положим $a_\theta = 0$, $c_\theta = 1$. Тогда вектор $\bar{E} = (e_0, \dots, e_{r-1})$ соседний с \bar{X}_0 по $(\theta+1)$ -й координате при $a_{\theta+1} = 0$, $e_{\theta+1} = 1$ и $a_i = e_i$ для всех $i \in \{0, \dots, r-1\} \setminus \{\theta+1\}$ (случай $a_{\theta+1} = 1$, $e_{\theta+1} = 0$ доказывается аналогично). При заданных равенствах $Y_0 - E = E - X_0 = 2^{r-\theta-1}$ векторы \bar{Y}_0 и $b(Y_0 + 2^{r-\theta-1})$ соседние по $(\theta+1)$ -й координате, векторы \bar{E} и $b(Y_0 + 2^{r-\theta-1})$ соседние по θ -й координате.

Выберем соседние по θ -й координате векторы $\Omega_X = (\bar{X}_0, \dots, \bar{X}_{n-1})$, $\Omega_Y = (\bar{Y}_0, \dots, \bar{Y}_{n-1}) \in V_{nr}$ такие, что $g_u(\bar{X}_0) \neq g_u(\bar{Y}_0)$ и

$$\sum_{j=0}^{n-1} a_j X_j \equiv 2^{r-\theta-1} \pmod{2^r}.$$

Тогда если переменная $y_{\theta+1}$ фиктивная для g_u , то $g_u(\bar{X}_0) = g_u(\bar{E})$, и в силу (9) и (11) имеем

$$\begin{aligned} \varphi_{u+r(n-1)}^g(\Omega_X) &= g_u(b(X_0 + 2^{r-\theta-1})) = g_u(\bar{E}) = g_u(\bar{X}_0) \\ &\neq g_u(\bar{Y}_0) = g_u(b(E + 2^{r-\theta-1})) = \varphi_{u+r(n-1)}^g(\Omega_E), \end{aligned}$$

где $\Omega_E = (\bar{E}, \bar{X}_1, \dots, \bar{X}_{n-1})$. Так как векторы $\Omega_X, \Omega_E \in V_{nr}$ соседние по $(\theta+1)$ -й координате, переменная $x_{\theta+1}$ существенна для функции $\varphi_{u+r(n-1)}^g$.

В силу доказанного если при $\theta + 1 < r - 1$ переменная $x_{\theta+1}$ существенная для $\varphi_{u+r(n-1)}^g$, то независимо от того, существенна или фиктивна $y_{\theta+2}$, переменная $x_{\theta+2}$ также существенная для $\varphi_{u+r(n-1)}^g$, и т. д. Отсюда если переменная y_θ существенная для функции g_u , $\theta \geq 0$, то переменные $x_\theta, x_{\theta+1}, \dots, x_{r-1}$ существенны для $\varphi_{u+r(n-1)}^g$. Теорема 2 доказана.

3.2. Множество контуров и сильная связность перемешивающего орграфа. Введём следующие обозначения: $L(g)$ — множество длин контуров орграфа $\Gamma(g)$; μ_u — наименьший номер существенной переменной координатной функции $g_u(y_0, \dots, y_{r-1})$; $U(g)$ — множество вершин орграфа $\Gamma(g)$ со свойством: $u \in U(g)$ тогда и только тогда, когда $\mu_u \leq u$.

Орграфу $\Gamma(g)$ соответствует орграф $\Gamma_E(g)$, в котором множество вершин есть $\{0, \dots, r-1\}$ и пара вершин (v, u) образует дугу в $\Gamma_E(g)$ тогда и только тогда, когда $v \geq \mu_u$.

Лемма 3. Если в орграфе $\Gamma(g)$ имеется простой контур длины k , то в орграфе $\Gamma_E(g)$ имеются простые контуры длин $1, 2, \dots, k$.

ДОКАЗАТЕЛЬСТВО. Пусть $k \geq 1$ и $c = c(i_1, \dots, i_k)$ — простой контур в орграфе $\Gamma(g)$. Тогда контур c имеется в орграфе $\Gamma_E(g)$, так как $\Gamma(g)$ — часть орграфа $\Gamma_E(g)$.

