МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.4

БИЕКТИВНЫЕ ОТОБРАЖЕНИЯ, ПОРОЖДАЕМЫЕ ФИЛЬТРУЮЩИМ ГЕНЕРАТОРОМ

М. И. Рожков

Московский институт электроники и математики Национального исследовательского университета «Высшая школа экономики», г. Москва, Россия

E-mail: rozhkov.m.i@yandex.ru

Рассматривается задача построения биективных отображений

$$B_{f,L}\colon (F_2)^n \to (F_2)^n,\ B_{f,L}(x) = (f(x), f(\delta(x)), \ldots, f(\delta^{n-1}(x))),\ x \in (F_2)^n,$$

набор координатных функций которых задаётся преобразованием $\delta = \delta_L$ регистра сдвига большой длины n с функцией обратной связи L и нелинейной функцией выхода f от небольшого числа k аргументов ($k \ll n$). При этом биективность отображения $B_{f,L}$ равносильна ортогональности системы его координатных функций. В работе развивается метод, который сводит исходную задачу проверки биективности отображения $B_{f,L}$ при больших значениях длины регистра n к проверке его биективности применительно к регистрам сдвига ограниченной длины $n \leqslant n_0$, что позволяет эффективно использовать для её решения вычислительную технику. На основе данного метода в работе построены новые бесконечные классы биективных отображений для случая нелинейной функции f, зависящей от $k \leqslant 6$ переменных. Ранее аналогичные результаты были известны для случая, когда функция f зависит от $k = 3$ переменных. Полученные результаты могут быть полезны при построении и обосновании статистических свойств датчиков случайных чисел на основе фильтрующих генераторов. При этом особый практический интерес представляет выбор пар (f, L), при которых одновременно обеспечивается биективность отображения $B_{f,L}$ и максимальность периода отображения δ_L.

Ключевые слова: *ортогональные системы функций, регистр сдвига, фильтрующий генератор, понижающее множество.*

1. Основные понятия и обозначения

Далее в работе будем придерживаться следующих основных понятий и обозначений (используемые алгебраические понятия изложены в [1]):

- F_2 — поле из двух элементов;
- $(f_1, f_2, \ldots, f_m)$ — задание отображения $(F_2)^n \to (F_2)^m$ в виде системы координатных функций;
- $L(x_1, x_2, \ldots, x_n) = L(x_1, x_2, \ldots, x_{s(1)}, x_{n-s(2)+1}, x_{n-s(2)+2}, \ldots, x_n)$ — функция обратной связи регистра сдвига длины $n \geqslant s(1) + s(2)$, линейная по переменной x_1, ($s(1) \geqslant 1$, $s(2) \geqslant 0$ — заданные параметры);
- $\delta = \delta_L$ — преобразование векторов пространства $(F_2)^n$, осуществляемое регистром сдвига с функцией обратной связи $L(x_1, x_2, \ldots, x_n)$, действующее на вектор

$(x_1, x_2, \ldots, x_n) \in (F_2)^n$ по правилу

$$\delta(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, L(x_1, x_2, \ldots, x_n));$$

— $f(x_1, x_2, \ldots, x_k)$ — функция от k аргументов без запретов (являющаяся фильтрующей функцией съёма с соответствующего регистра сдвига);
— $B_{f,L}$ — преобразование двоичных векторов длины n (отображение $(F_2)^n \to (F_2)^n$), задаваемое системой координатных функций

$$B_{f,L} = (f(x), f(\delta(x)), \ldots, f(\delta^{n-1}(x))), \quad x \in (F_2)^n.$$

В работе рассматриваются вопросы выбора нелинейной функции съёма f и функции обратной связи L, при которых преобразование $B_{f,L}$ является биективным. При этом биективность преобразования $B_{f,L}$ равносильна ортогональности системы его координатных функций [2]. В [2] показано, что при $n \geqslant 2^{k-1} + k - 1$ отсутствие запретов у функции $f = f(x_1, x_2, \ldots, x_k)$ является необходимым условием биективности отображения $B_{f,L}$ (функции без запрета называют также функциями без потери информации, сильно равновероятными и совершенно уравновешенными [3–5]).

Известно [4], что для функции без запретов $f(x_1, x_2, \ldots, x_k)$ при любом натуральном n существует ровно 2^{k-1} входных слов $x_1, x_2, \ldots, x_{n+k-1}$, перерабатываемых данной функцией в любое фиксированное выходное слово $y(1), y(2), \ldots, y(n)$ по закону

$$y(j) = f(x_j, x_{j+1}, \ldots, x_{j+k-1}), \quad j = 1, 2, \ldots, n.$$

Поэтому биективность преобразования $B_{f,L}$ равносильна тому, что среди этих 2^{k-1} входных слов ровно одно слово будет удовлетворять ограничениям

$$x_{n+1} = L(x) = L(x_1, x_2, \ldots, x_n),\ x_{n+2} = L(\delta_L(x)),\ \ldots,\ x_{n+k-1} = L((\delta_L)^{k-2}(x)). \qquad (1)$$

При этом $x_{n+1}, x_{n+2}, \ldots, x_{n+k-1}$ как функции от независимых переменных $x_1, x_2, \ldots, x_n$ (в силу ограничений на вид функции обратной связи L) зависят лишь от $k + s(1) - 2$ начальных переменных и от $s(2)$ последних переменных. Таким образом, выполняется ограничение 1 или нет для данного входного слова $x_1, x_2, \ldots, x_{n+k-1}$, зависит только от его начального отрезка $x_1, x_2, \ldots, x_{k+s(1)-2}$ длины $k + s(1) - 2$ и конечного отрезка $x_{n-s(2)+1}, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+k-1}$ длины $k + s(2) - 1$.

