V. G. Nikonov, D. V. Churov, Bijective coordinate-forbidden k-valued functions in a problem of synthesis of substitutions,
Comp. nanotechnol., 2016, Issue 1, 14–23

1.2. БИЕКТИВНО КООРДИНАТНО-ЗАПРЕТНЫЕ k-ЗНАЧНЫЕ ФУНКЦИИ В ЗАДАЧАХ СИНТЕЗА ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

Никонов Владимир Глебович, доктор технических наук, член Президиума РАЕН

Чуров Дмитрий Валерьевич, сотрудник ФГУП «НИИ «КВАНТ». E-mail: cdv1994@yandex.ru

Аннотация: Внимание к изучению преобразований в k-значной логике в значительной степени стимулируется развитием современной компьютерной техники, в частности, повышением скоростей обработки информации и увеличением её объёмов. Переход от булевых операций к k-значным не сводится лишь к количественному росту сложностных характеристик, но затрагивает внутренние логические основы реализации и функционирования схем.

В данной статье внимание будет сосредоточено на исследовании одной частной проблемы k-значной логики в её локальной постановке, а именно, проблемы расширительной трактовки операции логического отрицания, которая, несмотря на простоту её исходной постановки, привела к построению теории функций с запретными знаками подфункций. Интерес представляют также оригинальные практические приложения этой теории, связанные с изучением ряда типовых узлов переработки информации с применением функций изучаемого класса.

Ключевые слова: биективные отображения, k-значные функции с запретными знаками подфункций.

1.2. BIJECTIVE COORDINATE-FORBIDDEN k-VALUED FUNCTIONS IN A PROBLEM OF SYNTHESIS OF SUBSTITUTIONS

Nikonov Vladimir Glebovich, Doctor of Technical Sciences, a member of the Presidium of Russian Academy of Natural Sciences

Churov Dmitry Valeryevich, employee of Federal State Unitary Enterprise Scientific Research Institute KVANT

Abstract: The interest towards the study of transformations in a k-valued logic is driven to a great extent by the development of modern computer technology, particularly by the increase in the amount of information and the increasing speed of information processing. The transition from Boolean operations to k-valued operations is not limited to a quantitative increase in complexity, as it also affects the internal logical framework of the schemes' implementation and functioning.

This article will focus on the study of a specific locally defined problem of k-valued logic, namely, the problem of expansive interpretation of the logical negation operation, which, despite the simplicity of its original definition, has led to the creation of a theory of functions with forbidden signs of subfunctions. Of additional interest are original practical applications of this theory associated with the study of a range of typical information processing nodes using functions of the studied class.

Index terms: bijections, k-valued functions with forbidden signs of subfunctions.

Определение 1. Будем говорить, что функция k-значной логики $f(x_1, \dots, x_n)$ обладает запретным знаком α подфункции при фиксации $\left(x_{j_1}, x_{j_2}, \dots, x_{j_t}\right) = \left(\varepsilon_{i_1}, \varepsilon_{i_2}, \dots, \varepsilon_{i_t}\right)$, если $f\left(\left(x_{j_1}, x_{j_2}, \dots, x_{j_t}\right)/\left(\varepsilon_{i_1}, \varepsilon_{i_2}, \dots, \varepsilon_{i_t}\right)\right) \neq \alpha$.

Определение 2. Функция k-значной логики $f(x_1, \dots, x_n)$, обладающая запретными знаками подфункций при любой фиксации переменных, называется биективно координатно-запретной, если существует подстановка $\begin{pmatrix} \alpha_1 & \dots & \alpha_i & \dots & \alpha_k \\ \beta_{\alpha_1} & \dots & \beta_{\alpha_i} & \dots & \beta_{\alpha_k} \end{pmatrix}$ такая, что для любого $\alpha_i \in \mathbb{Z}_k$, при любых $i \in \overline{1,k}, j \in \overline{1,n}$ выполняется неравенство

$f(x_1, \dots, x_{j-1}, \alpha_i, x_{j+1}, \dots, x_n) \neq \beta_{\alpha_i}$ на всех наборах $(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n)$.

Пример 1. При $k = 3$, $n = 2$, рассмотрим функцию $f_1(x_1, \dots, x_n)$, заданную таблично:

Таблица 1.

(x_1, x_2)	$f_1(x_1, x_2)$
00	2
01	2
02	1
10	2
11	0
12	0
20	1
21	0
22	1

Из табличного задания вытекает, что функция $f_1(x_1, x_2)$ – биективно координатно-запретная, так как для неё выполняется определение 2.

Для изложения элементов теории биективно координатно-запретных функций необходимо ввести следующие понятия:

Множество всех биективно координатно-запретных k-значных функций от n переменных обозначим $\mathfrak{B}_n^k$. В дальнейшем для краткости функции из класса $\mathfrak{B}_n^k$ будем называть БКЗ функциями.

Подстановку $\begin{pmatrix} \alpha_1 & \dots & \alpha_i & \dots & \alpha_n \\ \beta_{\alpha_1} & \dots & \beta_{\alpha_i} & \dots & \beta_{\alpha_n} \end{pmatrix}$ назовём подстановкой соответствия биективно координатно-запретной функции f.

Множество всех биективно координатно-запретных k-значных функций от n переменных с подстановкой соответствия σ обозначим $\mathfrak{B}_n^k(\sigma)$.

Определение 3. Весом вектора $(x_1, \dots, x_n)$ назовём вектор

$$w(x_1, \dots, x_n) = \left(\sum_{i=1}^{n} Ind_0(x_i), \sum_{i=1}^{n} Ind_1(x_i), \dots, \sum_{i=1}^{n} Ind_{k-1}(x_i) \right), \text{где}$$

$$Ind_\alpha(x_i) = \begin{cases} 1, \text{если } x_i = \alpha \\ 0, \text{если } x_i \neq \alpha \end{cases}.$$

Обозначим

$\rho_w(x_1, \dots, x_n) = |\{\alpha \in \mathbb{Z}_k | \sum_{i=1}^{n} Ind_\alpha(x_i) \neq 0\}|$ – количество ненулевых координат в весе вектора $(x_1, \dots, x_n)$.