Пусть $i_s = \min\{i_1, \dots, i_k\}$ и $i_{s-1} = i_k$ при $s = 1$ и $i_{s+1} = i_1$ при $s = k$. Тогда $i_{s-1} > i_s$ и $i_{s+1} > i_s$. Так как в контуре c имеется дуга (i_s, i_{s+1}) , по определению орграфа $\Gamma(g)$ переменная с номером i_s существенна для g_u при $u = i_{s+1}$ и $u \in U(g)$. Следовательно, по определению орграфа $\Gamma_E(g)$ пара (v, u) образует дугу в $\Gamma_E(g)$ для любого $v \geq i_s$. В частности, в $\Gamma_E(g)$ имеется дуга (i_{s-1}, i_{s+1}) , так как $i_{s-1} > i_s$. Значит, имеется контур c' длины $k - 1$, полученный из c удалением вершины i_s . Из аналогичных рассуждений для контура c' получаем, что в $\Gamma_E(g)$ имеется контур длины $k - 2$, и т. д. Таким образом, в $\Gamma_E(g)$ имеются контуры длин $1, 2, \dots, k$. Лемма 3 доказана.

Для $l \in \mathbb{N}$ и множества $L = \{n-d_0, \dots, n-d_q\}$ определим отображение $\sigma_l: L^l \rightarrow \mathbb{N}$, где $\sigma_l(m_1, \dots, m_l) = \sum_{j=1}^l m_j$. Положим $\sigma(\bigcup_l L^l) = \bigcup_l \sigma_l(L^l)$.

Обозначим через $w(u, d_j) = w[u + r(n-1), u + r(n-2), \dots, u + rd_j]$ путь длины $n-1-d_j$ в орграфе $\Gamma(\varphi^g)$, $w(u) = w(u, 0)$, $V(u)$ — множество вершин пути $w(u)$; $u = 0, \dots, r-1$, $d_j \in D$.

Теорема 3. 1) В орграфе $\Gamma_E(g)$ есть простой контур $c = c(i_1, \dots, i_k)$ тогда и только тогда, когда в $\Gamma(\varphi^g)$ при любом $\delta = (\delta_1, \dots, \delta_k) \in D^k$ имеется простой контур $c^g(c, \delta) = w(i_1, \delta_1) \bullet (i_1 + r\delta_1, i_2 + r(n-1)) \bullet \dots \bullet$

$w(i_k, \delta_k) \bullet (i_k + r\delta_k, i_1 + r(n-1))$. Множество длин простых контуров орграфа $\Gamma(\varphi^g)$ совпадает с множеством $\sigma\left(\bigcup_{l=1}^k L^l\right)$, где k — наибольшая длина простого контура в $\Gamma_E(g)$.

2) Орграф $\Gamma(\varphi^g)$ сильно связный тогда и только тогда, когда в $\Gamma(g)$ имеется путь $w[0, r-1]$ и полустепень захода каждой вершины больше нуля.

ДОКАЗАТЕЛЬСТВО. 1) В соответствии с теоремой 2 в $\Gamma_E(g)$ имеется простой путь $w = w[i_1, \dots, i_k]$ тогда и только тогда, когда орграф $\Gamma(\varphi^g)$ при любом наборе $\delta = (\delta_1, \dots, \delta_{k-1}) \in D^{k-1}$ содержит дуги

$$(i_1 + r\delta_1, i_2 + r(n-1)), \dots, (i_{k-1} + r\delta_{k-1}, i_k + r(n-1)).$$

