Построение параметрического семейства латинских квадратов в векторной базе данных*

В.А. Носов

В работе обобщается конструкция параметрических классов латинских квадратов над множеством булевских векторов длины n, предложенная в работе [1], на случай векторов над простым полем $\mathbb{F}_p$. Даются критерии реализуемости данной конструкции и некоторые классификационные результаты.

1°. Латинские квадраты широко используются в теории кодирования, планирования эксперимента, связи в секретных системах ([4], [5]). При конструктивном задании латинского квадрата широко используется аналитический способ задания его с помощью функций, определяющих по номеру строки и номеру столбца значение соответствующего элемента квадрата. При этом не требуется запоминание (хранение) латинского квадрата целиком, а хранятся только соответствующие функции.

Особенностью используемых на практике алгоритмов является их фиксированность, то есть отсутствие в них изменяемых параметров, которые бы позволяли строить широкие классы латинских квадратов. Для случая множества n-мерных строк над полем $\mathbb{F}_2$ алгоритмы построения латинских квадратов, содержащие параметры и допускающие возможность их изменения в широком диапазоне, были предложены в работе [1]. Там же было установлено, что реализуемость данной конструкции определяется некоторым свойством используемых

*Работа поддержана грантом РФФИ № 01–01–00688.

функций, названным их правильностью. В данной работе рассматривается случай множества n-мерных строк над простым полем $\mathbb{F}_p$ и для данного множества предлагается соответствующая конструкция.

2°. Пусть $\mathbb{F}_p$ — поле вычетов по модулю простого числа p, $\mathbb{F}_p^n$ — множество n-мерных строк над полем $\mathbb{F}_p$. Всякий латинский квадрат над множеством $\mathbb{F}_p^n$ может быть задан системой n функций p-значной логики от $2n$ переменных:

$$\begin{aligned} &f_1(x_1,\dots,x_n,y_1,\dots,y_n)\\ &f_2(x_1,\dots,x_n,y_1,\dots,y_n)\\ &\vdots\\ &f_n(x_1,\dots,x_n,y_1,\dots,y_n), \end{aligned} \tag{1}$$

где набор $(x_1,\dots,x_n)$ задает номер строки, $(y_1,\dots,y_n)$ — номер столбца, соответствующие значения функций $(f_1,\dots,f_n)$ определяют элемент квадрата.

Используя результаты о регулярности семейства функций p-значной логики ([2]) можно получить критерии того, когда семейство вида (1) задает латинский квадрат. В частности, справедлива

Теорема 1. *Семейство функций p-значной логики $f=(f_1,\dots,f_n)$ от $2n$ переменных $x_1,\dots,x_n,y_1,\dots,y_n$ определяет латинский квадрат тогда и только тогда, когда во всех произведениях $f_{i_1}^{\alpha_1}\dots f_{i_k}^{\alpha_k}$, кроме $f_1^{p-1}\dots f_k^{p-1}$, где $1\leqslant i_1<\dots<i_k\leqslant n$, $1\leqslant\alpha_i\leqslant p-1$, $i=1,\dots,k$, $1\leqslant k\leqslant n$, коэффициенты при членах $x_1^{p-1}\dots x_n^{p-1}$ и $y_1^{p-1}\dots y_n^{p-1}$ в приведенных многочленах равны 0, а в произведении $f_1^{p-1}\dots f_n^{p-1}$ соответствующие коэффициенты равны 1.*

Данный критерий хотя и не дает эффективного способа построения нужных семейств функций, но позволяет получать достаточные условия путем выделения классов функций. Однако, в полученных классах неудобством является сложность включения параметра в заданную систему функций.

3°. Предложим следующую конструкцию, которая позволяет более эффективно решать поставленные вопросы.

Пусть задано семейство функций p-значной логики $g = (g_1, \ldots, g_n)$ от переменных $z_1, \ldots, z_n$. Пусть $\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)$ — система функций p-значной логики от 2-х переменных. Определим семейство функций p-значной логики $f_1, \ldots, f_n$ от переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$ соотношениями:

$$\begin{aligned} f_1 &= H_1(x_1, y_1, g_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \\ f_2 &= H_2(x_2, y_2, g_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \\ &\ldots \\ f_n &= H_n(x_n, y_n, g_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))), \end{aligned} \tag{2}$$

где H_i, $i \in \overline{1,n}$ — функции p-значной логики от 3-х переменных.