Очевидно, что множество $\mathfrak{B}_n^k$ представляется следующим образом:

$$\mathfrak{B}_n^k = \bigcup_{\sigma \in S(\mathbb{Z}_k)} \mathfrak{B}_n^k(\sigma).$$

Множества $\mathfrak{B}_n^k(\sigma)$, $\sigma \in S(\mathbb{Z}_k)$, могут иметь общие элементы.

Пример 2. При $n = 2$, $k = 4$, рассмотрим пример функции $f_2(x_1, x_2)$ с табличным заданием:

Таблица 2.

x_1	x_2	$f_2(x_1, x_2)$
0	0	2
0	1	2
0	2	3
0	3	2
1	0	2
1	1	2
1	2	3
1	3	2
2	0	3
2	1	3
2	2	3
2	3	0
3	0	2
3	1	2
3	2	0
3	3	0

Нетрудно проверить, что заданная функция $f_2(x_1, x_2)$ принадлежит к двум классам: $\mathfrak{B}_2^4(\sigma_1)$ и $\mathfrak{B}_2^4(\sigma_2)$, где $\sigma_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}$ и $\sigma_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 2 & 3 \end{pmatrix}$.

Утверждение 1. Если функция $f \in \mathfrak{B}_n^k$, то $n < k$.

Доказательство. Предположим, что f – БКЗ функция и для неё выполняется неравенство $n \geq k$. Рассмотрим подфункцию, полученную фиксацией её первых k переменных. Зафиксируем первую переменную числом 0, вторую 1 и так далее. При фиксации каждой новой переменной новым числом количество значений, которые может принимать эта подфункция, уменьшается на единицу. Следовательно, при фиксации k переменных различными числами, функция не может принимать ни одно значение из $\mathbb{Z}_k$. Из полученного противоречия следует, что $n < k$ для любой БКЗ функции.

Теорема 1. При любой подстановке $\sigma \in S(\mathbb{Z}_k)$ мощность класса функций $\mathfrak{B}_n^k(\sigma)$ равна

$$|\mathfrak{B}_n^k(\sigma)| = \prod_{i=1}^{n} (k-i)^{\binom{k}{i} S(n,i) i!},$$

где $S(n, i)$ – числа Стирлинга второго рода.

При $n = k - 1$ класс $\mathfrak{B}_n^k$ представим в виде

$$\mathfrak{B}_n^k = \coprod_{\sigma \in S(\mathbb{Z}_k)} \mathfrak{B}_n^k(\sigma),$$

и в этом случае его мощность определяется по формуле

$$\left|\mathfrak{B}_{k-1}^{k}\right| = \sum_{\sigma\in S(\mathbb{Z}_k)} \left|\mathfrak{B}_{k-1}^{k}(\sigma)\right| = k!\prod_{i=1}^{k-1}(k-i)^{\binom{k}{i}S(k-1,i)i!}.$$

Доказательство. Заметим, что число вариантов значений, которые может принимать функция на векторе $\vec{x} = (x_1, \dots, x_n)$ зависит только от значения $\rho_w(\vec{x})$. Если $\rho_w(\vec{x}) = i$, то функция может принять на этом векторе одно из $k - i$ значений. Следовательно, количество функций из класса $\mathfrak{B}_n^k(\sigma)$ равно

$$\prod_{\vec{x}\in\mathbb{Z}_k^n}\left(k - \rho_w(\vec{x})\right).$$

В свою очередь это число можно представить в виде

$$\prod_{i=0}^{k}(k-i)^{|\{\vec{x}\in\mathbb{Z}_k^n|\rho_w(\vec{x})=i\}|}.$$

Осталось найти значение $|\{\vec{x} \in \mathbb{Z}_k^n|\rho_w(\vec{x}) = i\}|$, которое равно числу векторов из $\mathbb{Z}_k^n$, содержащих ровно i различных значений координат. Сначала нужно выбрать i различных чисел из $\mathbb{Z}_k^n$, что можно сделать $\binom{k}{i}$ способами. Далее требуется разбить n-элементное множество на i непустых подмножеств, что соответствует выбору номеров координат, на местах которых будут находиться одинаковые числа. Эти значения описываются числами Стирлинга второго рода (см. [1]). Остаётся только установить соответствие между множествами из разбиения и числами из выбранного подмножества множества $\mathbb{Z}_k^n$. Таких вариантов $i!$. Получаем

$$|\{\vec{x} \in \mathbb{Z}_k^n|\rho_w(\vec{x}) = i\}| = \binom{k}{i} S(n,i)i!.$$

Подставляя полученное значение в предыдущую формулу получаем искомое выражение.

Пусть теперь $n = k - 1$. Зафиксируем переменные $k - 1$ различными значениями из $\mathbb{Z}_k$. Тогда среди значений зафиксированных переменных не встретится только одно число α из $\mathbb{Z}_k$ и функция на этом наборе однозначно определяет запретный знак, соответствующий числу α. Перебирая по очереди $k - 1$ наборов переменных, тем же способом однозначно определяем подстановку соответствия для рассматриваемой функции. Из этого следует, что классы $\mathfrak{B}_{k-1}^k(\sigma_1)$ и $\mathfrak{B}_{k-1}^k(\sigma_2)$ не пересекаются для любых $\sigma_1 \neq \sigma_2$. Следовательно,

$$\left|\mathfrak{B}_{k-1}^{k}\right| = \sum_{\sigma\in S(\mathbb{Z}_k)} \left|\mathfrak{B}_{k-1}^{k}(\sigma)\right|.$$

Учитывая сказанное выше, имеем

$$\left|\mathfrak{B}_{k-1}^{k}\right| = \sum_{\sigma\in S(\mathbb{Z}_k)} \left|\mathfrak{B}_{k-1}^{k}(\sigma)\right| = \sum_{\sigma\in S(\mathbb{Z}_k)}\prod_{i=1}^{k-1}(k-i)^{\binom{k}{i}S(k-1,i)i!}.$$

Так как $|S(\mathbb{Z}_k)| = k!$, получаем:

$$\left|\mathfrak{B}_{k-1}^{k}\right| = \sum_{\sigma\in S(\mathbb{Z}_k)} \left|\mathfrak{B}_{k-1}^{k}(\sigma)\right| = k!\prod_{i=1}^{k-1}(k-i)^{\binom{k}{i}S(k-1,i)i!}.$$