В силу (7) для $u = 0, \dots, r-1$ и любого $d_j \in D$ в $\Gamma(\varphi^g)$ имеются простые пути $w(u, d_j) = w[u + r(n-1), u + r(n-2), \dots, u + rd_j]$. Так как конкатенация путей $w \bullet w'$ определена тогда и только тогда, когда конечная вершина пути w совпадает с начальной вершиной пути w' , в $\Gamma_E(g)$ имеется простой путь $w = w[i_1, \dots, i_k]$ тогда и только тогда, когда для любого набора $\delta = (\delta_1, \dots, \delta_k) \in D^k$ в орграфе $\Gamma(\varphi^g)$ имеется простой путь $w^g(w, \delta)$ длины $\sum_{j=1}^k (n - \delta_j) - 1$:

$$w^g(w, \delta) = w(i_1, \delta_1) \bullet (i_1 + r\delta_1, i_2 + r(n-1)) \bullet \dots \bullet (i_{k-1} + r\delta_{k-1}, i_k + r(n-1)) \bullet w(i_k, \delta_k).$$

В соответствии с теоремой 2 наличие дуги (i_k, i_1) в $\Gamma_E(g)$ равносильно наличию в $\Gamma(\varphi^g)$ дуги $(i_k + r\delta_k, i_1 + r(n-1))$ при любом $\delta_k \in D$. Следовательно, в $\Gamma_E(g)$ имеется простой контур $c = c(i_1, \dots, i_k)$ тогда и только тогда, когда в $\Gamma(\varphi^g)$ имеется простой контур $c^g(c, \delta)$ длины $\sum_{j=1}^k (n - \delta_j)$, где $c^g(c, \delta) = w^g(w, \delta) \bullet (i_k + r\delta_k, i_1 + r(n-1))$.

Заметим, что $\text{len } c^g(c, \delta) \in \sigma\left(\bigcup_{l=1}^k L^l\right)$. Так как любой простой контур в $\Gamma(\varphi^g)$ имеет вид

$$w(i_1, \delta_1) \bullet (i_1 + r\delta_1, i_2 + r(n-1)) \bullet \dots \bullet w(i_k, \delta_k) \bullet (i_k + r\delta_k, i_1 + r(n-1)),$$

существует набор $\delta' = (\delta_1, \dots, \delta_m) \in D^m$, $m \leq k$, такой, что в $\Gamma(\varphi^g)$ имеется контур $c^g(c, \delta')$ длины λ для любого числа $\lambda \in \sigma\left(\bigcup_{l=1}^k L^l\right)$. Отсюда

с учётом леммы 3 получаем, что $\sigma\left(\bigcup_{l=1}^k L^l\right)$ есть множество длин простых контуров $\Gamma(\varphi^g)$, где k — наибольшая длина простого контура в $\Gamma_E(g)$.

2) В силу доказанного в 1) достижимость вершины j из вершины i в орграфе $\Gamma_E(g)$ равносильна достижимости в орграфе $\Gamma(\varphi^g)$ множества вершин $V(j)$ из множества вершин $V(i)$, $i, j = 0, \dots, r-1$.

Наличие в орграфе $\Gamma(g)$ дуги (v, u) равносильно тому, что переменная y_v существенная для функции $g_u(y_0, \dots, y_{r-1})$. В силу теоремы 2(3) последнее равносильно тому, что переменная x_j существенная для функции $\varphi_{u+r(n-1)}^g$, $j = v, \dots, r-1$, т. е. достижимости вершины $u + r(n-1)$ из вершин $v, \dots, r-1$ в $\Gamma(\varphi^g)$. Тогда с учётом путей $w(v), \dots, w(r-1)$ в орграфе $\Gamma(\varphi^g)$ наличие дуги (v, u) в $\Gamma(g)$ равносильно тому, что любая вершина из $V(u)$ достижима из любой вершины множества $\bigcup_{j=v}^{r-1} V(j)$.

Отсюда наличие пути $w[0, r-1] = w[i_1, \dots, i_k]$, где $i_1 = 0, i_k = r-1$, в орграфе $\Gamma(g)$ равносильно тому, что любая вершина из $V(i_{s+1})$ достижима из любой вершины множества $\bigcup_{j=i_s}^{r-1} V(j)$, $s = 1, \dots, k-1$, или тому, что любая вершина из $V(r-1)$ достижима из любой вершины графа $\Gamma(\varphi^g)$. Вместе с тем по условию в любую вершину j орграфа $\Gamma(g)$ заходит дуга, значит, по теореме 2(3) любая вершина графа $\Gamma(\varphi^g)$ достижима из вершин множества $V(r-1)$. Следовательно, наличие пути $w[0, r-1]$ в $\Gamma(g)$ равносильно сильной связности орграфа $\Gamma(\varphi^g)$. Теорема 3 доказана.