Напомним (см. [1]), что семейство функций $g = (g_1, \ldots, g_n)$ от переменных $z_1, \ldots, z_n$ называется правильным, если для любых различных наборов $z' = (z'_1, \ldots, z'_n)$ и $z'' = (z''_1, \ldots, z''_n)$ существует $\alpha \in \overline{1,n}$, такое, что выполнено

$$z'_\alpha \neq z''_\alpha \quad \text{и} \quad g_\alpha(z') = g_\alpha(z''). \tag{3}$$

Пусть функции H_i, $i \in \overline{1,n}$ удовлетворяют условиям:

В уравнении

$$H(x, y, z) = t$$

над F_p при любых фиксированных трех величинах однозначно определена четвертая. Данное свойство для краткости будем называть латинским свойством.

Справедлива

Теорема 2. *Для латинских функций трех переменных H_i, $i \in \overline{1,n}$ семейство функций $f = (f_1, \ldots, f_n)$ от $2n$ переменных вида* (2) *определяет латинский квадрат при любых функциях $\pi_1, \ldots, \pi_n$ в том и только том случае, когда семейство функций $g = (g_1, \ldots, g_n)$ является правильным.*

Доказательство. Пусть существуют функции двух переменных $\pi_1, \ldots, \pi_n$, такие, что семейство $f = (f_1, \ldots, f_n)$, определенное (2), не определяет латинский квадрат. Тогда имеем для некоторых $(x_1, \ldots, x_n)$, $(y'_1, \ldots, y'_n)$, $(y''_1, \ldots, y''_n)$, причем $(y'_1, \ldots, y'_n) \neq (y''_1, \ldots, y''_n)$, соотношение

$$\begin{gathered} f_1(x_1,\dots,x_n,y'_1,\dots,y'_n) = f_1(x_1,\dots,x_n,y''_1,\dots,y''_n) \\ \dots \\ f_n(x_1,\dots,x_n,y'_1,\dots,y'_n) = f_n(x_1,\dots,x_n,y''_1,\dots,y''_n) \end{gathered} \tag{4}$$

либо соотношение

$$\begin{gathered} f_1(x'_1,\dots,x'_n,y_1,\dots,y_n) = f_1(x''_1,\dots,x''_n,y_1,\dots,y_n) \\ \dots \\ f_n(x'_1,\dots,x'_n,y_1,\dots,y_n) = f_n(x''_1,\dots,x''_n,y_1,\dots,y_n) \end{gathered} \tag{5}$$

для некоторых $(x'_1,\dots,x'_n)$, $(x''_1,\dots,x''_n)$, $(y_1,\dots,y_n)$, причем $(x'_1,\dots,x'_n) \neq (x''_1,\dots,x''_n)$.

Пусть выполнено (5).

Тогда, используя (2), получаем, что выполнены соотношения

$$\begin{gathered} H_1(x'_1,y_1,g_1(\pi_1(x'_1,y_1),\dots,\pi_n(x'_n,y_n))) = \\ = H_1(x''_1,y_1,g_1(\pi_1(x''_1,y_1),\dots,\pi_n(x''_n,y_n))) \\ \dots \\ H_n(x'_1,y_1,g_1(\pi_1(x'_1,y_1),\dots,\pi_n(x'_n,y_n))) = \\ = H_n(x''_1,y_1,g_1(\pi_1(x''_1,y_1),\dots,\pi_n(x''_n,y_n))). \end{gathered} \tag{6}$$

Введем обозначения

$$\begin{array}{llll} z' = (z'_1,\dots,z'_n), & \text{где} \quad z'_i & = \pi_i(x'_i,y_i), & i \in \overline{1,n} \\ z'' = (z''_1,\dots,z''_n), & \text{где} \quad z''_i & = \pi_i(x''_i,y_i), & i \in \overline{1,n} \end{array}$$

и рассмотрим пару наборов

$$g(z') = (g_1(z'),\dots,g_n(z')) \quad \text{и} \quad g(z'') = (g_1(z''),\dots,g_n(z'')).$$

Если для всех $\alpha \in \overline{1,n}$ выполнено $g_\alpha(z') \neq g_\alpha(z'')$, то условие правильности семейства функций $g = (g_1,\dots,g_n)$ не выполнено на паре наборов z' и z''.