Структура графа автономного регистра сдвига с БКЗ функцией обратной связи

Определение 4. Графом де Брейна регистра длины n с функцией обратной связи $(x_1, \dots, x_n)$ называется ориентированный граф $J_n^k(f)$, вершинами которого являются все k^n состояний регистра $\overrightarrow{x_j} = (x_1^{(j)}, \dots, x_n^{(j)})$, $x_i^{(j)} \in \{0, \dots, k-1\}$, $j \in \overline{1, k^n}$, $i \in \overline{1, n}$, а ориентированной дугой соединяется вершина $\overrightarrow{x_{J_1}}$ с вершиной $\overrightarrow{x_{J_2}}$, если состояние $\overrightarrow{x_{J_1}}$ преобразуется в состояние $\overrightarrow{x_{J_2}}$ вследствие сдвига на один такт влево:

$$\overrightarrow{x_{J_1}} = \left(x_1^{(j_1)}, \dots, x_n^{(j_1)}\right) \to \overrightarrow{x_{J_2}} =$$
$$= \left(x_2^{(j_1)}, \dots, x_n^{(j_1)}, f\left(x_1^{(j_1)}, \dots, x_n^{(j_1)}\right)\right).$$

Схема, представленная на рисунке 1 аналогична схеме фильтрующего генератора (см [2]), функция усложнения которого является функцией обратной связи.

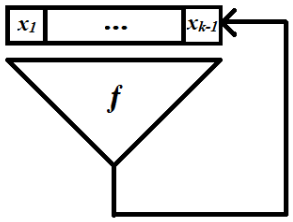

Рис. 1.

Теорема 2. Пусть $f(x_1, \dots, x_{k-1}) \in \mathfrak{B}_{k-1}^k(\varepsilon)$, ε – тождественная подстановка. Тогда верны следующие утверждения, описывающие строение графа де Брейна регистра с функцией обратной связи $f(x_1, \dots, x_{k-1})$.

Граф де Брейна регистра длины $k - 1$ с функцией обратной связи $f(x_1, \dots, x_{k-1})$ в точности состоит из $(k-1)!$ компонент связности, каждая из которых представляется в виде цикла

длины k с подходами. Каждый цикл имеет вид:

$$x_1^{(j)}x_2^{(j)}\dots x_{k-1}^{(j)} \to x_2^{(j)}x_3^{(j)}\dots x_k^{(j)} \to$$
$$x_3^{(j)}x_4^{(j)}\dots x_k^{(j)}x_1^{(j)} \to \dots \to x_1^{(j)}x_2^{(j)}\dots x_{k-1}^{(j)},$$

где $x_s^{(j)} \neq x_l^{(j)}$ при $s \neq l, j \in \overline{1,(k-1)!}$.

Между произвольной вершиной x вида $x_1'x_2'\dots x_{k-1}'$, находящейся на подходе, и y – ближайшей к ней цикловой вершине, существует ориентированный маршрут длины $k-1-s$, где s – длина максимально возможной последовательности вида $x_m', x_{m+1}', \dots, x_{k-1}'$, $m \in \overline{1,k-1}$, содержащей попарно различные числа. Количество вершин, находящихся на расстоянии i от цикла равно $\frac{k!}{(i+1)!}k^{i-1}(k-i-1)$.

Степень исхода любой вершины равна 1, степень захода не превосходит $k-1$, если её последняя координата не равна ни одной предыдущей, и равна 0 в противном случае.

Доказательство. 1) Заметим, что вершина вида $x_1'x_2'\dots x_{k-1}'$, где значения всех координат попарно различны, может перейти только в вершину вида $x_2'x_3'\dots x_k'$, где значения всех координат также попарно различны. Отсюда следует, что вершины такого вида образуют цикл, длина такого цикла равна k.

Рассмотрим вершину, в которой встречаются координаты с одинаковыми значениями. При переходе одной вершины в другую её координаты сдвигаются влево на 1, при этом первая координата исключается, а на место последней становится число, не равное ни одной координате начальной вершины. Это означает, что если вершина y была достигнута из вершины x за s шагов, где $s < k-1$, то последние $s+1$ координат будут иметь попарно различные значения. Из этого следует, что не более чем за $k-2$ шагов любая вершина переходит в вершину, у которой значения всех координат попарно различны. Таким образом, делаем вывод, что если вершина, в которой встречаются координаты с одинаковыми значениями, лежит на цикле, то на этом же цикле лежит и вершина, у которой значения всех координат попарно различны. Но такая вершина, как было показано выше, уже лежит на другом цикле, из чего следует противоречие.

Следовательно, в графе цикловыми вершинами являются те и только те, у которых значения всех координат попарно различны. Они образуют циклы длины k. Так как таких вершин всего $k!$, то количество циклов равно в точности $(k-1)!$.

2) Очевидно, что в конце любого вектора, соответствующего одноимённой вершине, содержится подвектор, состоящий из попарно различных координат (в худшем случае длины 1). При каждом переходе по дуге графа длина этого подвектора увеличивается на единицу. Как только его длина станет равной $k-1$, подход завершится. Следовательно, любая вершина попадает в цикл ровно за $k-1-s$ переходов, где s – длина указанного выше подвектора.

Найдём число вершин, которые попадают в ближайшую к ним цикловую вершину ровно за i шагов. По предыдущим рассуждениям получаем, что последние $k-i-1$ координат каждой такой вершины попарно различны. При этом координата с номером i равна одной из последних $k-i-1$ координат. Первые $i-1$ координат выбираются произвольно, это можно сделать k^{i-1} способами. Координату с номером i можно выбрать $k-i-1$ способами, а последние $k-1-i$ координат – $\binom{k}{k-i-1}(k-i-1)!$ способами. Получили, что число вершин такого вида равно

$$\binom{k}{k-i-1}(k-i-1)!\,k^{i-1}(k-i-1) = k^{i-1}(k-i-1)\frac{k!}{(i+1)!}.$$

3) Очевидно, что степень исхода любой вершины равна единице. Для описания степени захода произвольной вершины $x = x_1'x_2'\dots x_{k-1}'$ рассмотрим все возможные случаи:

а) Существует $r \in \overline{1,k-2}: x_{k-1}' = x_r'$. Известно, что, при переходе по дуге, к новой вершине добавляется координата со значением, отличающимся от всех предыдущих. Этот факт означает, что в вершину с указанным свойством не может входить ни одно ребро. Следовательно, степень захода этой вершины равна нулю.