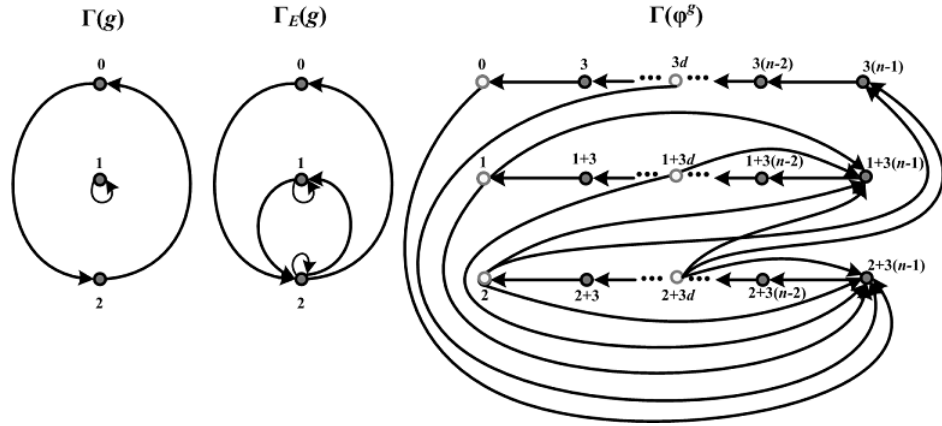


Рис. 1. Орграфы $\Gamma(g)$, $\Gamma_E(g)$ и $\Gamma(\varphi^g)$

Для примера на рис. 1 изображены орграфы $\Gamma(g)$, $\Gamma_E(g)$ и $\Gamma(\varphi^g)$ в случае $r = 3$, $g(y_0, y_1, y_2) = (y_2, y_1, y_0)$, $D = \{0, d\}$.

3.3. Примитивность и экспонент перемешивающего орграфа.

Пусть $L = \{n - d_0, \dots, n - d_q\}$.

Теорема 4. При $q = 0$ орграф $\Gamma(\varphi^g)$ не примитивный. При $q \geq 1$ сильно связный орграф $\Gamma(\varphi^g)$ примитивен тогда и только тогда, когда $\gcd(n, d_1, \dots, d_q) = 1$.

ДОКАЗАТЕЛЬСТВО. Ввиду универсального критерия сильно связный орграф примитивен тогда и только тогда, когда $\gcd(l_1, \dots, l_m) = 1$, где l_1, \dots, l_m суть длины простых контуров орграфа [2, 5]. При $q = 0$ имеем $L = \{n\}$, откуда в соответствии с теоремой 3(1) получаем, что длина любого контура в $\Gamma(\varphi^g)$ кратна n . Значит, $\Gamma(\varphi^g)$ не примитивный.

При $q \geq 1$ укажем в сильно связном орграфе $\Gamma(\varphi^g)$ контуры, длины которых взаимно просты при $\gcd(n, d_1, \dots, d_q) = 1$. По теореме 3(2) если орграф $\Gamma(\varphi^g)$ сильно связный, то в $\Gamma(g)$ имеется путь $w[0, r - 1]$, тем самым в $\Gamma(g)$ имеется дуга (v, u) , где $v \leq u$. Это означает, что переменная y_v существенная для координатной функции $g_u(y_0, \dots, y_{r-1})$. Отсюда в силу теоремы 2(3) переменные x_{j+rk} существенны для функции $\varphi_{u+r(n-1)}^g$ при $j = v, \dots, r - 1$ и любом $k \in D$. В частности, при $v \leq u$ переменная x_{u+rk} существенная для функции $\varphi_{u+r(n-1)}^g$. Следовательно, в $\Gamma(\varphi^g)$ при любом $k \in D$ имеются дуги $(u + rk, u + r(n - 1))$, которые при конкатенации с путями $w(u, k)$ образуют простые контуры

