УДК 512.13

ПОСТРОЕНИЕ ПОДСТАНОВОК НА ОСНОВЕ ПОРОГОВЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Д. А. Сошин

ФГУП «НИИ «Квант», г. Москва, Россия

Предложен алгоритм построения биективных отображений с помощью координатных пороговых функций k-значной логики. Алгоритм включает геометрический способ построения сбалансированных пороговых функций и два подхода к синтезу регулярных систем с приведением экспериментальных результатов.

Ключевые слова: *пороговые функции, многозначная логика, сбалансированные функции, регулярные системы.*

DOI 10.17223/20710410/32/2

CONSTRUCTING SUBSTITUTIONS ON THE BASIS OF THRESHOLD FUNCTIONS OF MULTIVALUED LOGIC

D. A. Soshin

Technology Federal State Unitary Enterprise "Research Institute Kvant", Moscow, Russia

E-mail: danil_re@list.ru

An algorithm for building one-to-one mappings (substitutions) with the help of coordinate threshold k-valued logic functions is presented. The algorithm includes a geometric way of generating balanced threshold functions and two ways to produce substitutions from these functions — by forming triangular systems and by algorithmic searching. Results of experimental testing the algorithms are given.

Keywords: *threshold functions, multiple-valued logic, balanced functions, regular systems.*

Введение

Работа посвящена построению подстановок на основе пороговых функций k-значной логики [1 – 4]. Для этого на первом этапе, в соответствии с требованиями критерия Хаффмана, строится класс сбалансированных пороговых k-значных функций от n переменных, для любых $n \geqslant 3$ и $k \geqslant 2$. Сбалансированные функции представляют и самостоятельный интерес при синтезе узлов переработки дискретной информации с точки зрения своих статистических свойств [5]. На втором этапе при помощи сбалансированных функций описанного класса строятся компактно реализуемые подстановки [4, 6]. В работе предложены два способа построения подстановок. Первый основан на формировании треугольных систем с использованием пороговых функций, которые заведомо порождают подстановки. Второй способ применяет алгоритмический поиск подстановки на базе одной из сбалансированных функций с помощью легко реализуемых операций, обобщающих преобразования движения или вращения. Доказаны утверждения, позволяющие сократить количество проверяемых вариантов. В заключение приведены результаты применения построенного алгоритма поиска регулярных систем.

1. Геометрический метод синтеза k-значных сбалансированных пороговых функций

Будем обозначать $\Omega_k = \{0, 1, \ldots, k-1\}$.

Определение 1. Функция k-значной логики $f : \Omega_k^n \longrightarrow \Omega_k$ называется пороговой, если для нее существует линейная форма

$$L(x_1, x_2, \ldots, x_n) = c_1x_1 + c_2x_2 + \ldots + c_nx_n, \quad c_i \in \mathbb{Z},\ i = 1, \ldots, n,$$

и пороги $b_0, b_1, \ldots, b_k \in \mathbb{Z}$, такие, что для любого $\alpha \in \{0, \ldots, k-1\}$ выполняется

$$f(x_1, x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant c_1x_1 + c_2x_2 + \ldots + c_nx_n < b_{\alpha+1}.$$

Определение 2. Слоем $D_\alpha(f)$ (носителем значения α) пороговой функции f будем называть те и только те точки множества Ω_k^n, в которых функция f принимает значение α, $\alpha = 0, \ldots, k-1$. Если из контекста понятно, слой какой функции рассматривается, будем опускать символ функции и писать D_α.

В геометрическом смысле каждое неравенство $c_1x_1 + c_2x_2 + \ldots + c_nx_n < b_\alpha$ задаёт полупространство, лежащее по одну сторону от гиперплоскости L_α, определяемой равенством $c_1x_1 + c_2x_2 + \ldots + c_nx_n = b_\alpha$, а слой D_α — множество целочисленных точек n-мерного куба со стороной длины $k-1$, расположенных между двумя соседними гиперплоскостями L_α и $L_{\alpha+1}$, включая точки гиперплоскости L_α.

Далее пороги b_0 и b_k и соответствующие им гиперплоскости L_0 и L_k рассматривать не будем, поскольку они не несут смысловой нагрузки.

Функция f является сбалансированной, если слои $D_\alpha(f)$, $\alpha = 0, \ldots, k-1$, равномощные.

Для описания метода построения сбалансированных пороговых функций введём понятие среза S_α — множества точек $\{(a_1, a_2, \ldots, a_{n-1}, \alpha) \in \Omega_k^n\}$. Будем говорить, что гиперплоскость $L_\alpha(x_1, x_2, \ldots, x_n) = 0$, где $L_\alpha(x_1, x_2, \ldots, x_n) = c_1x_1 + c_2x_2 + \ldots + c_nx_n + b_\alpha$, пересекает срез, если существуют две точки этого среза, для которых выполняется одно из условий:

1) эти точки лежат по разные стороны от гиперплоскости [7];
2) одна точка принадлежит гиперплоскости, а для другой выполнено неравенство $L_\alpha(x_1, x_2, \ldots, x_n) < 0$.

Если $L_\alpha(x_1, x_2, \ldots, x_n) = 0$ — уравнение гиперплоскости, то будем говорить, что гиперплоскость отделяет (отсекает) точки среза S_α, если для этих точек выполнено условие

$$L_\alpha(a_1, a_2, \ldots, a_{n-1}, \alpha) \geqslant 0.$$

Геометрический метод построения сбалансированных пороговых функций основан на задании семейства параллельных гиперплоскостей L_α, $\alpha = 1, \ldots, k-1$, в n-мерном пространстве, каждая гиперплоскость которого проходит через соответствующий набор точек:

$$\begin{gathered} t^{(1)} = (r, 0, 0, 0, \ldots, 0, 0, \alpha), \\ t^{(2)} = (0, r, 0, 0, \ldots, 0, 0, \alpha), \\ \ldots \\ t^{(n-1)} = (0, 0, 0, 0, \ldots, 0, r, \alpha), \\ t^{(n)} = (k-r, k-1, \ldots, k-1, \alpha-1), \end{gathered} \tag{1}$$