б) Не существует $r \in \overline{1,k-2}: x_{k-1}' = x_r'$ и $1 < \rho_w(x) \leq k-1$. В вершину x могут перейти

только вершины $y^{(j)} = y_1^{(j)} x'_2 \dots x'_{k-1}$со свойством $\rho_w(y) = \rho_w(x)$ или $\rho_w(y) = \rho_w(x) - 1$. Очевидно, что при переходе в графе де Брейна случай $\rho_w(y) = \rho_w(x) + 1$ невозможен согласно определению функции f. Действительно, это означало бы, что функция f приняла значение, равное значению одной из своих переменных. Рассмотрим два случая:

Пусть для y выполняется $\rho_w(x) = \rho_w(y)$, значит не существует $r \in \overline{2, k-1}: y_1 = x'_r$. Тогда $\rho_w(y_1 x'_2 \dots x'_{k-1}) = \rho_w(x) - 1$ и $y_0 \neq x_{k-1}$. Следовательно, y_0 может принимать ровно $k - (\rho_w(x) - 1) - 1 = k - \rho_w(x)$ значений.

Пусть $\rho_w(y) = \rho_w(x) - 1$, значит существует $r \in \overline{2, k-1}: y_1 = x'_r$. Тогда

$$\rho_w(y_1 x'_2 \dots x'_{k-1}) = \rho_w(x) - 1 \text{ и } y_0$$

равно одному из значений $y_1, x'_2, \dots, x'_{k-1}$. Следовательно, y_1 может принимать ровно $\rho_w(x) - 1$ значений.

Таким образом, степень захода x не превышает суммы этих значений, то есть $k - \rho_w(x) + \rho_w(x) - 1 = k - 1$.

Следствие: Пусть $f \in \mathfrak{B}_n^k(\varepsilon)$, $n < k - 1$. Тогда:

1) Все циклы графа де Брейна регистра длины n имеют вид:

$x_1 x_2 \dots x_n \to x_2 x_3 \dots x_{n+1} \to \dots \to x_i x_{i+1} \dots x_{n+i-1} \to \dots \to x_1 x_2 \dots x_n$**,** где $x_s \neq x_l$ при $s \neq l$.

2) Степень исхода любой вершины равна 1, степень захода не превосходит $k - 1$, если её последняя координата не равна ни одной предыдущей, и равна 0 в противном случае.

Пример 3. Рассмотрим функцию $f(x_1, x_2, x_3) \in \mathfrak{B}_3^4(\varepsilon)$.

Её граф имеет вид:

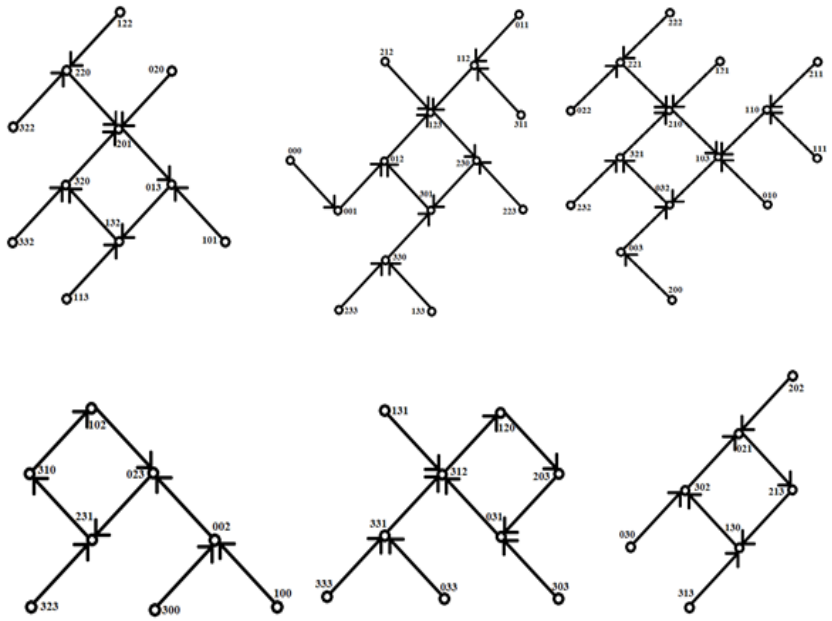

Рис. 2

Синтез подстановочных преобразований на основе БКЗ функций

Рассмотрим возможность использования БКЗ функций для построения подстановок $\pi \in S(\mathbb{Z}_k^n)$, осуществляющих биективное отображение векторов $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_k^n$ по формуле $\pi(x_1, x_2, \dots, x_n) =$

$= (\pi_1(x_1, x_2, \dots, x_n), \pi_2(x_1, x_2, \dots, x_n), \dots, \pi_n(x_1, x_2, \dots, x_n))$,

где $\pi_1, \pi_2, \dots, \pi_n$ – координатные функции подстановки π.

В данном разделе рассматриваются вопросы построения и изучения свойств подстановок, с координатными БКЗ функциями из класса $\mathfrak{B}_n^k(\varepsilon)$. Класс всех таких подстановок обозначим $\Pi = \{\pi \in S(\mathbb{Z}_k^n) | \pi = (\pi_1, \pi_2, \dots, \pi_n), \pi_1, \pi_2, \dots, \pi_n \in \mathfrak{B}_n^k(\varepsilon)\}$, а сами подстановки назовём БКЗ подстановками.

Как было замечено в доказательстве теоремы 1, ни одна БКЗ функция из класса $\mathfrak{B}_n^k(\varepsilon)$ не может принимать на векторе$(x_1, x_2, \dots, x_n)$

значение, равное любой из его координат. Таким образом, для каждого вектора $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_k^n$ образуется некоторое множество значений, которые не может принимать ни одна функция из $\mathfrak{B}_n^k(\varepsilon)$ при фиксации её переменных значениями из мультимножества $\langle x_1, x_2, \dots, x_n \rangle$. Назовём такое множество множеством недостижимых значений для вектора $(x_1, x_2, \dots, x_n)$. Аналогичное свойство наблюдается и в случае БКЗ подстановок с тем отличием, что значением подстановки является не элемент множества $\mathbb{Z}_k$, а вектор из $\mathbb{Z}_k^n$.