$$c(u, k) = c(u + r(n - 1), u + r(n - 2), \dots, u + rk)$$

длины $n - k$. Значит, при $q \geq 1$ в орграфе $\Gamma(\varphi^g)$ имеется система не менее двух простых контуров с множеством длин L . Так как общий делитель множества чисел делит разность любой пары из этих чисел, имеем $\gcd L = \gcd(n, d_1, \dots, d_q)$. Отсюда если $\gcd(n, d_1, \dots, d_q) = \mu = 1$, то система контуров $\{c(u, k), k \in D\}$ определяет примитивность орграфа $\Gamma(\varphi^g)$. Если же $\mu > 1$, то в соответствии с теоремой 3(1) μ делит длину любого контура в орграфе $\Gamma(\varphi^g)$. Теорема 4 доказана.

Замечание 1. При $q \geq 1$ выполнено

$$\gcd(n, d_1, \dots, d_q) = \gcd(n, d_1 - d_0, \dots, d_q - d_{q-1}).$$

Пусть $\langle i, r - 1 \rangle$ обозначает кратчайший путь из i в $r - 1$ в графе $\Gamma_E(g)$, $i = 0, \dots, r - 1$, $\rho = \max\{\text{len}\langle 0, r - 1 \rangle, \dots, \text{len}\langle r - 1, r - 1 \rangle\}$.

Лемма 4. Для графа $\Gamma_E(g)$ имеет место $\rho = \text{len}\langle 0, r - 1 \rangle$.

ДОКАЗАТЕЛЬСТВО. По определению если в графе $\Gamma_E(g)$ есть дуга (v, u) , то для любого $v' \geq v$ в нём есть и дуга (v', u) . Таким образом, если

$\langle 0, r-1 \rangle = w[0, i_1, \dots, i_{k-1}, r-1]$, где $\text{len}\langle 0, r-1 \rangle = k \geq 1$, то в графе $\Gamma_E(g)$ имеется путь $w[i, i_1, \dots, i_{k-1}, r-1]$ из i в $r-1$ длины k , откуда $\text{len}\langle i, r-1 \rangle \leq k$, $i = 0, \dots, r-1$. Лемма 4 доказана.

Оценим при $q \geq 1$ экспонент примитивного орграфа $\Gamma(\varphi^g)$. Обозначим $\Delta = \max\{d_1 - d_0, \dots, d_q - d_{q-1}, n - d_q\}$, $\Phi(a_1, \dots, a_m)$ — число Фробениуса (при $m > 1$ равное наибольшему числу, не принадлежащему аддитивной полугруппе $\langle a_1, \dots, a_m \rangle$, порождённой натуральными взаимно простыми числами a_1, \dots, a_m , $\Phi(1, a_2, \dots, a_m) = -1$).

Вершину орграфа назовём *узловой*, если в ней имеется петля или через неё проходит не менее двух контуров с множеством взаимно простых длин.

Теорема 5. Если орграф $\Gamma(\varphi^g)$ примитивный, то

$$\exp \Gamma(\varphi^g) \leq \Delta + (n - d_q)\rho + \Phi(L) + n, \quad (12)$$

где $L = \{n - d_0, \dots, n - d_q\}$.

ДОКАЗАТЕЛЬСТВО. В вершине r орграфа $\Gamma_E(g)$ имеется петля, поэтому в примитивном орграфе $\Gamma(\varphi^g)$ вершина $nr - 1$ является узловой, через неё проходят контуры с множеством L взаимно простых длин (показано в доказательстве теоремы 4). Путь $w[i, j]$ в $\Gamma(\varphi^g)$, проходящий через вершину $nr - 1$, при любых $i, j \in \{0, \dots, nr - 1\}$ представляется конкатенацией:

$$w[i, j] = w[i, nr - 1] \bullet c(nr - 1) \bullet w[nr - 1, j],$$

где $c(nr - 1)$ — контур, проходящий через узловую вершину $nr - 1$. Варьируя кратность обхода простых контуров, проходящих через $nr - 1$, можно (в соответствии с определением числа Фробениуса) построить контур $c(nr - 1)$ длины t при любом $t > \Phi(L)$. Отсюда

$$\begin{aligned} \exp \Gamma(\varphi^g) &\leq \max_{i \in \{0, \dots, nr - 1\}} \text{len } w[i, nr - 1] \\ &\quad + \Phi(L) + 1 + \max_{j \in \{0, \dots, nr - 1\}} \text{len } w[nr - 1, j]. \end{aligned}$$