то есть при подстановке их в $L_\alpha(x_1, x_2, \ldots, x_n)$ выполняется равенство

$$L_\alpha\left(t^{(j)}\right) = 0, \quad j = 1, \ldots, n.$$

Проходя через точки $t^{(1)}, t^{(2)}, \ldots, t^{(n-1)}$, гиперплоскость L_α отделяет в срезе S_α множество точек

$$\left\{(a_1, a_2, \ldots, a_{n-1}, \alpha) \in \Omega_k^n : a_1 + \ldots + a_{n-1} \geqslant r\right\},$$

которые не войдут в слой $D_{\alpha-1}$. Прохождение гиперплоскости через точку $t^{(n)}$ позволяет отделить в срезе $S_{\alpha-1}$ множество точек

$$\left\{(a_1, a_2, \ldots, a_{n-1}, \alpha - 1) \in \Omega_k^n : a_1 + \ldots + a_{n-1} \geqslant (k-1)(n-1) - r + 1\right\},$$

которые войдут в слой $D_{\alpha-1}$. В силу равномощности множеств

$$\left\{(a_1, a_2, \ldots, a_{n-1}, \alpha) \in \Omega_k^n : a_1 + \ldots + a_{n-1} \leqslant r - 1\right\}$$
$$\text{и} \quad \left\{(a_1, a_2, \ldots, a_{n-1}, \alpha - 1) \in \Omega_k^n : a_1 + \ldots + a_{n-1} \geqslant (k-1)(n-1) - r + 1\right\}$$

и в случае, если гиперплоскости L_α не пересекают более двух срезов, такая последовательная компенсация для каждого слоя позволяет сохранит сбалансированность.

Расстояние r будем называть *отступом* точек $t^{(1)}, t^{(2)}, \ldots, t^{(n-1)}$ от точки $(0, 0, \ldots, 0, \alpha)$ среза S_α. Отступ первых $n-1$ точек в системе (1) связан с удобством задания точки $t^{(n)}$ в срезе $S_{\alpha-1}$, через которую пройдёт гиперплоскость. Для случая произвольного выбора отступов необходимо найти самую близкую целочисленную точку среза $S_{\alpha-1}$ к прямой (для $n \geqslant 4$ — к гиперплоскости) пересечения плоскости L_α и плоскости $\widetilde{S}_{\alpha-1}$, описываемой уравнением $x_n = \alpha - 1$. В рассмотренном случае выбор последней точки не вызывает сложности. Для произвольных параметров n, k и произвольных отступов от крайней точки последняя задача не имеет общего решения, но для каждого фиксированного случая её можно решить и построить любую сбалансированную пороговую функцию.

Следующая теорема описывает пороговые сбалансированные функции, соответствующие данному семейству гиперплоскостей, задаваемых системами точек (1).

Теорема 1. Пусть $R_n = k - 2r + (n-2)(k-1)$, $P_\alpha^n = r + \alpha R_n$ для некоторых $k \geqslant 2$, $r \geqslant 1$, $n \geqslant 2$; $\alpha = 1, \ldots, k-1$. Пороговая функция $f(x_1, x_2, \ldots, x_n)$, заданная двусторонними неравенствами

$$f(x_1, x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant x_1 + x_2 + \ldots + R_n x_n < b_{\alpha+1}, \tag{2}$$

где $(b_1, b_2, \ldots, b_{k-1}) = (P_1^n, P_2^n, \ldots, P_{k-1}^n)$, при $(k-1)(n-1) > 3r - 2$ является сбалансированной пороговой.

Доказательство. Покажем, что пороговая функция (2) соответствует семейству гиперплоскостей L_α, отвечающим системам точек (1). Пусть уравнения семейства гиперплоскостей L_α имеют вид

$$c_1 x_1 + c_2 x_2 + \ldots + c_n x_n = b_\alpha.$$

Покажем, что значения порогов и коэффициентов линейной формы в условии теоремы равны соответствующим параметрам:

$$(b_1, b_2, \ldots, b_{k-1}) = (P_1^n, P_2^n, \ldots, P_{k-1}^n), \quad (c_1, c_2, \ldots, c_n) = (1, 1, \ldots, 1, R_n).$$

Уравнение $(n-1)$-мерной гиперплоскости, проходящей через точки $t^{(1)}, t^{(2)}, \ldots, t^{(n)}$, которые не лежат на одной $(n-2)$-мерной гиперплоскости, задаётся следующим образом [7]:

$$\left|\begin{pmatrix} x_1 - t_1^{(1)} & x_2 - t_2^{(1)} & \ldots & x_{n-1} - t_{n-1}^{(1)} & x_n - t_n^{(1)} \\ t_1^{(2)} - t_1^{(1)} & t_2^{(2)} - t_2^{(1)} & \ldots & t_{n-1}^{(2)} - t_{n-1}^{(1)} & t_n^{(2)} - t_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_1^{(n-1)} - t_1^{(1)} & t_2^{(n-1)} - t_2^{(1)} & \ldots & t_{n-1}^{(n-1)} - t_{n-1}^{(1)} & t_n^{(n-1)} - t_n^{(1)} \\ t_1^{(n)} - t_1^{(1)} & t_2^{(n)} - t_2^{(1)} & \ldots & t_{n-1}^{(n)} - t_{n-1}^{(1)} & t_n^{(n)} - t_n^{(1)} \end{pmatrix}\right| = 0.$$

Найдём данный определитель для рассматриваемого случая:

$$\Delta = \left|\begin{pmatrix} x_1 - r & x_2 & x_3 & x_4 & \ldots & x_{n-1} & x_n - \alpha \\ -r & r & 0 & 0 & \ldots & 0 & 0 \\ -r & 0 & r & 0 & \ldots & 0 & 0 \\ -r & 0 & 0 & r & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -r & 0 & 0 & 0 & \ldots & r & 0 \\ k-2r & k-1 & k-1 & k-1 & \ldots & k-1 & -1 \end{pmatrix}\right|.$$