Для заданных функции $f(x_1, x_2, \ldots, x_k)$, натуральных $r, s \geqslant k - 1$ и выходного слова $Y = y(1), y(2), \ldots, y(m)$ через $I = I(Y) = I_{r,s}(Y)$ обозначим систему пар векторов $\left(\alpha^{(i)}, \beta^{(i)}\right), i = 1, 2, \ldots, 2^{k-1}$, где $\alpha^{(i)} = x_1, x_2, \ldots, x_r$ и $\beta^{(i)} = x_{m+k-s}$, $x_{m+k-s+1}, \ldots, x_{m+k-1}$ являются соответственно началами и концами входных слов $X = x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_{k+m-1}$, перерабатываемых функцией f в выходное слово Y:

$$y(j) = f(x_j, x_{j+1}, \ldots, x_{j+k-1}), \quad j = 1, 2, \ldots, m.$$

Так как число различных входов X, отвечающих заданному выходу Y, в точности равно 2^{k-1}, то полагаем, что $I(Y)$ состоит из 2^{k-1} элементов. При этом соответствующие системы $I(Y)$ и $I(Z)$ считаем равными ($I(Y) = I(Z)$), если любой элемент $(\alpha, \beta) \in I(Y)$ встречается в $I(Z)$ ровно столько раз, сколько он встречается в $I(Y)$.

Определение 1. Двоичные последовательности $Y = y(1), y(2), \ldots, y(n)$ и $Z = z(1), z(2), \ldots, z(m)$ назовём эквивалентными (обозначим $Y \sim Z$), если $I_{k-1,k-1}(Y) = I_{k-1,k-1}(Z)$.

Пример 1. Для функции от трёх переменных $f(x_1, x_2, x_3) = x_1x_2 + x_2 + x_3$ выходным словам $Y_1 = (y(1), y(2), y(3), y(4)) = (0, 0, 0, 0)$ и $Z_1 = (z(1), z(2), z(3)) = (0, 0, 0)$ соответствуют следующие наборы входных слов:

(0,0,0,0,0,0), (1,0,0,0,0,0), (0,1,1,0,0,0), (1,1,0,0,0,0) для Y_1,
(0,0,0,0,0), (1,0,0,0,0), (0,1,1,0,0), (1,1,0,0,0) для Z_1.

Начала и окончания длины 2 входных векторов свидетельствуют, что

$$I_{2,2}(Y_1) = I_{2,2}(Z_1) = \{(00, 00), (10, 00), (01, 00), (11, 00)\}.$$

Следовательно, слова Y_1 и Z_1 являются эквивалентными. Аналогичным образом можно убедиться, что эквивалентны также слова $Y_2 = (0, 1, 0, 1, 0, 1)$ и $Z_2 = (0, 1)$, для которых

$$I_{2,2}(Y_2) = I_{2,2}(Z_2) = \{(00, 01), (10, 01), (01, 11), (11, 01)\}.$$

Определение 2. Упорядоченное множество натуральных чисел $\{h, t_1, t_2, \ldots, t_\theta\}$, $h > t_1 > \ldots > t_\theta$, $\theta \geqslant 1$, назовём *понижающим для функции* $f(x_1, x_2, \ldots, x_k)$, если для любой последовательности Y длины h найдётся эквивалентная ей последовательность Z длины $t \in \{t_1, t_2, \ldots, t_\theta\}$. Понижающее множество $\{h, t_1, t_2, \ldots, t_\theta\}$ называем *равновесным*, если для любого $t \in \{t_1, t_2, \ldots, t_\theta\}$ и любой последовательности Y длины t найдётся эквивалентная ей последовательность длины h. Понижающее множество $\{h, t\}$, состоящее из двух элементов, будем также называть *понижающей парой* и обозначать (h, t).

Пример 2. Для функции от двух переменных $f(x_1, x_2) = x_1 + x_2$ выходным словам Y длины 1 и 2 соответствуют следующие множества входов: слову $0 — \{(0, 0), (1, 1)\}$, слову $1 — \{(0, 1), (1, 0)\}$, слову $00 — \{(0, 0, 0), (1, 1, 1)\}$, слову $10 — \{(0, 1, 1), (1, 0, 0)\}$, слову $01 — \{(0, 0, 1), (1, 1, 0)\}$, слову $11 — \{(0, 1, 0), (1, 0, 1)\}$. Отсюда получаем

$$I_{1,1}(Y = 0) \cup I_{1,1}(Y = 1) = \{\{(0, 0), (1, 1)\}, \{(0, 1), (1, 0)\}\};$$
$$I_{1,1}(Y = 00) \cup I_{1,1}(Y = 10) \cup I_{1,1}(Y = 01) \cup I_{1,1}(Y = 11) = \{\{(0, 0), (1, 1)\}, \{(0, 1), (1, 0)\}\}.$$

Следовательно, для рассматриваемой функции множество $(h, t) = (2, 1)$ является равновесной понижающей парой.

Определение 3. *Длиной* (*расстоянием*) *эквивалентности* для заданной функции без запретов $f = f(x_1, x_2, \ldots, x_k)$ назовём натуральное число n_0, при котором любое слово длины $n > n_0$ эквивалентно некоторому слову длины $\leqslant n_0$.

Для функции из примера 2 расстояние эквивалентности, очевидно, равно 1.

Заметим, что если n_0 — длина эквивалентности функции f, то и любое $n > n_0$ также является её длиной эквивалентности. Кроме того, непосредственно из определения 3 вытекает: если n_0 — длина эквивалентности функции f, то множество

$$\{n_0 + 1, n_0, n_0 - 1, \ldots, 2, 1\}$$

является для данной функции понижающим.

2. Вспомогательные утверждения

Лемма 1. Пусть $r, s \geqslant k-1$, $I_{r,s}(Y) = I_{r,s}(Z)$, $\varepsilon \in \{0,1\}$, $Y1 = \varepsilon Y$, $Z1 = \varepsilon Z$, $Y2 = Y\varepsilon$, $Z2 = Z\varepsilon$. Тогда $I_{r+1,s}(Y1) = I_{r+1,s}(Z1)$, $I_{r,s+1}(Y2) = I_{r,s+1}(Z2)$.