Пусть $i \in V(l)$ и w — кратчайший путь длины k в графе $\Gamma_E(g)$ из l в $r - 1$, $l \in \{0, \dots, r - 1\}$. Более точно, $i = l + r\xi$, где $0 \leq \xi < n$, и $w = (l, l_1) \bullet \dots \bullet (l_{k-1}, l_k)$, где $l_k = r - 1$. Тогда в $\Gamma(\varphi^g)$ имеется путь

$$w[i, nr - 1] = w[l + r\xi, l + rd] \bullet (l + rd, l_1 + r(n - 1)) \bullet w[l_1 + r(n - 1), nr - 1],$$

где d — наибольшее число из D такое, что $d \leq \xi$, а также есть пути $w[l_s + r(n-1), nr-1]$, $s = 1, \dots, k-1$, определённые следующим образом:

$$w[l_s + r(n-1), nr-1] = w[l_s + r(n-1), l_s + rd_q] \\ \bullet (l_s + rd_q, l_{s+1} + r(n-1)) \bullet w[l_{s+1} + r(n-1), nr-1].$$

Здесь $w[l_k + r(n-1), nr-1]$ — пустой путь. Так как

$$\text{len } w[l + r\xi, l + rd] \leq \Delta - 1, \text{ len } w[l_1 + r(n-1), nr-1] = (n - d_q)(k-1),$$

имеем $\text{len } w[i, nr-1] \leq \Delta + (n - d_q)(k-1)$. С учётом леммы 4 получаем

$$\text{len } w[i, nr-1] \leq \Delta + (n - d_q)(\rho - 1) \quad \text{при любом } i \in V(l).$$

Пусть $j \in V(l)$, где $l \in \{0, \dots, r-1\}$, т. е. $j = l + r\xi$, где $0 \leq \xi < n$. Поскольку в графе $\Gamma_E(g)$ имеются дуги (r, u) для $u = 0, \dots, r-1$, в $\Gamma(\varphi^g)$ есть путь

$$w[nr-1, j] = w[nr-1, r-1 + rd_q] \bullet (r-1 + rd_q, l + r(n-1)) \bullet w[l + r(n-1), j],$$

где $\text{len } w[nr-1, j] \leq n - d_q + n - 1$. Следовательно,

$$\exp \Gamma(\varphi^g) \leq \Delta + (n - d_q)\rho + \Phi(L) + n.$$

Теорема 5 доказана.

Следствие 1. Если $d_q = n - 1$ и в $\Gamma_E(g)$ есть дуга $(0, r-1)$, то

$$\exp \Gamma(\varphi^g) \leq \Delta + n. \quad (13)$$

Замечание 2. Для ряда приложений важной характеристикой модифицированного аддитивного генератора является так называемый локальный экспонент [4], определяемый как наименьшее число γ такое, что в орграфе $(\Gamma(\varphi^g)^t)$ при любом $t \geq \gamma$ каждая из r вершин вида $r(n-1), 1 + r(n-1), \dots, nr-1$ инцидентна любой вершине орграфа. Из следствия 1 получаем, что $\gamma \leq \Delta + (n - d_q)\rho + \Phi(L) + 1$. В частности, если $d_q = n - 1$ и в $\Gamma_E(g)$ есть дуга $(0, r-1)$, то $\gamma \leq \Delta + 1$.