Добавим к первому столбцу все столбцы, кроме последнего. Столбец с номером n, умноженный на $k - 2r + (n-2)(k-1)$, прибавим к первому столбцу; к остальным столбцам добавим его же, умноженным на $k-1$. Через $*$ обозначим элементы матрицы, которые не влияют на значение определителя. В результате получим

$$\Delta = \left|\begin{pmatrix} x_1 + x_2 + \ldots + x_{n-1} + (x_n - \alpha)(k - 2r + (n-2)(k-1)) - r & * & * & \ldots & * & * \\ 0 & r & 0 & \ldots & 0 & 0 \\ 0 & 0 & r & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & r & 0 \\ 0 & 0 & 0 & \ldots & 0 & -1 \end{pmatrix}\right| =$$

$$= -r^{n-2}\left(x_1 + x_2 + \ldots + x_{n-1} + (x_n - \alpha)(k - 2r + (n-2)(k-1)) - r\right).$$

Приравняем $\Delta = 0$ и перенесём свободный член в правую часть:

$$-r^{n-2}(x_1 + x_2 + \ldots + x_{n-1} + (x_n - \alpha)(k - 2r + (n-2)(k-1)) - r) = 0,$$
$$x_1 + x_2 + \ldots + x_{n-1} + (x_n - \alpha)(k - 2r + (n-2)(k-1)) - r = 0,$$
$$x_1 + x_2 + \ldots + x_{n-1} + x_n(k - 2r + (n-2)(k-1)) = \alpha(k - 2r + (n-2)(k-1)) + r,$$
$$x_1 + x_2 + \ldots + x_{n-1} + x_n R_n = P_\alpha^n.$$

Последнее равенство доказывает требуемое соответствие.

Докажем выполнение условия сбалансированности. Для этого необходимо проверить, что гиперплоскость L_α не пересекает срез $S_{\alpha-2}$. Для выполнения этого условия достаточно, чтобы линейная форма $L = x_1 + \ldots + x_{n-1} + x_n R_n$ в точке $t = (k-1, k-1, \ldots, k-1, \alpha-2)$ принимала значение строго меньше P_α^n:

$$L(t) = (n-1)(k-1) + (\alpha-2)R_n < P_\alpha^n = r + \alpha R_n.$$

Последовательно получаем

$$r + \alpha R_n > (n-1)(k-1) + (\alpha - 2)R_n,$$
$$r > (n-1)(k-1) - 2R_n.$$
$$r > (k-1)(n-1) - 2(k - 2r + (n-2)(k-1)),$$
$$r > -(k-1)(n-1) + 4r - 2,$$
$$(k-1)(n-1) > 3r - 2.$$

Последнее неравенство выполнено по условию. ■

Замечание 1. При добавлении фиктивных переменных у функций, построенных в теореме 1, свойство сбалансированности не нарушается. Теорема 2 описывает сбалансированные функции построенного типа с произвольным количеством фиктивных переменных.

Теорема 2. В обозначениях теоремы 1 при $(k-1)(n-m-1) > 3r-2, 0 \leqslant m \leqslant n-2$ пороговая функция $f^k(x_1, x_2, \ldots, x_n)$, заданная двусторонними неравенствами

$$f(x_1, x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant x_{m+1} + x_{m+2} + \ldots + x_n R_{n-m} < b_{\alpha+1}, \tag{3}$$

где $(b_1, b_2, \ldots, b_{k-1}) = (P_1^{n-m}, P_2^{n-m}, \ldots, P_{k-1}^{n-m})$, является сбалансированной пороговой.

Доказательство. Справедливость теоремы 2 следует из замечания 1 и теоремы 1 при замене n на $n - m$. ■

При $m = 0$ утверждение теоремы 2 совпадает с утверждением теоремы 1.

Приведём пример построения функции для фиксированных параметров с неодинаковыми отступами.

Пример 1. Пусть $n = 3$, $k = 3$, отступы от крайней точки равны 2 по первой и 1 по второй переменной. Тогда набор точек, через которые пройдёт соответствующее семейство плоскостей, следующий:

$$t^{(1)} = (2, 0, \alpha), \quad t^{(2)} = (0, 1, \alpha), \quad t^{(3)} = (1, 2, \alpha - 1), \quad \alpha \in \{1, 2\}.$$

Найдём уравнения плоскостей, проходящих через точки $t^{(1)}, t^{(2)}, t^{(3)}$; для этого необходимо найти соответствующий определитель Δ и приравнять его к нулю:

$$\Delta = \left| \begin{pmatrix} x_1 - 2 & x_2 & x_3 - \alpha \\ -2 & 1 & 0 \\ -1 & 2 & -1 \end{pmatrix} \right| = \left| \begin{pmatrix} x_1 - x_3 + \alpha - 2 & x_2 + 2x_3 - 2\alpha & x_3 - \alpha \\ -2 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right| =$$
$$= \left| \begin{pmatrix} x_1 - x_3 + \alpha - 2 + 2(x_2 + 2x_3 - 2\alpha) & x_2 + 2x_3 - 2\alpha & x_3 - \alpha \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right| =$$
$$= -(x_1 - x_3 + \alpha - 2 + 2(x_2 + 2x_3 - 2\alpha)) = -(x_1 + 2x_2 + 3x_3 - 3\alpha - 2).$$

Приравнивая $\Delta = 0$, получим уравнения плоскостей для $\alpha \in \{1, 2\}$:

$$x_1 + 2x_2 + 3x_3 = 3\alpha + 2.$$

Вектор порогов данной функции следующий: $(b_1, b_2) = (5, 8)$. Прохождение плоскостей через соответствующий куб изображено на рис. 1.