Доказательство. Пусть $X = x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_{k+n-1}$ — произвольное входное слово, соответствующее выходному слову Y длины $|Y| = n$. Тогда входные слова, соответствующие выходному слову $Y2 = Y\varepsilon$, имеют следующий вид:

1) $X\sigma$, если имеется единственное значение $\sigma \in \{0,1\}$, для которого

$$f(x_{n+1}, \ldots, x_{n+k-1}, \sigma) = \varepsilon;$$

2) $X0, X1$, если $f(x_{n+1}, \ldots, x_{n+k-1}, 0) = f(x_{n+1}, \ldots, x_{n+k-1}, 1) = \varepsilon$;
3) таких входных слов не существует, если

$$f(x_{n+1}, \ldots, x_{n+k-1}, 0) = f(x_{n+1}, \ldots, x_{n+k-1}, 1) \neq \varepsilon.$$

Отсюда вытекает справедливость леммы для пары $Y2, Z2$. Аналогичным образом проводится доказательство и для пары $Y1, Z1$. ■

Лемма 2. Пусть $f(x_1, x_2, \ldots, x_k) = \varphi(x_1, x_2, \ldots, x_{k-1}) + x_k$. Двоичные последовательности $y(1), y(2), \ldots, y(n)$ и $z(1), z(2), \ldots, z(m)$ являются эквивалентными, если и только если при любом $\alpha \in (F_2)^{k-1}$

$$\delta_{y(n)}\delta_{y(n-1)} \ldots \delta_{y(1)}(\alpha) = \delta_{z(m)}\delta_{z(m-1)} \ldots \delta_{z(1)}(\alpha),$$

где $\delta_\varepsilon(x_1, x_2, \ldots, x_{k-1}) = (x_2, x_3, \ldots, x_{k-1}, \varphi(x_1, x_2, \ldots, x_{k-1}) + \varepsilon)$.

Доказательство. Для функции $f(x_1, x_2, \ldots, x_k) = \varphi(x_1, x_2, \ldots, x_{k-1}) + x_k$ слова $X = x_1, x_2, \ldots, x_{n+k-1}$, перерабатываемые этой функцией в фиксированное выходное слово $y(1), y(2), \ldots, y(n)$, $y(j) = f(x_j, x_{j+1}, \ldots, x_{j+k-1})$, $j = 1, 2, \ldots, n$, задаются последовательностью векторов

$$\begin{gathered}
\alpha_0 = (x_1, x_2, \ldots, x_{k-1}), \\
\alpha_1 = (x_2, x_3, \ldots, x_k),\ x_k = \varphi(\alpha_0) + y(1)\ \Rightarrow \alpha_1 = \delta_{y(1)}(\alpha_0), \\
\ldots \\
\alpha_n = (x_{n+1}, x_{n+2}, \ldots, x_{n+k-1}),\ x_{n+k-1} = \varphi(\alpha_{n-1}) + y(n)\ \Rightarrow \alpha_n = \delta_{y(n)}(\alpha_{n-1}).
\end{gathered}$$

Отсюда и получаем утверждение леммы. ■

Лемма 3. Пусть $\{h, t_1, t_2, \ldots, t_\theta\}$ — понижающее множество. Тогда

1. При любом натуральном ε множество $\{h+\varepsilon, t_1+\varepsilon, t_2+\varepsilon, \ldots, t_\theta+\varepsilon\}$ также является понижающим. При этом оно будет равновесным, если таким является исходное множество.

2. При любом фиксированном $n_0 \geqslant t_\theta$ произвольное слово $Y = y(1), y(2), \ldots, y(n)$ длины $n \geqslant n_0$ эквивалентно некоторому слову длины $t \in \{n_0, n_0+1, \ldots, n_0+h-t_\theta-1\}$.

Доказательство. С учётом леммы 1 доказательство первой части леммы 3 легко проводится индукцией по ε. Докажем вторую часть. Пусть произвольное заданное слово $Y = y(1), y(2), \ldots, y(n)$ длины $n \geqslant n_0$ эквивалентно некоторому слову $Z = z(1), z(2), \ldots, z(t)$ длины $t \in \{n_0, n_0+1, \ldots, n_0+h-t_\theta-1\}$. Тогда слово $Y_1 = (y(1), y(2), \ldots, y(n), a) = Ya$ эквивалентно слову $Z_1 = Za$, длина которого

принадлежит множеству $\{n_0+1, n_0+2, \ldots, n_0+h-t_\theta\}$. Далее достаточно рассмотреть случай, когда длина слова Z_1 равна $t = n_0+h-t_\theta$. Слово Z_1 можно представить в виде $Z_1 = VW$, где V — начало слова Z_1 (длины $(n_0-t_\theta) \geqslant 0$), а W — его окончание длиной h. Тогда слово W эквивалентно некоторому слову W_1 длины $t \in \{t_1, t_2, \ldots, t_\theta\}$. Значит, слово $Z_1 = VW$ эквивалентно слову VW_1, длина которого равна $(n_0-t_\theta+t) \in \{n_0, n_0+1, \ldots, n_0+t_1-t_\theta\}$. Так как $n_0+t_1-t_\theta < n_0+h-t_\theta$, то утверждение леммы верно и для слов дины $n+1$. ■

3. Оценка длины эквивалентности

Утверждение 1. Пусть $f = f(x_1, x_2, \ldots, x_k)$ — произвольная двоичная функция без запретов от k переменных. Тогда её минимальная длина эквивалентности не превосходит величины $n_0 = \begin{pmatrix} 2^{2(k-1)}+2^{k-1}-1 \\ 2^{k-1} \end{pmatrix} - 1$.

Доказательство. Через I_s обозначим множество $\cup I_{k-1,k-1}(Y)$, где объединение производится по всем словам Y длины s. Система $I_{k-1,k-1}(Y)$, соответствующая слову Y длины n, которое не имеет эквивалентных слов меньшей длины, очевидно, не принадлежит множеству $\cup I_{k-1,k-1}(Z)$, где объединение производится по всем словам Z длины меньше n (системы $I(Y)$ и $I(Z)$ при этом рассматриваются как отдельные элементы соответствующих объединений). В таком случае, учитывая очевидное равенство $|I_1| = 2$, получим соотношение

$$|\cup I_s| \geqslant |I_1| + \omega - 1 = \omega + 1. \tag{2}$$

(объединение по $s = 1, 2, \ldots, \omega$, которые не являются длиной эквивалентности). Заметим далее, что общее число различных систем вида $I_{k-1,k-1}(Y)$ не превосходит числа вариантов выбора 2^{k-1} элементов из множества пар $(\alpha^{(i)}, \beta^{(i)})$, $\alpha^{(i)}, \beta^{(i)} \in (F_2)^{k-1}$, т. е. числа сочетаний с повторениями из $2^{2(k-1)}$ элементов по 2^{k-1}. С учётом (2) отсюда получаем, что при

$$\omega = \begin{pmatrix} 2^{2(k-1)}+2^{k-1}-1 \\ 2^{k-1} \end{pmatrix}$$

любое слово длины $\geqslant \omega$ эквивалентно некоторому слову длины $< \omega$. ■

Из данного утверждения вытекает, что длина эквивалентности имеется у любой двоичной функции без запретов. При этом важной задачей является нахождение минимальной длины эквивалентности.