Обратим внимание на то, что для некоторых наборов фиксаций всех переменных подстановки $\pi \in \Pi$ такие множества совпадают.

Пример 4. В данном примере представлено табличное задание БКЗ подстановки π.

Таблица 3.

(x_1,x_2,x_3)	$\pi(x_1,x_2,x_3)$
000	143
001	234
002	413
003	421
004	312
010	342
011	324
012	444
013	422
014	222
020	431
021	434
022	341
023	144
024	331
030	412
031	244
032	114
033	214
034	221
040	213
041	032
042	313
043	112
044	132
100	423
101	233
102	433
103	424
104	223
110	432
111	243
112	340
113	440
114	302
120	443
121	034
122	043
123	040
124	030
130	224
131	402

(x_1,x_2,x_3)	$\pi(x_1,x_2,x_3)$
132	000
133	204
134	022
140	322
141	320
142	333
143	002
144	203
200	134
201	343
202	314
203	441
204	301
210	344
211	403
212	304
213	004
214	303
220	334
221	430
222	013
223	410
224	031
230	141
231	044
232	140
233	104
234	100
240	131
241	300
242	310
243	011
244	103
300	142
301	242
302	411
303	241
304	111
310	442
311	042
312	400
313	420

(x_1,x_2,x_3)	$\pi(x_1,x_2,x_3)$
314	200
320	414
321	404
322	014
323	401
324	110
330	124
331	240
332	041
333	024
334	012
340	212
341	220
342	001
343	211
344	120
400	231
401	332
402	311
403	121
404	123
410	323
411	023
412	003
413	020
414	232
420	113
421	033
422	133
423	101
424	330
430	122
431	202
432	010
433	021
434	210
440	321
441	230
442	130
443	201
444	102

Как можно было заметить, множество недостижимых значений определяется только значениями различных координат в векторе $(x_1, x_2, \dots, x_n)$. Далее будет удобным объединить вектора с одним и тем же множеством недостижимых значений во множества

$$\left\{ A_{\nu_1\nu_2\dots\nu_s} = (x_1, x_2, \dots, x_n) \in \mathbb{Z}_k^n \middle| \prod_{i=1}^{s} \left(\sum_{j=1}^{n} Ind_{\nu_i}(x_j) \right) > 0, \sum_{\alpha \in \mathbb{Z}_k \setminus \{\nu_1\nu_2\dots\nu_s\}} \left(\sum_{j=1}^{n} Ind_{\alpha}(x_j) \right) = 0 \right\},$$

где $\{\nu_1, \nu_2, \dots, \nu_s\}$ – множество недостижимых значений для любого элемента $A_{\nu_1\nu_2\dots\nu_s}$.

Фактически такое определение множества говорит о том, что в него входят только те элементы, у векторов веса которых множества ненулевых координат совпадают. Или, иными словами, множество $A_{\nu_1\nu_2\dots\nu_s}$ состоит из векторов, в которых в качестве координат встречаются все элементы множества $\{\nu_1, \nu_2, \dots, \nu_s\}$ и только они.

Из вышесказанного следует, что ни одна БКЗ подстановка не сможет перевести вектор из $A_{\nu_1\nu_2\dots\nu_s}$ в вектор, содержащий в качестве одной из своих координат элемент множества $\{\nu_1, \nu_2, \dots, \nu_s\}$. Этот факт позволяет ввести новое определение.

Определение 5. Множеством запретных векторов для $A_{\nu_1\nu_2\dots\nu_s}$ назовём множество $B_{\nu_1\nu_2\dots\nu_s} = \left\{ (x_1, x_2, \dots, x_n) \in \mathbb{Z}_k^n | \exists l \in \overline{1,n} : x_l \in \{\nu_1, \nu_2, \dots, \nu_s\} \right\}$.

Для дальнейших рассуждений требуется выделить множество преобразований

$M = \{\sigma \in S(\mathbb{Z}_k^n) | \forall s \in \overline{1,n}\ \forall \nu_1, \nu_2, \dots, \nu_s \in \mathbb{Z}_k\ \sigma(A_{\nu_1\nu_2\dots\nu_s}) = A_{\nu_1\nu_2\dots\nu_s}\}$.

Множество M состоит из тех и только тех подстановок, которые переставляют элементы внутри множеств $A_{\nu_1\nu_2\dots\nu_s}$, не выходя за их пределы.

Пример 5. В данном примере представлено табличное задание подстановки σ из класса M.

Таблица 4.

(x_1,x_2,x_3)	$\sigma(x_1,x_2,x_3)$
000	000
001	110
002	020
003	030
004	040
010	100
011	001
012	021
013	031
014	041
020	200
021	102
022	002
023	032
024	042
030	300
031	103
032	203
033	003
034	043
040	400
041	104
042	204
043	304
044	004
100	011
101	101
102	120
103	130
104	140
110	010
111	111
112	121
113	131
114	141
120	201
121	211
122	112
123	132
124	142
130	301
131	311

(x_1,x_2,x_3)	$\sigma(x_1,x_2,x_3)$
132	213
133	113
134	143
140	401
141	411
142	214
143	314
144	114
200	220
201	210
202	022
203	230
204	240
210	012
211	221
212	122
213	231
214	241
220	202
221	212
222	222
223	232
224	242
230	302
231	312
232	322
233	223
234	243
240	402
241	412
242	422
243	324
244	224
300	330
301	310
302	320
303	033
304	340
310	013
311	331
312	321
313	133

(x_1,x_2,x_3)	$\sigma(x_1,x_2,x_3)$
314	341
320	023
321	123
322	332
323	233
324	342
330	303
331	313
332	323
333	333
334	343
340	403
341	413
342	423
343	433
344	334
400	440
401	410
402	420
403	430
404	044
410	014
411	441
412	421
413	431
414	144
420	024
421	124
422	442
423	432
424	244
430	034
431	134
432	234
433	443
434	344
440	404
441	414
442	424
443	434
444	444

Утверждение 2. Множество M является группой.