ПРИМЕР. Пусть $n = 11$, $r = 32$, $D = \{0, 5, 6, 10\}$. Тогда $\Delta = 5$. В качестве преобразования g множества V_{32} возьмём треугольную подстановку T , заданную системой координатных булевых функций

$$\{g_0(y_0), g_1(y_0, y_1), \dots, g_{31}(y_0, \dots, y_{31})\},$$

где переменная y_0 существенная для $g_{31}(y_0, \dots, y_{31})$. Подстановку регистра сдвига обозначим через φ^T , перемешивающий оргграф — через $\Gamma(\varphi^T)$.

В оргграфе $\Gamma_E(T)$ есть дуга $(0, 31)$, оргграф $\Gamma(\varphi^T)$ примитивный при данных n, r, D . Из формул (12) и (13) получаем $\exp \Gamma(\varphi^T) \leq 16$, а в силу замечания 2 имеем $\gamma \leq 6$.

Сравним (табл. 1) при тех же n и r оценку $\exp \Gamma(\varphi^T)$ по формуле (13) с оценками, вычисленными по формулам (1), (2), относящимся к произвольным примитивным nr -вершинным графам, и по формулам (3), (4) для класса примитивных перемешивающих графов всех подстановочных регистров сдвига длины n над V_r .

Т а б л и ц а 1

Формула	(1)	(2)	(3)	(4)	(13)
$\exp \Gamma(\varphi^T)$	123202	702	4202	702	16

Заметим, что для данного примера в формуле (2) следует положить $l = 1$, а в формуле (4) — $l_1 = 1$. Табл. 1 показывает, что оценка $\exp \Gamma(\varphi^T)$ существенно уточнена с использованием полученных формул.

Заключение. С помощью матрично-графового подхода исследованы перемешивающие свойства преобразований множеств состояний модифицированных аддитивных генераторов. Для перемешивающих оргграфов преобразований описаны множества дуг и контуров, доказаны критерий сильной связности, критерий примитивности и получена оценка экспонента. Для рассмотренного класса оргграфов на примере показана более высокая точность полученной оценки экспонента по сравнению с известными оценками.

ЛИТЕРАТУРА

1. Дорохова А. М., Фомичёв В. М. Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикл. дискрет. математика. 2014. № 1. С. 77–83.
2. Когос К. Г., Фомичёв В. М. Положительные свойства неотрицательных матриц // Прикл. дискрет. математика. 2012. № 4. С. 5–13.
3. Коренева А. М., Фомичёв В. М. Об одном обобщении блочных шифров Фейстеля // Прикл. дискрет. математика. 2012. № 3. С. 34–40.
4. Кяжин С. Н., Фомичёв В. М. Локальная примитивность графов и неотрицательных матриц // Прикл. дискрет. математика. 2014. № 1. С. 68–80.

5. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
6. Фомичёв В. М. Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
7. Фомичёв В. М. Свойства путей в графах и в мультиграфах // Прикл. дискрет. математика. 2010. № 1. С. 118–124.
8. Фомичёв В. М. Оценки экспонентов примитивных графов // Прикл. дискрет. математика. 2011. № 2. С. 101–112.
9. Фомичёв В. М. Оценка экспонента некоторых графов с помощью чисел Фробениуса для трёх аргументов // Прикл. дискрет. математика. 2014. № 2. С. 88–96.
10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные коды на языке Си. М.: Триумф, 2002. 816 с.
11. Kim B. M., Song B. C., Hwang W. Nonnegative primitive matrices with exponent 2 // Linear Algebra Appl. 2005. Vol. 407. P. 162–168.
12. Shader B. L., Suwilo S. Exponents of nonnegative matrix pairs // Linear Algebra Appl. 2003. Vol. 363. P. 275–293.
13. Wielandt H. Unzerlegbare, nicht negative Matrizen // Math. Z. 1950. Bd. 52. S. 642–648.

Коренева Алиса Михайловна,
Фомичёв Владимир Михайлович

Статья поступила
19 февраля 2016 г.
Исправленный вариант —
25 июля 2016 г.