Утверждение 2. Пусть функция без запретов от k переменных линейна по последней переменной: $f(x_1, x_2, \ldots, x_k) = \varphi(x_1, x_2, \ldots, x_{k-1}) + x_k$. Тогда её минимальная длина эквивалентности не превосходит величины $n_0 = d^d - 1$, $d = 2^{k-1}$.

Доказательство. В условиях данного утверждения (с учётом леммы 2) двоичные последовательности $y(1), y(2), \ldots, y(n)$ и $z(1), z(2), \ldots, z(m)$ являются эквивалентными, если и только если при любом $\alpha \in (F_2)^{k-1}$

$$\delta_{y(n)}\delta_{y(n-1)} \ldots \delta_{y(1)}(\alpha) = \delta_{z(m)}\delta_{z(m-1)} \ldots \delta_{z(1)}(\alpha),$$

где $\delta_\varepsilon(x_1, x_2, \ldots, x_{k-1}) = (x_2, x_3, \ldots, x_{k-1}, \varphi(x_1, x_2, \ldots, x_{k-1}) + \varepsilon)$. Число различных систем $I_{k-1,k-1}(Y)$ не превосходит числа отображений множества $(F_2)^{k-1}$ в себя, которое равно d^d, $d = 2^{k-1}$. С учётом неравенства (2) отсюда и вытекает справедливость утверждения. ■

Утверждение 3. Пусть функция без запретов от k переменных линейна по обеим крайним переменным: $f(x_1, x_2, \ldots, x_k) = x_1 + \lambda(x_2, x_3, \ldots, x_{k-1}) + x_k$. Тогда её минимальная длина эквивалентности не превосходит величины $n_0 = (2^{k-1})! - 1$.

Доказательство проводится по аналогичной схеме с учётом того, что в условиях данного утверждения отображения δ_0 и δ_1 являются биективными, а число биективных отображений множества $(F_2)^{k-1}$ в себя равно $(2^{k-1})!$.

Замечание 1. Если функция линейна по обеим крайним переменным, то её длина эквивалентности, очевидно, связана с известными понятиями длины (и ширины) покрытия группы G, порождённой подстановками δ_0 и δ_1 [6].

Утверждение 4. Для любой двоичной функции без запретов от k переменных существует равновесная понижающая пара (h, t), $t < h \leqslant H$, где $H = 2^n$, $n = \begin{pmatrix} 2^{2(k-1)} + 2^{k-1} - 1 \\ 2^{k-1} \end{pmatrix}$.

Доказательство. Рассмотрим последовательность $I_1, I_2, \ldots$ множеств, введённых в доказательстве утверждения 1. Как уже отмечалось при доказательстве утверждения 1, множество I_s при любом $s = 1, 2, \ldots$ является непустым подмножеством конечного множества M, мощность которого не превосходит величины $n = \begin{pmatrix} 2^{2(k-1)} + 2^{k-1} - 1 \\ 2^{k-1} \end{pmatrix}$. Следовательно, найдутся два индекса $h > t$, при которых $I_h = I_t$. При этом индекс h можно выбрать так, что он не превосходит числа всех подмножеств множества M, т. е. величины $H = 2^n$. ■

Замечание 2. Аналогичными рассуждениями можно показать, что если функция f удовлетворяет условиям утверждений 2 или 3, то она обладает равновесной понижающей парой (h, t), $t < h \leqslant 2^n$, где $n = d^d$, $d = 2^{k-1}$ в условиях утверждения 2 и $n = (2^{k-1})!$ — в условиях утверждения 3.

Для заданной функции без запретов f через $O(f)$ обозначим множество функций

$$\{f(x), f(x)+1, f(x+e), f(x+e)+1, f(s(x)), f(s(x))+1, f(s(x)+e), f(s(x)+e)+1\},$$

где e — двоичный вектор с единичными координатами (преобразование $x + e$ заключается в инвертировании координат двоичного вектора x); $s(x) = s(x_1, x_2, \ldots, x_k) = (x_k, x_{k-1}, \ldots, x_1)$.

Утверждение 5. Пусть функция без запрета $f(x_1, x_2, \ldots, x_k)$ обладает равновесной понижающей парой (H, T). Тогда (H, T) является равновесной понижающей парой для любой функции $\varphi \in O(f)$.

Доказательство. Для заданной функции без запрета $f(x_1, x_2, \ldots, x_k)$ и выходного слова $Y = (y(1), y(2), \ldots, y(n))$ через $f^{-1}(Y)$ обозначим множество входных слов

$$f^{-1}(Y) = \{x_1(j), x_2(j), \ldots, x_{n+k-1}(j) : j = 1, 2, \ldots, 2^{k-1}\},$$

перерабатываемых функцией f в слово Y:

$$y(t) = f(x_t(j), x_{t+1}(j), \ldots, x_{t+k-1}(j)), \quad t = 1, 2, \ldots, n; \quad j = 1, 2, \ldots, 2^{k-1}.$$

Пусть $\varphi(x) = f(x + e)$. Тогда для любого слова Y множество векторов $\varphi^{-1}(Y)$ получено из векторов множества $f^{-1}(Y)$ путём их инвертирования. Следовательно, слова Y и Z эквивалентны относительно функции f в том и только в том случае,

если они эквивалентны относительно функции φ. А значит, если пара (H, T) является понижающей для функции f, то она будет понижающей и для функции φ.

Пусть $\varphi(x) = f(s(x))$. Для заданного слова $Y = (y(1), y(2), \ldots, y(n))$ через $Y^* = (y(n), y(n-1), \ldots, y(1))$ будем обозначать слово, полученное выписыванием в обратном порядке координат вектора Y. Соответственно через $f^{-1}(Y)^*$ обозначим множество двоичных последовательностей, полученных выписыванием в обратном порядке элементов последовательностей, содержащихся в множестве $f^{-1}(Y)$. Заметим, что $f^{-1}(Y)^* = \varphi^{-1}(Y^*)$. Значит, слово Y длины H эквивалентно слову Z длины T относительно функции f в том и только в том случае, когда слово Y эквивалентно слову Z относительно функции φ. Значит, пара (H, T) является понижающей для функции φ.