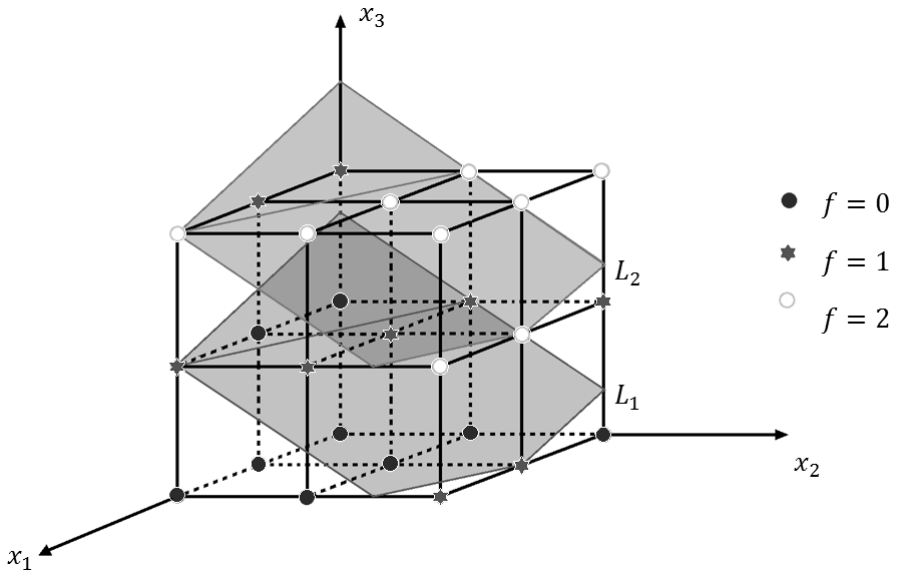

Рис. 1. Функция, построенная в примере 1 на трёхмерном кубе трёхзначной логики; L_1 и L_2 — построенные плоскости

2. Построение подстановок на основе сбалансированных k-значных пороговых функций

Рассмотрим два способа построения подстановок. Система координатных функций задаёт подстановку, если она регулярна. Проверка системы на регулярность является сложной задачей. Существующие критерии, в частности критерий Хаффмана, не позволяют оптимизировать проверку на регулярность, но в некоторых случаях дают возможность сузить множество проверяемых на регулярность систем, отбраковав заведомо ложные.

Определение 3. Координатное отображение $F : \Omega_k^n \to \Omega_k^n$,

$$F(x_1, x_2, \ldots, x_n) = (f_1(x), f_2(x), \ldots, f_n(x)), \tag{4}$$

где $f_i(x) = f_i(x_1, x_2, \ldots, x_n)$ — k-значные функции, называется биективным, а система функций $f_1(x), f_2(x), \ldots, f_n(x)$ — регулярной системой, если F — взаимно-однозначное отображение.

Первый предлагаемый способ основан на построении треугольных регулярных систем, второй — на построении подстановок, координатные функции которых являются однотипными k-значными функциями, полученными из одной путём действия преобразований перестановки переменных и их инвертирования.

2.1. Построение подстановок на основе сбалансированных k-значных пороговых функций

Определение 4. Система функций $f_1(x), f_2(x), \ldots, f_n(x)$ называется треугольной, если она имеет вид

$$\begin{cases} f_1(x) = \varphi_1(x_1), \\ f_2(x) = \varphi_2(x_1, x_2), \\ \ldots \\ f_i(x) = \varphi_i(x_1, x_2, \ldots, x_i), \\ \ldots \\ f_n(x) = \varphi_n(x_1, x_2, \ldots, x_n), \end{cases} \tag{5}$$

где $\varphi_1, \varphi_2, \ldots, \varphi_n$ — произвольные k-значные функции.

Если функция φ_i, $i = 1, \ldots, n$, биективна по переменной x_i, т. е. при каждой фиксации переменных $x_1, x_2, \ldots, x_{i-1}$ функция φ_i задаёт подстановочное отображение [8, с. 166], то система (5) задаёт биекцию. Действительно, пусть задано равенство

$$(\varphi_1, \varphi_2, \ldots, \varphi_n)(x_1, x_2, \ldots, x_n) = (a_1, a_2, \ldots, a_n), \tag{6}$$

тогда $\varphi_1(x_1) = (a_1)$. В силу биективности функции $\varphi_1(x_1)$ по переменной x_1 существует и единственен элемент $b_1 \in \Omega_k$, такой, что $\varphi_1(b_1) = a_1$. Положим $x_1 = b_1$. Ввиду биективности функции φ_2 по переменной x_2 существует и единственен $b_2 \in \Omega_k$, такой, что $\varphi_2(b_1, b_2) = a_2$. Положим $x_2 = b_2$. Продолжая дальше по индукции, получаем, что существует единственный набор $(x_1, x_2, \ldots, x_n) = (b_1, b_2, \ldots, b_n) \in \Omega_k^n$, удовлетворяющий равенству (6).

В качестве треугольной регулярной системы можно предложить систему вида

$$\begin{cases} \varphi_1(x_1) = x_1, \\ \varphi_2(x_1, x_2) = x_2 + \psi_2(x_1) \mod k, \\ \ldots \\ \varphi_n(x_1, x_2, \ldots, x_n) = x_n + \psi_n(x_1, x_2, \ldots, x_{n-1}) \mod k. \end{cases} \tag{7}$$

Данная система регулярна для любых k-значных функций $\psi_2, \psi_3, \ldots, \psi_n$, поскольку каждая φ_i биективна по крайней переменной независимо от значений функции ψ_i.

Среди систем (7) представляют интерес системы на основе функций (3) из теоремы 2. Пороговые функции (3) будем обозначать следующим образом:

$$T_r^m(x_1, x_2, \ldots, x_n), \tag{8}$$

где m — количество фиктивных переменных; r — параметр, отвечающий за размер отступа от крайних точек среза, тем самым отвечающий за размер отсекаемой области среза. Систему порогов и максимальный коэффициент линейной формы будем обозначать $(b_1, b_2, \ldots, b_{k-1}) = \left(P_1^{n-m}(r), P_2^{n-m}(r), \ldots, P_{k-1}^{n-m}(r)\right)$ и $R_{n-m}(r)$ соответственно.

Для дальнейшего использования доопределим множество функций (8) для случая $n = 1$: $T_r^0(x_1) = x_1$, $R_1(r) = 1$, $P_i(r) = i$, $i = 1, \ldots, k-1$.