UDC 519.17

DOI: 10.17377/daio.2017.24.528

THE MIXING PROPERTIES OF MODIFIED
ADDITIVE GENERATORSA. M. Koreneva^{1,a} and V. M. Fomichev^{1,2,3,b}¹National Research Nuclear University MEPhI,
31 Kashirskoe Highway, 115409 Moscow, Russia²Financial University under the Government of the Russian Federation,
49 Leningradsky Ave., 125993 Moscow, Russia³Institute of Problems of Informatics (Russian Academy of Sciences),
44-2 Vavilova St., 119333 Moscow, Russia*E-mail:* ^aalisa.koreneva@gmail.com, ^bfomichev@nm.ru

Abstract. We develop a matrix-graph approach to estimating the mixing properties of bijective shift registers over a set of binary vectors. Such shift registers generalize, on the one hand, the class of ciphers based on the Feistel network and, on the other hand, the class of transformations of additive generators (the additive generators are the base for the Fish, Pike, and Mush algorithms). It is worth noting that the original schemes of additive generators are found insecure due to their weak mixing properties. The article contains the results of investigations for the mixing properties of modified additive generators. For the mixing directed graph of a modified additive generator, we define the sets of arcs and cycles, obtain primitivity conditions, and give a bound for the exponent. We show that the determination of parameters for the modified additive generator allows us to achieve a full mixing in a number of iterations that is substantially less than the number of vertices in the mixing digraph. Tab. 1, illustr. 1, bibliogr. 13.

Keywords: additive generator, modified additive generator, mixing digraph, primitive digraph, shift register, exponent of digraph.

REFERENCES

1. A. M. Dorokhova and V. M. Fomichev, Revised values of exponents for mixing graphs of bijective shift registers over a set of binary vectors, *Prikl. Diskretn. Mat.*, No. 1, 77–83, 2014 [Russian].
2. K. G. Kogos and V. M. Fomichev, Positive properties of nonnegative matrices, *Prikl. Diskretn. Mat.*, No. 4, 5–13, 2012 [Russian].
3. A. M. Koreneva and V. M. Fomichev, On a Feistel block cipher generalization, *Prikl. Diskretn. Mat.*, No. 3, 34–40, 2012 [Russian].

4. **S. N. Kyazhin** and **V. M. Fomichev**, Local primitiveness of graphs and nonnegative matrices, *Prikl. Diskretn. Mat.*, No. 3, 68–80, 2014 [Russian].
5. **V. N. Sachkov** and **V. E. Tarakanov**, *Kombinatorika neotritsatel'nykh matrits*, TVP, Moscow, 2000 [Russian]. Translated under the title *Combinatorics of nonnegative matrices*, AMS, Providence, 2002 (Transl. Math. Monogr., Vol. 213).
6. **V. M. Fomichev**, *Metody diskretnoi matematiki v kriptologii* (Methods of Discrete Mathematics in Cryptology), Dialog-MIFI, Moscow, 2010 [Russian].
7. **V. M. Fomichev**, Properties of paths in graphs and multigraphs, *Prikl. Diskretn. Mat.*, No. 1, 118–124, 2010 [Russian].
8. **V. M. Fomichev**, The estimates for exponents of primitive graphs, *Prikl. Diskretn. Mat.*, No. 2, 101–112, 2011 [Russian].
9. **V. M. Fomichev**, Estimates for exponent of some graphs by means of Frobenius's numbers of three arguments, *Prikladn. Diskretn. Matem.*, **24**, No. 2, 88–96, 2014 [Russian].
10. **B. Schneier**, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, New York, 1996. Translated under the title *Prikladnaya kriptografiya: Protokoly, algoritmy, iskhodnye teksty na yazyke Si*, Triumph, Moscow, 2002 [Russian].
11. **B. M. Kim**, **B. C. Song**, and **W. Hwang**, Nonnegative primitive matrices with exponent 2, *Linear Algebra Appl.*, **407**, 162–168, 2005.
12. **B. L. Shader** and **S. Suwilo**, Exponents of nonnegative matrix pairs, *Linear Algebra Appl.*, **363**, 275–293, 2003.
13. **H. Wielandt**, Unzerlegbare, nicht negative Matrizen, *Math. Z.*, **52**, 642–648, 1950 [German].

Alisa M. Koreneva,
Vladimir M. Fomichev

Received
19 February 2016
Revised
25 July 2016