Пусть $\varphi(x) = f(x)+1$. Тогда $\varphi^{-1}(Y+e) = f^{-1}(Y)$. Значит, слова Y и Z эквивалентны относительно функции f в том и только в том случае, если слова $(Y + e)$ и $(Z + e)$ эквивалентны относительно функции φ. А значит, пара (H, T) будет понижающей и для функции φ. Оставшиеся варианты рассматриваются по аналогичной схеме. ■

4. Условия биективности отображений $B_{f,L}$

Теорема 1. Пусть $\{h, t_1, t_2, \ldots, t_\theta\}$ — понижающее множество для функции $f(x_1, x_2, \ldots, x_k)$, $n_0 \geqslant t_\theta + s(1) + s(2) - 1$. Если отображение $B_{f,L}$ является биективным для всех $n \in \{n_0, n_0 + 1, \ldots, n_0 + h - t_\theta - 1\}$, то оно биективно при любом $n \geqslant n_0$.

Доказательство. Для функции без запретов $f(x_1, x_2, \ldots, x_k)$ существует ровно 2^{k-1} входных слов $x_1, x_2, \ldots, x_{n+k-1}$, перерабатываемых данной функцией в фиксированное выходное слово $Y = y(1), y(2), \ldots, y(n)$ по закону $y(j) = f(x_j, x_{j+1}, \ldots, x_{j+k-1})$, $j = 1, 2, \ldots, n$. Биективность отображения $B_{f,L}$ равносильна тому, что любому фиксированному выходному слову $y(1), y(2), \ldots, y(n)$ соответствует единственное входное слово $x_1, x_2, \ldots, x_{n+k-1}$ с ограничениями (1). Заметим, что выполнение (или невыполнение) условий (1) для входного слова зависит только от его начала $x_1, x_2, \ldots, x_{k+s(1)-2}$ длины $k + s(1) - 2$ и конца $x_{n-s(2)+1}, x_{n-s(2)+2}, \ldots, x_{n+k-1}$ длины $k + s(2) - 1$. С учётом леммы 3 в условиях теоремы для любого слова $Y = y(1), y(2), \ldots, y(n)$ длины $n \geqslant n_0$ найдётся эквивалентное ему слово $Z = z(1), z(2), \ldots, z(n_0)$, имеющее такие же начальный и конечный отрезки длины $s(1) - 1$ и $s(2)$:

$$y(j) = z(j), j \in \{1, 2, \ldots, s(1) - 1\}, \quad y(n + 1 - j) = z(n_0 + 1 - j), j \in \{1, 2, \ldots, s(2)\}.$$

В таком случае у этих слов одинаковы системы $I_{r,s}(Y) = I_{r,s}(Z)$ для $r = k + s(1) - 2$, $s = k + s(2) - 1$. Следовательно, и условия (1) применительно к данным последовательностям одновременно выполнены или нет. ■

Теорема 2. Пусть (h, t) — равновесная понижающая пара, $n_0 \geqslant t + s(1) + s(2) - 1$.

1) Если отображение$B_{f,L}$ является биекцией для $n = n_0$, то оно является биекцией при всех $n = n_0 + (h - t)d$, $d = 0, 1, \ldots$
2) Если отображение$B_{f,L}$ не является биекцией для $n = n_0$, то оно не является биекцией ни при каком $n = n_0 + (h - t)d$, $d = 0, 1, \ldots$
3) Задача нахождения биективных отображений $B_{f,L}$ при всех $n \geqslant t+s(1)+s(2)-1$ эквивалентна задаче нахождения биективных отображений $B_{f,L}$ при $n = n_0 \in \in \{t + s(1) + s(2) - 1, t + s(1) + s(2), \ldots, h + s(1) + s(2) - 2\}$.

Доказательство. Доказательство части 1 и 2 теоремы. Используя рассуждения, аналогичные доказательству теоремы 1, получим, что в условиях теоремы 2 для любого слова $Y = y(1), y(2), \ldots, y(n)$ найдется слово $Z = z(1), z(2), \ldots, z(n_0)$, при котором $I_{r,s}(Y) = I_{r,s}(Z)$, $r = k + s(1) - 2, s = k + s(2) - 1$. Таким образом, если для выходного

слова $z(1), z(2), \ldots, z(m)$ длины $m = n_0$ существует единственное входное слово с ограничениями (1), то это верно и для слова $y(1), y(2), \ldots, y(n)$ длины $n = n_0 + (h-t)d$. С другой стороны, пусть для некоторого выходного слова $Z = z(1), z(2), \ldots, z(m)$ длины $m = n_0$ нарушено условие единственности входного слова $x_1, x_2, \ldots, x_{m+k-1}$ с ограничениями (1). Тогда в силу равновесности понижающей пары (h, t) для слова Z найдётся слово $Y = y(1), y(2), \ldots, y(n)$ длины $n = n_0 + (h-t)d$, такое, что $I_{r,s}(Y) = I_{r,s}(Z)$, $r = k + s(1) - 2$, $s = k + s(2) - 1$. Следовательно, для слова Y также нарушено условие единственности входного слова $x_1, x_2, \ldots, x_{n+k-1}$ с ограничениями (1). На этом доказательство частей 1 и 2 завершено. Справедливость третьей части вытекает из доказанных частей 1, 2 с учётом того, что в условиях теоремы любое натуральное число $n \geqslant t + s(1) + s(2) - 1$ представимо в виде

$$n = n_0 + (h-t)d, d \in \{0, 1, \ldots\}, n_0 \in \{t+s(1)+s(2)-1, t+s(1)+s(2), \ldots, h+s(1)+s(2)-2\}.$$

Теорема доказана. ■

Таким образом, наличие понижающего множества для функции $f(x_1, x_2, \ldots, x_k)$ в принципиальном плане сводит вопрос о биективности отображений $B_{f,L}$ для всех достаточно больших n к исследованию соответствующих отображений при ограниченных значениях n. Особенно ярко это проявляется для понижающей пары (h, t) при $h = t+1$. В этом случае биективность $B_{f,L}$ для $n = n_0 = t + s(1) + s(2) - 1$ равносильна его биективности при любом $n \geqslant n_0$.

5. Преобразования, сохраняющие биективность отображения $B_{f,L}$

Рассмотрим преобразования исходных функций (f, L), при которых сохраняется биективность отображения $B_{f,L}$. Так, например, при биективности $B_{f,L}$ биективным будет и отображение $B_{f+1,L}$. Кроме того, биективным будет и отображение $B_{g,L}$, где $g(x) = f((\delta_L)^j(x)), j \in \{1, 2, \ldots\}$.