Доказательство. Напомним что**,** конечное непустое подмножество H группы G является её подгруппой тогда и только тогда, когда для любых $g,h \in H$ $(g \cdot h \in H)$ (см [3]).

Пусть $\sigma_1,\sigma_2 \in M$, тогда $\sigma_1 \cdot \sigma_2\left(A_{\nu_1\nu_2\dots\nu_s}\right) = = \sigma_2\left(\sigma_1\left(A_{\nu_1\nu_2\dots\nu_s}\right)\right) = \sigma_2\left(A_{\nu_1\nu_2\dots\nu_s}\right) = A_{\nu_1\nu_2\dots\nu_s}$. По определению $\sigma_1 \cdot \sigma_2 \in M$.

Утверждение 3. Мощность множества M составляет

$$\prod_{i=1}^{n}\left((S(n,i)s!)!\right)^{\binom{k}{s}}.$$

Доказательство. Из определения следует, что в разложениях подстановок из класса M в произведение независимых циклов циклы не могут состоять одновременно из элементов двух и более множеств $A_{\nu_1\nu_2\dots\nu_s}$. Следовательно, множества элементов этих циклов являются подмножествами множеств $A_{\nu_1\nu_2\dots\nu_s}$. Таким образом, элементы множества M задают локальные подстановки на $A_{\nu_1\nu_2\dots\nu_s}$, что верно и в обратную сторону – набор преобразований всех множеств $A_{\nu_1\nu_2\dots\nu_s}$ задаёт подстановку из M. Общее число способов выбора такого набора очевидно равно

$$\prod_{\{\nu_1,\nu_2,\dots,\nu_s\}\in\mathbb{Z}_k}\left(\left(\left|A_{\nu_1\nu_2\dots\nu_s}\right|\right)!\right).$$

Из теоремы 1 следует, что множество $A_{\nu_1\nu_2\dots\nu_s}$ имеет мощность $S(n,i)s!$. Общее количество преобразований этого множества составляет $\left((S(n,i)s!)!\right)$. При этом для заданного числа s количество множеств $A_{\nu_1\nu_2\dots\nu_s}$ равно $\binom{k}{s}$, что позволяет привести указанное выше выражение к виду

$$\prod_{i=1}^{n}\left((S(n,i)s!)!\right)^{\binom{k}{s}}.$$

Теорема 3. Для существования подстановки $\pi = (\pi_1,\pi_2,\dots,\pi_n)\colon \mathbb{Z}_k^n \to \mathbb{Z}_k^n$, где $\pi_1,\pi_2,\dots,\pi_n \in \mathfrak{B}_n^k(\varepsilon)$, необходимо выполнение неравенства $k \geq \frac{\sqrt[n]{2}}{\sqrt[n]{2}-1}$.

Доказательство.

Обозначим

$\pi(B_\nu) = \{\pi(x_1,x_2,\dots,x_n)|(x_1,x_2,\dots,x_n) \in B_\nu\}$.

Заметим, что по условию $\pi(B_\nu) \subseteq \mathbb{Z}_k^n \backslash B_\nu$ для любого $\nu \in \mathbb{Z}_k$. Так как f – подстановка, то $|\pi(B_\nu)| = |B_\nu|$. Значит, выполняется условие

$$|B_\nu| \leq k^n - |B_\nu|.$$

Нетрудно показать, что

$$|B_\nu| = \sum_{i=1}^{n}\binom{n}{i}(k-1)^{n-i} = k^n - (k-1)^n.$$

Преобразуем полученное неравенство:

$$k^n - (k-1)^n \le \frac{k^n}{2};$$
$$\frac{k}{\sqrt[n]{2}} \le k-1;$$
$$1 \le k\left(1 - \frac{1}{\sqrt[n]{2}}\right);$$
$$\frac{\sqrt[n]{2}}{\sqrt[n]{2}-1} \le k.$$

Следствие: Данное условие также можно представить в виде:

$$n \le \log_{\frac{k}{k-1}} 2.$$

Доказательство.

$$\frac{k}{\sqrt[n]{2}} \le k-1;$$
$$ln\left(\frac{k}{k-1}\right) \le \frac{1}{n} ln2;$$
$$\log_2\left(\frac{k}{k-1}\right) \le \frac{1}{n};$$
$$n \le \log_{\frac{k}{k-1}} 2.$$

Теорема 4. Пусть $\pi: \mathbb{Z}_k^n \to \mathbb{Z}_k^n$ – полноцикловая подстановка и $\pi \in \Pi$. Тогда для любой подстановки $\sigma \in M \subseteq S(\mathbb{Z}_k^n)$ выполняется $\tau = \sigma^{-1} \cdot \pi \cdot \sigma$ – полноцикловая подстановка, где $\tau_1, \tau_2, \dots, \tau_n \in \mathfrak{B}_n^k(\varepsilon)$.

Доказательство. Построим цепочку равносильных утверждений. π – подстановка с координатными функциями из $\mathfrak{B}_n^k(\varepsilon) \Leftrightarrow$ для любого $(x_1, x_2, \dots, x_n) \in A_{\nu_1\nu_2\dots\nu_s}\ \pi(x_1, x_2, \dots, x_n) \notin B_{\nu_1\nu_2\dots\nu_s} \Leftrightarrow \pi(A_{\nu_1\nu_2\dots\nu_s}) \cap B_{\nu_1\nu_2\dots\nu_s} = \emptyset$.

Подстановка π представляется циклом:

$$\left(\vec{y}_1, \vec{y}_2, \dots, \vec{y}_{j_1}, \vec{y}_{j_1+1}, \dots, \vec{y}_{j_2}, \vec{y}_{j_1+2}, \dots,\right.$$
$$\left.\vec{y}_{j_{|A_{\nu_1\nu_2\dots\nu_s}|}}, \vec{y}_{j_{|A_{\nu_1\nu_2\dots\nu_s}|+1}}, \dots, \vec{y}_{k^n}\right),$$

где $y_{j_l} \in A_{\nu_1\nu_2\dots\nu_s}$, а $y_{j_l+1} \in \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$ для любого $l \in \overline{1, |A_{\nu_1\nu_2\dots\nu_s}|}$.