Можно рассмотреть два способа задания функций $\psi_2, \psi_3, \ldots, \psi_n$. Первый способ позволяет параллельно вычислять значения координатных функций, что ускоряет ре-

ализацию подстановки, а именно:

$$\begin{cases} \psi_2(x_1) = T_{r_1}^{n-1}(0,0,\ldots,0,x_1), \\ \psi_3(x_1,x_2) = T_{r_2}^{n-2}(0,0,\ldots,0,x_1,x_2), \\ \ldots \\ \psi_i(x_1,x_2,\ldots,x_{i-1}) = T_{r_{i-1}}^{n-i+1}(0,0,\ldots,0,x_1,x_2,\ldots,x_{i-1}), \\ \ldots \\ \psi_n(x_1,x_2,\ldots,x_{n-1}) = T_{r_{n-1}}^{1}(0,x_1,x_2,\ldots,x_{n-1}). \end{cases} \tag{9}$$

Второй способ реализует рекуррентное определение значений координатных функций, основанное на последовательном задании функций ψ_i:

$$\begin{cases} \psi_2(y_1) = T_{r_1}^{n-1}(0,0,\ldots,0,y_1), \\ \psi_3(y_1,y_2) = T_{r_2}^{n-2}(0,0,\ldots,0,y_1,y_2), \\ \ldots \\ \psi_i(y_1,y_2,\ldots,y_{i-1}) = T_{r_{i-1}}^{n-i+1}(0,0,\ldots,0,y_1,y_2,\ldots,y_{i-1}), \\ \ldots \\ \psi_n(y_1,y_2,\ldots,y_{n-1}) = T_{r_{n-1}}^{1}(0,y_1,y_2,\ldots,y_{n-1}), \end{cases} \tag{10}$$

где

$$\begin{cases} y_1(x_1) = \varphi_1(x_1) = x_1, \\ y_2(x_1,x_2) = \varphi_2(x_1,x_2) = x_2 + \psi_2(x_1) \mod k, \\ \ldots \\ y_{n-1}(x_1,x_2,\ldots,x_{n-1}) = \varphi_{n-1}(x_1,x_2,\ldots,x_{n-1}) = x_{n-1} + \psi_n(x_1,x_2,\ldots,x_{n-2}) \mod k. \end{cases}$$

Удобство использования систем (7) с функциями (9) или (10) заключается в том, что для задания подстановки достаточно хранить коэффициенты линейных форм пороговых функций и систему порогов. Матрицы C и P содержат всю информацию о задаваемых подстановках указанного типа:

$$C = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & R_1(r_1) \\ 0 & 0 & 0 & \ldots & 0 & 1 & R_2(r_2) \\ 0 & 0 & 0 & \ldots & 1 & 1 & R_3(r_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \ldots & 1 & 1 & R_{n-2}(r_{n-2}) \\ 0 & 1 & 1 & \ldots & 1 & 1 & R_{n-1}(r_{n-1}) \end{pmatrix}, \tag{11}$$

$$P = \begin{pmatrix} P_1^1(r_1) & P_2^1(r_1) & \ldots & P_{k-1}^1(r_1) \\ P_1^2(r_2) & P_2^2(r_2) & \ldots & P_{k-1}^2(r_2) \\ \vdots & \vdots & \ddots & \vdots \\ P_1^{n-1}(r_{n-1}) & P_2^{n-1}(r_{n-1}) & \ldots & P_{k-1}^{n-1}(r_{n-1}) \end{pmatrix}.$$

Элемент $c_{i,j}$ матрицы C задаёт коэффициент линейной формы i-й координатной пороговой функции при переменной x_j. Например, линейная форма i-й пороговой функции имеет вид $L = x_1 + x_2 + \ldots + x_{i-1} + x_i R_i(r_i)$ и соответствует линейной форме функции $\psi_i(x_1,x_2,\ldots,x_i)$ систем (9) и (10). В матрице P строка с номером i задаёт систему порогов i-й пороговой функции.

2.2. Построение подстановок на основе систем однотипных пороговых функций

Второй способ основан на построении подстановок, координатные функции которых являются однотипными k-значными функциями, полученными из одной (стрелки Лукашевича) путём действия преобразований перестановки переменных и их инвертирования. В этом способе представления нашли своё воплощение три идеи, каждая из которых определяет потенциальные преимущества при реализации подстановки.

Во-первых, в предложенном способе заложен принцип компактной реализации, при котором для вычисления координат результирующего вектора используется единая функция с простым сервисным преобразованием, аналогичным преобразованию однотипности в булевом случае.

Во-вторых, по всем координатам функции, задающие отображение, — пороговые, для которых в перспективной элементной базе, например оптической, может быть осуществлена реализация в среде-носителе сигнала с высоким быстродействием.

И наконец, третьим преимуществом является сбалансированность и временнàя синхронизация выработки значений всех координат выходного вектора.

Остановимся подробно на преобразованиях, используемых при генерации функций по каждому каналу. Группой движения G_n назовем группу, порождённую группами S_n и N_n:

$$G_n = \langle S_n, N_n \rangle,$$

где S_n — группа подстановок на множестве $\{1, \dots, n\}$; $N_n = \{-1, 1\}^n$ — группа инвертирования переменных. Действие данных групп на множестве Ω_k^n определяется следующим образом: для любой точки $(a_1, a_2, \dots, a_n) \in \Omega_k^n$, для любых преобразований $s \in S_n$ и $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in N_n$

$$(a_1, a_2, \dots, a_n)^s = (a_{s^{-1}(1)}, a_{s^{-1}(2)}, \dots, a_{s^{-1}(n)}),$$

$$(a_1, a_2, \dots, a_n)^\beta = (u_1, u_2, \dots, u_n), \qquad u_i = \begin{cases} a_i, \text{ если } \beta_i = 1, \\ k - 1 - a_i, \text{ если } \beta_i = -1. \end{cases}$$

Обозначим через $(\beta s)\, T_r^m$ функцию, полученную из функции T_r^m по правилу $(\beta s)\, T_r^m = T_r^m(x^{\beta s})$. Системе k-значных пороговых функций

$$F_r^m(\beta, s) = \left(\beta^{(1)} s^{(1)}\right) T_r^m, \left(\beta^{(2)} s^{(2)}\right) T_r^m, \dots, \left(\beta^{(n)} s^{(n)}\right) T_r^m, \tag{12}$$