Утверждение 6. Пусть при $f = f(x_1, x_2, \ldots, x_n)$ и $L = x_1 + L_0(x_2, x_3, \ldots, x_n)$ отображение $B_{f,L}$ является биективным. Тогда биективно и отображение $B_{g,H}$, где $g = f(x_1 + 1, x_2 + 1, \ldots, x_n + 1)$, $H = x_1 + L_0(x_2 + 1, x_3 + 1, \ldots, x_n + 1)$.

Доказательство. Справедливость утверждения вытекает из легко проверяемого равенства $\tau\delta_L^{-1}\tau^{-1} = \delta_H$, где преобразование τ заключается в инвертировании всех координат двоичного вектора. ■

Утверждение 7. Пусть при $f = f(x_1, x_2, \ldots, x_k)$ и $L = x_1 + L_0(x_2, x_3, \ldots, x_n)$, $k \leqslant n$, отображение $B_{f,L}$ является биективным. Тогда биективно и отображение $B_{g,H}$, где $g = f(x_k, x_{k-1}, \ldots, x_1)$, $H = x_1 + L_0(x_n, x_{n-1}, \ldots, x_2)$.

Доказательство. Рассмотрим случай $k = n$. В силу биективности отображения δ_L система функций $\{f(x), f((\delta_L)(x)), \ldots, f((\delta_L)^{n-1}(x))\}$ будет ортогональной в том и только в том случае, когда такой будет система функций

$$\{z_1 = f((\delta_L)^{-1}(sx)), z_2 = f(sx), z_3 = f((\delta_L)(sx)), \ldots, z_n = f((\delta_L)^{n-2}(sx))\},$$

где $s\colon (F_2)^n \to (F_2)^n, s(x_1, x_2, \ldots, x_n) = (x_n, x_{n-1}, \ldots, x_1)$. Из равенства $s\delta_L s^{-1} = (\delta_H)^{-1}$ следует, что

$$z_1 = f((\delta_L)^{-1})s(x)) = f(s\delta_H(x)) = g(\delta_H(x)),$$
$$z_2 = f(s(x)) = g(x),$$

$$z_3 = f((\delta_L)s(x)) = f(s(\delta_H)^{-1}(x)) = g((\delta_H)^{-1}(x)),$$
$$\dots$$
$$z_n = f((\delta_L)^{n-2}s(x)) = f(s(\delta_H)^{-n+2}(x)) = g((\delta_H)^{-n+2}(x)).$$

Далее из ортогональности системы $\{z_1(x), z_2(x), \dots, z_n(x)\}$ следует ортогональность системы $\{z_1(B(x)), z_2(B(x)), \dots, z_n(B(x))\}$, где B — произвольная биекция на множестве векторов $(F_2)^n$. В частности, при $B = (\delta_H)^{n-2}$ получаем ортогональность системы $\{g((\delta_H)^{n-1}(x)), \dots, g(\delta_H(x)), g(x)\}$. Поскольку свойство ортогональности системы функций не зависит от порядка следования функций, на этом доказательство утверждения для $k = n$ завершено.

Пусть теперь $k < n$. Рассматривая функцию $f(x_1, x_2, \dots, x_k)$ как функцию от n переменных $x_1, x_2, \dots, x_n$, из доказанного выше получаем биективность отображения $B_{\varphi,H}$, где $\varphi = f(x_n, x_{n-1}, \dots, x_{n-k+1})$. В таком случае биективно и $B_{g,H}$, где $g = \varphi((\delta_H)^{n-k}(x)) = f(x_k, x_{k-1}, \dots, x_1)$, что и завершает доказательство. ■

6. Случай $k = 3$

Для заданной понижающей пары (h, t) и параметров $s(1), s(2)$ через M будем обозначать множество

$$M = \{t + s(1) + s(2) - 1, t + s(1) + s(2), \dots, h + s(1) + s(2) - 2\}.$$

Так как функции без запрета от трёх переменных $f(x_1, x_2, x_3)$ являются линейными по одной из крайних переменных, то с учётом утверждения 5 множество понижающих пар нелинейных функций задаётся понижающими парами (h, t) функции $f_1 = x_1x_2 + +x_2 + x_3$, для которой $(h, t) = (6, 4)$, и функции $f_2 = x_1x_2 + x_3$, для которой $(h, t) = (11, 8)$. Для пары функций $f = x_1x_2 + x_2 + x_3$, $L = x_1 + x_{n-1}$ экспериментальными расчётами установлена биективность отображения $B_{f,L}$ при $n = 7 \in M = \{6, 7\}$. Следовательно, по теореме 2 отображение $B_{f,L}$ с указанными функциями f, L биективно при всех нечётных $n \geqslant 7$. Аналогичный результат другими методами ранее получен в [7].

7. Случай $k = 4$

Экспериментальные исследования на ЭВМ привели к нахождению биективных отображений $B_{f,L}$ для некоторых ограниченных значений $n = n_0 \in M$. С учётом теоремы 2 это позволило построить бесконечные перечни длин регистра, при которых биективно отображение $B_{f,L}$. В частности, биективные отображения исследуемого вида найдены для следующих четырёх функций f и соответствующих функций L :

$$\begin{aligned}
f_1 &= x_1 + x_4 + x_1x_2 + x_1x_3 + x_1x_2x_3, && L = x_1 + x_n;\\
f_2 &= x_3 + x_4 + x_1x_3 + x_2x_3 + x_1x_2x_3, && L \in \{x_1 + x_{n-2}, x_1 + x_n\};\\
f_3 &= x_4 + x_1x_2 + x_1x_3 + x_2x_3, && L = x_1 + x_{n-1};\\
f_4 &= x_2 + x_3 + x_1x_3 + x_3x_4 + x_1x_3x_4, && L = x_1 + x_{n-2}.
\end{aligned}$$

Общие характеристики функций f и L, значения $n = n_0 \in M$, а также бесконечные перечни длин регистра, при которых биективно отображение $B_{f,L}$, приведены в табл. 1.