После её сопряжения подстановкой σ имеем:

$$\left(\sigma(\vec{y}_1), \sigma(\vec{y}_2), \dots, \sigma\left(\vec{y}_{j_1}\right), \sigma\left(\vec{y}_{j_1+1}\right), \dots, \sigma\left(\vec{y}_{j_2}\right),\right.$$
$$\left.\sigma\left(\vec{y}_{j_2+2}\right), \dots, \sigma\left(\vec{y}_{j_{|A_{\nu_1\nu_2\dots\nu_s}|}}\right), \sigma\left(\vec{y}_{j_{|A_{\nu_1\nu_2\dots\nu_s}|+1}}\right), \dots, \sigma(\vec{y}_{k^n})\right),$$

где $\sigma(y_{j_l}) \in A_{\nu_1\nu_2\dots\nu_s}$ для любого $l \in \overline{1, |A_{\nu_1\nu_2\dots\nu_s}|}$.

Достаточно доказать, что $\sigma(y_{j_l+1}) \in \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$ для любого $l \in \overline{1, |A_{\nu_1\nu_2\dots\nu_s}|}$.

Известно, что $y_{j_l+1} \in \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$ для любого $l \in \overline{1, |A_{\nu_1\nu_2\dots\nu_s}|}$. Зафиксируем l значением из диапазона $\overline{1, |A_{\nu_1\nu_2\dots\nu_s}|}$. Тогда существует единственный набор попарно различных чисел $\mu_1, \mu_2, \dots, \mu_m$, $\mu_i \in \mathbb{Z}_k$, $m \in \overline{1, n-s}$, удовлетворяющий условию $y_{j_l+1} \in A_{\mu_1\mu_2\dots\mu_m}$ и $\{\mu_1, \mu_2, \dots, \mu_m\} \cap \{\nu_1, \nu_2, \dots, \nu_s\} = \emptyset$.

Отсюда следует, что $A_{\mu_1\mu_2\dots\mu_m} \subseteq \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$. По определению подстановки σ имеем: $\sigma(y_{j_l+1}) \in \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$.

Следовательно,

$\tau\left(\sigma(y_{j_l})\right) = \sigma(y_{j_l+1}) \in \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$ для любого $l \in \overline{1, |A_{\nu_1\nu_2\dots\nu_s}|}$. Тогда $\tau(A_{\nu_1\nu_2\dots\nu_s}) \subseteq \mathbb{Z}_k^n \backslash B_{\nu_1\nu_2\dots\nu_s}$, откуда $\tau(A_{\nu_1\nu_2\dots\nu_s}) \cap B_{\nu_1\nu_2\dots\nu_s} = \emptyset$.

Следствие: Пусть $\pi \in \Pi$. Тогда для любой подстановки $\sigma \in M \subseteq S(\mathbb{Z}_k^n)$ $\tau = \sigma^{-1} \cdot \pi \cdot \sigma$ – подстановка, где $\tau_1, \tau_2, \dots, \tau_n \in \mathfrak{B}_n^k(\varepsilon)$. При этом цикловые структуры подстановок π и τ совпадают.

Доказательство. Доказательство следствия проводится аналогично доказательству теоремы.

Замечание. Подстановки $\pi: \mathbb{Z}_k^n \to \mathbb{Z}_k^n$ с координатными функциями из $\mathfrak{B}_n^k(\varepsilon)$ не содержат единичных циклов.

Доказанная теорема позволяет ввести отношение эквивалентности на множестве Π.

Определение 6. Подстановки $\pi, \tau \in \Pi$ назовём эквивалентными и обозначим $\pi \sim \tau$, если существует подстановка $\sigma \in M$ такая, что $\sigma^{-1} \cdot \pi \cdot \sigma = \tau$.

Утверждение 4. Бинарное отношение «~» на множестве Π является отношением эквивалентности.

Доказательство. Доказательство очевидно, так как множество M является группой.

Предыдущее утверждение позволяет представить множество Π в виде объединения попарно непересекающихся классов эквивалентных элементов вида $[\pi]_\sim = \{\sigma^{-1} \cdot \pi \cdot \sigma | \sigma \in M\}$, где $\pi \in \Pi$. Причем все подстановки из одного класса будут иметь одну и ту же цикловую структуру. Тот факт, что сопряжение подстановки π из Π подстановкой из M приводит лишь к перестановке элементов множеств $A_{\nu_1\nu_2\dots\nu_s}$ в разложении π в произведение независимых циклов (то есть если на каком-либо месте в цикле находился элемент из $A_{\nu_1\nu_2\dots\nu_s}$, то после сопряжения там также будет элемент множества $A_{\nu_1\nu_2\dots\nu_s}$), позволяет ввести некоторое обоб-

щение разложения подстановки в произведение независимых циклов.

Рассмотрим множество

$K = \{i_1 i_2 \dots i_s | i_1 < i_2 < \dots < i_s, s \le n, i_1, i_2, \dots, i_s \in \mathbb{Z}_k\}$

и введём в функцию-индикатор $I: \mathbb{Z}_k^n \to K$, которая определяется следующим образом: если $(x_1, x_2, \dots, x_n) \in A_{\nu_1 \nu_2 \dots \nu_s}$, то $I(x_1, x_2, \dots, x_n) = \nu_1 \nu_2 \dots \nu_s$. (Так как множества $A_{\nu_1 \nu_2 \dots \nu_s}$ не пересекаются, функция определена корректно)

Определение 7. Пусть $\pi \in \Pi$. Назовём обобщённым разложением подстановки π таблицу, построенную следующим способом:

Подстановка π раскладывается в произведение независимых циклов, каждый цикл записывается в качестве строки таблицы;

К элементам строк применяется функция I.

Замечание. Для любой подстановки $\pi \in \Pi$ обобщённое разложение определено однозначно с точностью до перестановки строк и циклического сдвига элементов в них.

Приведённые рассуждения позволяют предложить алгоритм построения функций из множества Π с любой заранее заданной цикловой структурой, если множество Π не пусто. Основная идея алгоритма заключается в том, что вместо всех возможных подстановок опробуются их обобщённые разложения, количество которых значительно меньше $(k^n)!$.

Алгоритм

Вход: Цикловая структура подстановки π.

Выход: Подстановка $\pi \in \Pi$ либо сообщение, что такой подстановки не существует.