где $\beta = (\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(n)}) \in (N_n)^n$; $s = (s^{(1)}, s^{(2)}, \dots, s^{(n)}) \in (S_n)^n$, поставим в соответствие матрицу $C = (c_{i,j})_{n \times n}$ аналогично матрице (11) с учётом действия преобразований из группы N_n. Например, функции $(\beta\varepsilon) T_r^m$, где ε — нейтральный элемент группы S_n, $\beta = (\beta_1, \beta_2, \dots, \beta_n)$, соответствует строка матрицы $(\beta_1, \beta_2, \dots, \beta_n R_{n-m}(r))$. Каждой системе (12) соответствует отображение, задаваемое по правилу

$$\begin{gathered} \pi[F_r^m(\beta, s)](x_1, x_2, \dots, x_n) = \\ = \left(\left(\beta^{(1)} s^{(1)}\right) T_r^m(x_1,\ x_2, \dots, x_n), \dots, \left(\beta^{(n)} s^{(n)}\right) T_r^m(x_1, x_2, \dots, x_n)\right). \end{gathered} \tag{13}$$

В случае регулярности системы $F_r^m(\beta, s)$ отображение $\pi[F_r^m(\beta, s)]$ задаёт подстановку на множестве Ω_k^n.

Поиск регулярной системы осуществляется алгоритмическим способом, а именно путём перебора функций $\left(\beta^{(i)} s^{(i)}\right) T_r^m$ и проверки факта порождения подстановки. Приведём формулировку критерия Хаффмана и утверждение, позволяющее сократить количество проверяемых систем $F_r^m(\beta, s)$ на регулярность для произвольных параметров m и r, удовлетворяющих условиям теоремы 2.

Теорема 3 (критерий Хаффмана). Система k-значных функций $f_i(x_1, \ldots, x_n)$, $i = 1, \ldots, n$, регулярна тогда и только тогда, когда для любых $r \in \{1, \ldots, n\}$, $1 \leqslant i_1 < i_2 < \ldots < i_r \leqslant n$ и $\alpha_1, \alpha_2, \ldots, \alpha_r \in \{0, \ldots, k-1\}$ выполняется

$$\left| \bigcap_{w=1}^{r} D_{\alpha_w}(f_{i_w}) \right| = k^{n-r}.$$

Теорема 4. Пусть для некоторых $(s^{(1)}, s^{(2)}, \ldots, s^{(n)}) \in (S_n)^n$ и любых $\beta = (\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)}) \in (N_n)^n$ при $k > 3$ в матрице C, отвечающей системе $F_r^m(\beta, s)$, существуют две различные строки вида

$$\left(\theta_1^i\beta_1^{(i)} \quad \theta_2^i\beta_2^{(i)} \quad \ldots \quad \theta_{p-1}^i\beta_{p-1}^{(i)} \quad \beta_p^{(i)}R_{n-m}(r) \quad \theta_{p+1}^i\beta_{p+1}^{(i)} \quad \ldots \quad \theta_n^i\beta_n^{(i)}\right),$$
$$\left(\theta_1^j\beta_1^{(j)} \quad \theta_2^j\beta_2^{(j)} \quad \ldots \quad \theta_{p-1}^j\beta_{p-1}^{(j)} \quad \beta_p^{(j)}R_{n-m}(r) \quad \theta_{p+1}^j\beta_{p+1}^{(j)} \quad \ldots \quad \theta_n^j\beta_n^{(j)}\right),$$

где θ_u^i, θ_u^j — индикаторы фиктивности (существенности) соответствующих переменных; $\sum\limits_{u \neq p} \theta_u^i = \sum\limits_{u \neq p} \theta_u^j = n - m + 1$. Тогда отображение $\pi[F_r^m(\beta, s)]$ не является биекцией.

Доказательство. Не ограничивая общности, положим $p = n$. Пусть f и g — функции, соответствующие строкам i и j матрицы C. Зафиксируем $\alpha = \beta_n^{(i)}(0)$ и $\delta = \beta_n^{(j)}(k-1)$. Тогда справедливы включения $D_\alpha(f) \subset S_0 \cup S_1$, $D_\delta(g) \subset S_{k-2} \cup S_{k-1}$. Поскольку $k > 3$, то $(S_0 \cup S_1) \cap (S_{k-2} \cup S_{k-1}) = \varnothing$. Из последних трёх выражений получаем $D_\alpha(f) \cap D_\delta(g) = \varnothing$, что противоречит условию критерия Хаффмана. ■

Следствие 1. Теорема 4 позволяет сократить перебор отображений (13), проверяемых на регулярность при фиксированных параметрах r и m, где $(k-1)(n-m-1) > 3r - 2$, в n^n раз

Доказательство. Действительно, тотальный поиск биективных отображений (13) состоит из задания соответствующей матрицы C и проверки на регулярность порождаемого ею преобразования. Выбор матриц C осуществляется за счёт расположения коэффициента $R_{n-m}(r)$ в каждой строке (n^n вариантов), задания у каждой координатной функции фиктивных переменных (C_{n-1}^m вариантов) и определения инвертирования существенных переменных, что потребует рассмотрения $2^{(n-m)n}$ вариантов, где $(n-m)n$ — количество ненулевых элементов матрицы C. Следовательно, на основе матрицы C проверке подвергаются $N = n^n C_{n-1}^m 2^{(n-m)n}$ систем.

Из теоремы 4 следует, что в каждом столбце и в каждой строке матрицы, соответствующей отображению (13), должен присутствовать единственный максимальный по модулю коэффициент $\beta_p^{(j)}R_{n-m}(r)$. Перестановкой строк матрицы C можно расположить коэффициенты $\beta_p^{(j)}R_{n-m}(r)$ на главной диагонали, поскольку перестановка координатных функций не нарушает биективности. Таким образом, перебор заключается в фиксации фиктивных переменных и расстановке инвертирования существенных переменных, что составляет $C_{n-1}^m 2^{(n-m)n}$ вариантов. ■

Приведём алгоритм поиска биективных отображений (алгоритм 1).