Таблица 1

Параметры биекций $B_{f,L}$, f от четырёх переменных

$f(x)$	$L(x)$	$s(1)$	$s(2)$	(h,t)	$n=n_0\in M$ ($B_{f,L}$ — биекция)	Бесконечный перечень длин регистра ($B_{f,L}$ — биекция)
f_1	x_1+x_n	1	1	(9, 6)	$n_0=8$	$n\equiv 2 \mod 3,\ n\geqslant 8$
f_2	x_1+x_{n-2}	1	3	(8, 5)	$n_0=10$	$n\equiv 1 \mod 3,\ n\geqslant 10$
f_2	x_1+x_n	1	1	(8, 5)	$n_0=8$	$n\equiv 2 \mod 3,\ n\geqslant 8$
f_3	x_1+x_{n-1}	1	2	(12, 8)	$n_0=11,13$	$n\equiv 1 \mod 2,\ n\geqslant 11$
f_4	x_1+x_{n-2}	1	3	(6, 5)	$n_0=8$	$n\geqslant 8$

8. Случай $k=5$

Примеры функций от пяти переменных и соответствующие им бесконечные классы биекций $B_{f,L}$ приведены в табл. 2 и 3.

Таблица 2

Перечень функций f от пяти переменных, для которых найдены биекции $B_{f,L}$

$f(x)=f(x_0,x_1,x_2,x_3,x_4)$
$f_1=x_0x_3+x_0x_2x_3+x_4$
$f_2=x_1+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_2x_3+x_4$
$f_3=x_1x_3+x_0x_1x_3+x_4$
$f_4=x_0x_3+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3+x_4$
$f_5=x_0+x_3+x_0x_1+x_0x_2+x_0x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3+x_4$
$f_6=x_2+x_3+x_0x_2+x_1x_2+x_1x_3+x_0x_1x_2+x_4$
$f_7=x_0+x_3+x_0x_1+x_0x_2+x_0x_4+x_0x_1x_2+x_0x_1x_4+x_0x_2x_4+x_0x_1x_2x_4$
$f_8=x_3+x_2x_4+x_0x_2x_4+x_1x_2x_4+x_0x_1x_2x_4$
$f_9=x_3+x_0x_4+x_0x_1x_4$
$f_{10}=x_2+x_3+x_0x_3+x_1x_3+x_3x_4+x_0x_1x_3+x_0x_3x_4+x_1x_3x_4+x_0x_1x_3x_4$
$f_{11}=x_1+x_0x_2+x_1x_2+x_2x_3+x_2x_4+x_3x_4+x_0x_2x_3+x_0x_2x_4+x_0x_3x_4+$ $x_1x_2x_3+x_1x_2x_4+x_1x_3x_4$
$f_{12}=x_3+x_0x_1+x_1x_4+x_0x_1x_2+x_0x_1x_4+x_1x_2x_4+x_0x_1x_2x_4$

Таблица 3

Параметры биекций $B_{f,L}$, f от пяти переменных

$f(x)$	$L(x)$	$s(1)$	$s(2)$	(h,t)	$n=n_0\in M$ ($B_{f,L}$ — биекция)	Бесконечный перечень длин регистра ($B_{f,L}$ — биекция)
f_1	x_0+x_{n-2}	1	2	(11, 7)	$n_0=9$	$n\equiv 1 \mod 4,\ n\geqslant 9$
f_2	x_0+x_{n-2}	1	2	(12, 8)	$n_0=11,13$	$n\equiv 1 \mod 4,\ n\geqslant 13$ $n\equiv 3 \mod 4,\ n\geqslant 11$
f_3	x_0+x_{n-1}	1	1	(10, 6)	$n_0=10$	$n\equiv 2 \mod 4,\ n\geqslant 10$
f_4	x_0+x_{n-1}	1	1	(14, 8)	$n_0=11,14$	$n\equiv 2 \mod 3,\ n\geqslant 11$
f_5	x_0+x_{n-1}	1	1	(18, 12)	$n_0=14,17$	$n\equiv 2 \mod 3,\ n\geqslant 14$
f_6	x_0+x_{n-3}	1	3	(10, 7)	$n_0=11$	$n\equiv 2 \mod 3,\ n\geqslant 11$
f_7	x_0+x_{n-2}	1	2	(12, 9)	$n_0=13$	$n\equiv 1 \mod 3,\ n\geqslant 11$
f_8	x_0+x_{n-2}	1	2	(7, 6)	$n_0=8$	$n\geqslant 8$
f_9	x_0+x_{n-2}	1	2	(10, 8)	$n_0=10,11$	$n\geqslant 10$
f_{10}	x_0+x_{n-3}	1	3	(9, 8)	$n_0=11$	$n\geqslant 11$
f_{11}	x_0+x_{n-3}	1	3	(8, 7)	$n_0=10$	$n\geqslant 10$
f_{12}	x_0+x_{n-1}	1	1	(14, 9)	$n_0=10$	$n\equiv 0 \mod 5,\ n\geqslant 10$

Замечание 3. Отсутствие запретов у функций $g \in \{f_7, \ldots, f_{12}\}$ из табл. 2 следует из утверждения 3 работы [8] с учётом полученной с помощью экспериментальных расчётов равновероятности 16-грамм $(y_1, y_2, \ldots, y_{16})$, где $y_j = g(x_j, x_{j+1}, \ldots, x_{j+4})$, $j = 1, 2, \ldots, 16$.

Замечание 4. Описание всех функций $f(x_1, x_2, \ldots, x_k)$ без запрета при небольших значениях k можно проводить экспериментальными методами на основе результатов работ [8, 9]. Методы построения функций без запрета рассматриваются также в [4, 5, 10] и др.

9. Случай $k = 6$

В табл. 4 приведены параметры биективных отображений $B_{f,L}$ для следующих функций от шести переменных:

$f_1 = x_1x_2 + x_1x_2x_3 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_3x_4x_5 + x_6$;

$f_2 = x_1x_2+x_1x_2x_3+x_1x_2x_4+x_1x_2x_3x_4+x_1x_2x_5+x_1x_2x_3x_5+x_1x_2x_4x_5+x_1x_2x_3x_4x_5+x_6$;

$f_3 = x_3 + x_4 + x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_6$;

$f_4 = x_3 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3x_5 + x_4x_5 + x_6$.