Шаг 1. Составляется таблица с количеством строк равным количеству циклов в цикловой структуре, длина строки равна длине соответствующего ей цикла. Пусть для определённости число строк равно m.

Шаг 2. Создаётся мультимножество $\langle I(x_1, x_2, \dots, x_n) | (x_1, x_2, \dots, x_n) \in \mathbb{Z}_k^n \rangle$, состоящее из всех образов функции I от элементов множества $\mathbb{Z}_k^n$.

Шаг 3. Последовательно опробуются все варианты размещений элементов мультимножества в ячейках таблицы до достижения успеха. Успехом считается такое заполнение таблицы, при котором для любых двух соседних элементов $i_1 i_2 \dots i_s$ и $j_1 j_2 \dots j_t$ любой строки (соседними также считаются первый и последний элементы строки) выполняется условие $\{i_1, i_2, \dots, i_s\} \cap \{j_1, j_2, \dots, j_t\} = \emptyset$. В случае, если были опробованы все возможные размещения, а успех не был достигнут, алгоритм заканчивает работу сообщением о невозможности существования подстановки π.

Шаг 4. Последовательно перебираются все элементы множества K , при этом если выбран элемент $i_1 i_2 \dots i_s$, то все элементы таблицы с таким же значением заменяются элементами множества $A_{i_1 i_2 \dots i_s}$ по схеме случайной выборки без возвращения. Таким образом, в строках полученной таблицы выписаны все циклы из разложения подстановки π в произведение независимых циклов. Оно и подаётся на выход алгоритма.

Теорема 5. Алгоритм построения подстановки из класса Π работает корректно.

Доказательство. В процессе работы алгоритма происходит опробование всех возможных обобщённых разложений подстановок из $S(\mathbb{Z}_k^n)$. Для каждого опробуемого варианта производится проверка выполнения условия, эквивалентного условию $\pi(A_{\nu_1 \nu_2 \dots \nu_s}) \cap B_{\nu_1 \nu_2 \dots \nu_s} = \emptyset$, которое является критерием проверки принадлежности подстановки к классу Π. Таким образом, любая подстановка, обладающая обобщённым разложением, удовлетворяющим данному условию, принадлежит к множеству Π. Из способа построения строк таблицы видно, что цикловая структура полученной в результате работы алгоритма подстановки соответствует искомой.

Замечание. Данный алгоритм применялся для построения примера 4.

Утверждение 5. В процессе работы алгоритма происходит не более

$$\frac{(k^n)!}{\left(\prod_{i=1}^{r} m_i! l_i^{m_i}\right)\left(\prod_{i=1}^{n} ((S(n,i)s!)!)^{\binom{k}{s}}\right)}$$

опробований заполнений таблицы, где $\left[l_1^{m_1}, l_2^{m_2}, \dots, l_r^{m_r}\right]$ – цикловая структура подстановки π.

Доказательство. Общее количество подстановок с заданной цикловой структурой $\left[l_1^{m_1}, l_2^{m_2}, \dots, l_r^{m_r}\right]$ равно $\frac{(k^n)!}{\left(\prod_{i=1}^{r} m_i! l_i^{m_i}\right)}$. Заметим, что подстановки $\varphi, \tau \epsilon S(\mathbb{Z}_k^n)$ обладают одинаковым обобщённым разложением тогда и только то-

гда, когда существует $\sigma \in M$, для которой $\varphi = \sigma^{-1} \cdot \tau \cdot \sigma$. Отсюда получаем, что каждому варианту обобщённого разложения соответствуют ровно $\prod_{i=1}^{n}\left((S(n,i)s!)!\right)^{\binom{k}{s}}$ подстановок с одинаковой цикловой структурой. Тогда количество возможных обобщённых разложений для заданной цикловой структуры в $\prod_{i=1}^{n}\left((S(n,i)s!)!\right)^{\binom{k}{s}}$ раз меньше количества всех подстановок. Следовательно, их количество равно $\frac{(k^n)!}{\left(\prod_{i=1}^{r} m_i! l_i^{m_i}\right)\left(\prod_{i=1}^{n}((S(n,i)s!)!)^{\binom{k}{s}}\right)}$.

Список литературы:

1. Сачков В.Н. Курс комбинаторного анализа. М.-Ижевск: НИЦ «РХД», 2013.

2. Фомичёв В.М. Дискретная математика и криптология. –Москва: «Диалог-МИФИ», 2003.

3. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра . 2003. Т. 1, 2.

4. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. –Москва: Гелиос АРВ, 2005.

5. Глухов М.М., Шишков А.Б. Математическая логика. Дискретные функции. Теория алгоритмов. СПб. –М. –Краснодар: Лань, 2012.

РЕЦЕНЗИЯ

Высокоскоростная передача больших объемов информации в современных каналах связи и управления делает актуальным переход к обработке даже не битовых, а векторных массивов данных (по существу, k-значных при $k = 2^m$). В связи с этим возрастает интерес к проведению теоретических и прикладных исследований в области реализации дискретных преобразований в k-значной логике. Переход от булевых операций к k-значным приводит к обнаружению их новых интересных свойств. В представленной статье внимание авторов сосредоточено на изучении класса k-значных функций с запретными знаками подфункций, существующего при $k \geq 3$. Исследуемый класс введен в рассмотрение впервые, поэтому данная статья характеризуется несомненной новизной и, как показали полученные результаты, оригинальностью постановок задач и выводов.

В статье выделяются три части, первая из которых посвящена общей характеризации изучаемого класса функций. Во второй части проведено изучение периодических свойств автономного регистра сдвига с функцией обратной связи из выделенного класса. Наибольший интерес представляет третья часть статьи, в которой разработаны способы синтеза биективных отображений с помощью изучаемых функций.

Авторы придерживаются математического стиля изложения материала, формулируя основные результаты в виде теорем, которые строго доказываются. Возможно, статья бы выиграла, если бы она содержала большее количество примеров и пояснений.

В целом, можно заключить, что данная статья посвящена анализу перспективных подходов к созданию узлов переработки k-значной информации на новой элементной базе и может быть рекомендована к опубликованию в журнале Computational Nanotechnology.

Кандидат физико-математических наук,
доцент

Рыбников К.К.