Приведём результаты применения программы, реализующей данный алгоритм на основе матрицы C. Во всех случаях n — размерность пространства, k — значность логики, m — количество фиктивных переменных, r — параметр, отвечающий за размер отсекаемой области, $R_{n-m}(r)$ определено условием теоремы 2, $\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)} \in N_n$ — перебираемые параметры.

Алгоритм 1. Поиск биективных отображений

1: Инициализируем параметры $j := 0$, n, k, m, r, $R_{n-m}(r)$, $P_0^{n-m}(r)$, $(P_1^{n-m}(r), \ldots, P_{k-2}^{n-m}(r))$.
2: Проверяем условие сбалансированности $(k-1)(n-m-1) > 3r+2$. Если выполнено, то на шаг 3, иначе сообщение «Функция не сбалансирована», конец алгоритма.
3: Инициализируем матрицу коэффициентов C. На главной диагонали располагаем максимальный коэффициент $R_{n-m}(r)$, оставшиеся элементы каждой строчки заполняем m нулями и $n-m-1$ единицами согласно рассматриваемому случаю.
4: Для каждого из 2^{n-m} способов задаём знаки ненулевых коэффициентов матрицы C, проверяем на биективность получившуюся систему. Если биекция, то $j := j+1$.

Выход: j — количество найденных подстановок для проверяемого случая.

С л у ч а й 1. Общие параметры $m = 0$,

$$C^{(1)} = \begin{pmatrix} \beta_1^{(1)} R_n(r) & \beta_2^{(1)} & \ldots & \beta_{n-1}^{(1)} & \beta_n^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} R_n(r) & \ldots & \beta_{n-1}^{(2)} & \beta_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta_1^{(n-1)} & \beta_2^{(n-1)} & \ldots & \beta_{n-1}^{(n-1)} R_n(r) & \beta_n^{(n-1)} \\ \beta_1^{(n)} & \beta_2^{(n)} & \ldots & \beta_{n-1}^{(n)} & \beta_n^{(n)} R_n(r) \end{pmatrix}.$$

Для заданных m и $C^{(1)}$ рассмотрим два способа задания размера отступа r.

Первый способ соответствует $r = 1$, количество подстановок, полученных за счёт перебора $\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)} \in N_n$, представлено в табл. 1.

Т а б л и ц а 1

	k														
n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	–	8	8	8	8	8	8	8	8	8	8	8	8	8	8
3	192	64	64	64	64	64	64	64	64	64	64	64	64	64	64
4	3328	768	768	768	768	768	768	–	–	–	–	–	–	–	–
5	76800	12288	12288	–	–	–	–	–	–	–	–	–	–	–	–

Во втором способе для каждого варианта параметров n и k будем задавать максимально возможный размер отступа $r = r_{\max}(k, n, m)$, удовлетворяющий условию сбалансированности теоремы 2. Значения $r_{\max}(k, n, m)$ и количества подстановок, полученных за счёт перебора $\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)} \in N_n$, представлены в табл. 2.

Т а б л и ц а 2

	k												
n	2	3	4	5	6	7	8	9	10	11	12	13	14
3	1; 192	1; 64	2; 0	3; 0	3; 0	4; 0	5; 0	5; 0	6; 0	7; 0	7; 0	8; 0	9; 0
4	1; 3328	2; 0	3; 0	4; 0	5; 0	6; 0	7; 0	–	–	–	–	–	–
5	1; 76800	3; 0	3; 0	–	–	–	–	–	–	–	–	–	–

По результатам, представленным в табл. 1, можно сделать предположение, что с ростом k количество подстановок на основе матрицы $C^{(1)}$ стабилизируется. Из табл. 2

можно предположить, что для значений $1 < r \leqslant r_{\max}(k,n,m)$ подстановок указанного вида нет.

С л у ч а й 2. Общие параметры $m = 1$,

$$C^{(2)} = \begin{pmatrix} \beta_1^{(1)} R_{n-1}(r) & 0 & \beta_3^{(1)} & \dots & \beta_{n-1}^{(1)} & \beta_n^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} R_{n-1}(r) & 0 & \dots & \beta_{n-1}^{(2)} & \beta_n^{(2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta_1^{(n-1)} & \beta_2^{(n-1)} & \beta_3^{(n-1)} & \dots & \beta_{n-1}^{(n-1)} R_{n-1}(r) & 0 \\ 0 & \beta_2^{(n)} & \beta_3^{(n)} & \dots & \beta_{n-1}^{(n)} & \beta_n^{(n)} R_{n-1}(r) \end{pmatrix},$$

где нули расположены на второй главной диагонали.

Для $r = 1$ нашлись биекции только для случаев $k = 2$, $n = 3, 4, 5$.

Для $r = r_{\max}(k,n,m)$ биекции были найдены только при $k = 2$, $n = 3, 4, 5$, при этом $r_{\max}(k,n,m) = 1$.

При $r > 1$ биекций на основе матрицы $C^{(2)}$ не найдено.

С л у ч а й 3. Общие параметры $m = 1$, $n = 4$,

$$C^{(3)} = \begin{pmatrix} \beta_1^{(1)} R_3(r) & \beta_2^{(1)} & \beta_3^{(1)} & 0 \\ \beta_1^{(2)} & \beta_2^{(2)} R_3(r) & 0 & \beta_4^{(2)} \\ \beta_1^{(3)} & 0 & \beta_3^{(3)} R_3(r) & \beta_4^{(3)} \\ 0 & \beta_2^{(4)} & \beta_3^{(4)} & \beta_4^{(4)} R_3(r) \end{pmatrix}.$$

Для $r = 1$, $k = 1, \dots, 8$ нашлись биекции только для случая $k = 2$.

Для $r = r_{\max}(k,n,m)$, $k = 1, \dots, 8$ результат совпадает со случаем $r = 1$.