Таблица 4

Примеры биекций $B_{f,L}$, f от шести переменных

f	(h, t)	L	$s(1)$	$s(2)$	$n = n_0 \in M$ ($B_{f,L}$ — биекция)	Бесконечный перечень длин регистра ($B_{f,L}$ — биекция)
f_1	(14, 9)	$x_1 + x_{n-1}$	1	2	13	$n \equiv 3 \mod 5$, $n \geqslant 11$
f_1	(14, 9)	$x_1 + x_{n-1} + x_n$	1	2	13	$n \equiv 3 \mod 5$, $n \geqslant 11$
f_2	(14, 9)	$x_1 + x_n$	1	1	12, 13, 14	$n \geqslant 10$, $n \equiv 2 \mod 5$ или $n \equiv 3 \mod 5$ или $n \equiv 4 \mod 5$
f_2	(14, 9)	$x_1 + x_{n-1}$	1	2	13, 14	$n \geqslant 11$, $n \equiv 3 \mod 5$ или $n \equiv 4 \mod 5$
f_2	(14, 9)	$x_1 + x_{n-1} + x_n$	1	2	13, 14	$n \geqslant 11$, $n \equiv 3 \mod 5$ или $n \equiv 4 \mod 5$
f_3	(24, 16)	$x_1 + x_{n-3}$	1	4	21, 22, 23, 25, 26, 27	$n \neq 0 \mod 4$, $n \geqslant 20$
f_4	(22, 14)	$x_1 + x_{n-1}$	1	2	17, 19, 21, 23	$n \equiv 1 \mod 2$, $n \geqslant 16$

Замечание 5. В работе приведены только классы биекций $B_{f,L}$, отвечающих функциям

$$L = L(x_1, x_2, \ldots, x_{s(1)}, x_{n-s(2)+1}, x_{n-s(2)+2}, \ldots, x_n) \neq x_1.$$

Приведённые классы биективных отображений не являются окончательными и могут быть расширены, в том числе путём дополнительных экспериментов на ЭВМ с целью поиска биекций $B_{f,L}$ в ограниченной области длин регистра $n = n_0$, $h+s(1)+s(2)-2 \geqslant n_0 \geqslant t + s(1) + s(2) - 1$, при $s(1) + s(2) > 4$.

Замечание 6. Предлагаемый в работе метод построения биекций $B_{f,L}$ полностью применим и для случая нелинейной функции обратной связи L рассматриваемого вида.

Заключение

В работе развивается новый метод построения биективных отображений $B_{f,L}$, задаваемых регистром сдвига большой длины n с функцией обратной связи

$L(x_1, x_2, \ldots, x_n)$, которая зависит от ограниченного числа крайних переменных, и нелинейной функцией-фильтром $f(x_1, x_2, \ldots, x_k)$ от небольшого числа переменных $k \ll n$. Метод основан на поиске понижающих множеств функции f, наличие которых сводит исходную задачу для бесконечного множества длин генератора n к проверке биективности конечного числа отображений, отвечающих генераторам ограниченной длины $n \leqslant n_0$. На основе предложенного метода построены новые бесконечные классы биективных отображений $B_{f,L}$ для случая нелинейной функции $f = f(x_1, x_2, \ldots, x_k)$ от $k \leqslant 6$ переменных. Ранее аналогичные результаты были известны для случая, когда f зависит от трёх переменных.

Полученные результаты могут быть полезны при построении и обосновании статистических свойств датчиков случайных последовательностей на основе фильтрующих генераторов (их автоматная модель изложена, например, в [11]). При этом особое практическое значение имеет выбор пар (f, L), при которых одновременно обеспечивается биективность отображения $B_{f,L}$ и максимальность периода отображения δ_L. В этой связи отметим: если функция L обратной связи регистра сдвига длины n выбрана так, что соответствующая подстановка δ_L обладает циклом длины $2^n - 1$, то имеется в точности $2^{t+1}(1 - 2^{-n})$, где $t = 2^{n-1}$, булевых функций f от n переменных, при которых отображение $B_{f,L}$ является биективным [12, следствие 1].

Биективные отображения $B_{f,L}$ возникают также при исследовании классов регистров сдвига, обладающих одинаковой цикловой структурой. Действительно, как следует из результатов работы [12], если $B_{f,L}$ — биекция на двоичных векторах длины n, то регистры сдвига с функциями обратной связи $L(x)$ и $\varphi(x) = f((\delta_L)^n B_{f,L}^{-1}(x))$ имеют одинаковую цикловую структуру. Тем самым для получения явного вида функции обратной связи $\varphi(x)$ необходимо знать аналитический вид координатных функций отображения $B_{f,L}^{-1}$. В этой связи отметим, что в работе [7] получены оценки для степени нелинейности координатных функций (и их линейных комбинаций) отображения $B_{f,L}^{-1}$ для случая функции f от трёх переменных.

ЛИТЕРАТУРА

1. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2-х т. М.: Мир, 1988. 822 с.
2. *Рожков М. И.* К вопросу построения ортогональных систем двоичных функций с использованием регистра сдвига // Лесной вестник. 2011. Вып. 3. С. 180–185.
3. *Huffman D. A.* Canonical forms for information loss less finite state logical mashines // IRE Trans. Circuit Theory. 1959. V. 6, spec. suppl. P. 41–59.
4. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 1994. Т. 1. Вып. 1. С. 33–35.
5. *Логачев О. А., Смышляев С. В., Ященко В. В.* Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21. № 2. С. 51–74.
6. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: учебник. В 2-х т. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
7. *Саранцев А. В.* Построение регулярных систем однотипных двоичных функций с использованием регистра сдвига // Лесной вестник. 2004. № 1(32). С. 164–169.
8. *Рожков М. И.* Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m-грамм. Ч. 2 // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 2008. Т. 15. Вып. 5. С. 785–806.

9. *Рожков М. И.* Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m-грамм. Ч. 3 // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 2009. Т. 16. Вып. 1. С. 35–60.
10. *Михайлов В. Г., Чистяков В. П.* О задачах теории конечных автоматов, связанных с числом прообразов выходной последовательности // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 1994. Т. 1. Вып. 1. С. 7–32.
11. *Фомичев В. М.* Дискретная математика и криптология. Курс лекций / под общ. ред. Н. Д. Подуфалова. М.: ДИАЛОГ-МИФИ, 2003. 400 с.
12. *Рожков М. И.* О некоторых классах нелинейных регистров сдвига, обладающих одинаковой цикловой структурой // Дискретная математика. 2010. Т. 22. № 2. С. 96–119.