Отсюда сделаем вывод, что возможно построение подстановок с однотипными координатными пороговыми функциями из теоремы 2 и предположительно только для размера отступа $r = 1$.

Приведём утверждение, использующее блочную структуру и позволяющее итеративно увеличивать размер подстановки, основанной на пороговых функциях.

Теорема 5. Пусть заданы две подстановки π_1, π_2, основанные на пороговых функциях, такие, что

$$\pi_1 : \Omega_k^{n_1} \to \Omega_k^{n_1}, \quad \pi_2 : \Omega_k^{n_2} \to \Omega_k^{n_2}, \quad n_1, n_2 \geqslant 2;$$

матрица $C^{(v)} = \left(c_{i,j}^{(v)}\right)_{n_v \times n_v}$ — матрица коэффициентов линейных форм и $P^{(v)} = \left(p_{i,j}^{(v)}\right)_{n_v \times (k-1)}$ — матрица порогов координатных функций подстановки π_v, $v = 1, 2$; $\Theta^{(1)}, \Theta^{(2)}$ — нулевые матрицы размеров $n_1 \times n_2$ и $n_2 \times n_1$ соответственно. Тогда матрицы

$$\tilde{C} = \begin{pmatrix} C^{(1)} & \Theta^{(1)} \\ \Theta^{(2)} & C^{(2)} \end{pmatrix}, \quad \tilde{P} = \begin{pmatrix} P^{(1)} \\ P^{(2)} \end{pmatrix}$$

задают подстановку $\tilde{\pi} : \Omega_k^{n_1+n_2} \to \Omega_k^{n_1+n_2}$.

Доказательство. Достаточно заметить, что первые n_1 координатных функций фиктивно зависят от последних n_2 переменных и реализуют подстановку π_1 на первых n_1 переменных. Последние n_2 координатных функций реализуют подстановку π_2 на последних n_2 переменных. Поэтому $\tilde{\pi}$ представляется следующим образом:

$$\tilde{\pi}(x_1, x_2, \dots, x_{n_1+n_2}) = (\pi_1(x_1, x_2, \dots, x_{n_1}), \pi_2(x_{n_1+1}, x_{n_1+2}, \dots, x_{n_1+n_2})).$$

Данное представление задаёт подстановку. ■

ЛИТЕРАТУРА

1. *Никонов В. Г., Саранцев А. В.* Методы компактной реализации биективных отображений, заданных регулярными системами однотипных булевых функций // Вестник Российского университета дружбы народов. Сер. Прикладная и компьютерная математика. 2003. Т. 2. № 1. С. 94–105.
2. *Никонов В. Г., Саранцев А. В.* Построение и классификация регулярных систем однотипных функций // Материалы XXXI Междунар. конф. «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». М., 2004. Т. 5. С. 173–174.
3. *Никонов В. Г., Сидоров Е. С.* О способе построения взаимно однозначных отображений при помощи квазиадамаровых матриц // Вестник Московского государственного университета леса — Лесной вестник. 2009. № 2(65). С. 155–157.
4. *Никонов В. Г., Сошин Д. А.* Геометрический метод построения сбалансированных k-значных пороговых функций и синтез подстановок на их основе // Образовательные ресурсы и технологии. 2014. № 2(5). С. 76–80.
5. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
6. *Дертоузос М.* Пороговая логика. М.: Мир, 1967.
7. *Ефимов Н. В., Розендорн Э. Р.* Линейная алгебра и многомерная геометрия. М.: Наука, 1970.
8. *Глухов М. М., Шишков А. Б.* Математическая логика. Дискретные функции. Теория алгоритмов. М.: Лань, 2012.

REFERENCES

1. *Nikonov V. G. and Sarantsev A. V.* Metody kompaktnoy realizatsii biektivnykh otobrazheniy, zadannykh regulyarnymi sistemami odnotipnykh bulevykh funktsiy [Methods of compact realization of bijective mappings proposed by regular systems of one-type Boolean functions]. Vestnik RUDN. Ser. Prikladnaya i Komp'yuternaya Matematika, 2003, vol. 2, no. 1, pp. 94–105. (in Russian)
2. *Nikonov V. G. and Sarantsev A. V.* Postroenie i klassifikatsiya regulyarnykh sistem odnotipnykh funktsiy [The construction and classification of the regular systems of one-type functions]. Proc. XXXI Int. conf. "Informatsionnye tekhnologii v nauke, obrazovanii, telekommunikatsii i biznese". Moscow, 2004, vol. 5, pp. 173–174. (in Russian)
3. *Nikonov V. G. and Sidorov E. S.* O sposobe postroeniya vzaimno odnoznachnykh otobrazheniy pri pomoshchi kvaziadamarovykh matrits [About the possibility of one-to-one mappings representation by the quasi-hadamard matrixes]. Vestnik Moskovskogo Gosudarstvennogo Universiteta Lesa — Lesnoy Vestnik, 2009, no. 2(65), pp. 155–157. (in Russian)
4. *Nikonov V. G. and Soshin D. A.* Geometricheskiy metod postroeniya sbalansirovannykh k-znachnykh porogovykh funktsiy i sintez podstanovok na ikh osnove [The geometric method for constructing a balanced k-valued threshold functions and construction of substitutions based on them]. Obrazovatel'nye Resursy i Tekhnologii, 2014, no. 2(5), pp. 76–80. (in Russian)
5. *Alferov A. P., Zubov A. Yu., Kuz'min A. S., and Cheremushkin A. V.* Osnovy kriptografii [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2001. (in Russian)
6. *Dertouzos M.* Porogovaya logika [Threshold Logic]. Moscow, Mir Publ., 1967. (in Russian)
7. *Efimov N. V. and Rozendorn E. R.* Lineynaya algebra i mnogomernaya geometriya [Linear Algebra and Multidimensional Geometry]. Moscow, Nauka Publ., 1970. (in Russian)
8. *Glukhov M. M. and Shishkov A. B.* Matematicheskaya logika. Diskretnye funktsii. Teoriya algoritmov [Mathematical Logic. Discrete Functions. Algorithms Theory]. Moscow, Lan' Publ., 2012.