Если существует $\alpha \in \overline{1,n}$ такое, что выполнено $g_\alpha(z') = g_\alpha(z'')$, то из (6) получаем

$$H_\alpha(x'_\alpha,y_\alpha,g_\alpha(z')) = H_\alpha(x''_\alpha,y_\alpha,g_\alpha(z'')),$$

причем две координаты наборов аргументов совпадают, и тогда по свойству функций H_i, $i \in \overline{1,n}$ быть латинскими имеем $x'_\alpha = x''_\alpha$. Следовательно, выполнено $\pi_\alpha(x'_\alpha, y_\alpha) = \pi_\alpha(x''_\alpha, y_\alpha)$ и поэтому $z'_\alpha = z''_\alpha$. Значит, в этом случае также не выполняется условие правильности семейства $g = (g_1, \ldots, g_n)$ на паре наборов z' и z''.

Случай (4) разбирается аналогично случаю (5). Таким образом, если система функций (2) не определяет латинский квадрат при некоторых функциях $(\pi_1, \ldots, \pi_n)$, то семейство функций $g = (g_1, \ldots, g_n)$ не является правильным.

Пусть теперь семейство функций $g = (g_1, \ldots, g_n)$ не является правильным. Это значит, что существует пара различных наборов $z' = (z'_1, \ldots, z'_n)$ и $z'' = (z''_1, \ldots, z''_n)$, такая, что при всех $\alpha \in \overline{1,n}$, для которых $z'_\alpha \neq z''_\alpha$ выполнено $g_\alpha(z') \neq g_\alpha(z'')$.

Выберем произвольный набор элементов из $\mathbb{F}_p$ $(a_1, \ldots, a_n)$ и рассмотрим системы уравнений над $\mathbb{F}_p$

$$\begin{aligned} H_1(x_1, y_1, g_1(z')) &= a_1 \\ &\ldots \\ H_n(x_n, y_n, g_n(z')) &= a_n \end{aligned} \tag{7}$$

и

$$\begin{aligned} H_1(x_1, y_1, g_1(z'')) &= a_1 \\ &\ldots \\ H_n(x_n, y_n, g_n(z'')) &= a_n. \end{aligned} \tag{8}$$

Фиксируем произвольные $y_1, \ldots, y_n$. Согласно свойства функций H_i, $i \in \overline{1,n}$ быть латинскими, существуют решения этих систем $x'_1, \ldots, x'_n$ и $x''_1, \ldots, x''_n$ соответственно, причем $x'_\alpha \neq x''_\alpha$, если $g_\alpha(x') \neq g_\alpha(z'')$ в силу тех же условий на функции H_i, $i \in \overline{1,n}$.

Выберем теперь функции $\pi_1, \ldots, \pi_n$ так, чтобы

$$\pi_i(x'_i, y_i) = z'_i \quad \text{и} \quad \pi_i(x''_i, y_i) = z''_i.$$

Это нельзя сделать лишь в случае, когда $x'_i = x''_i$, но $z'_i \neq z''_i$. Однако, если $x'_i = x''_i$, то $g_i(z') = g_i(z'')$ по свойству H_i и имеем $z'_i = z''_i$. Следовательно, элементы квадрата в строках $(x'_1, \ldots, x'_n)$ и $(x''_1, \ldots, x''_n)$ и в столбце $(y_1, \ldots, y_n)$ совпадают в силу (7) и (8), поэтому квадрат, определенный функциями (2), не является латинским.

4°. Рассмотрим вопрос о выполнении латинского свойства на функции H_i, $i \in \overline{i,n}$. Ясно, что им обладают линейные функции, зависящие от всех трех переменных над $\mathbb{F}_p$. Нетрудно доказать, что таковыми будут, в частности, все функции вида $\varphi_1(x) + \varphi_2(y) + \varphi_3(z)$, где φ_i — перестановочные многочлены над $\mathbb{F}_p$. Имеются классы перестановочных многочленов и их классификация для малых степеней и малых p (см. [3]).

5°. Рассмотрим теперь вопрос о выполнении условий правильности для семейств функций p-значной логики. Отметим сначала, что условие правильности семейства функций может быть сведено к условию регулярности в следующем смысле.

Справедлива

Теорема 3. *Функции p-значной логики $g = (g_1, \ldots, g_n)$ от переменных $x_1, \ldots, x_n$ образуют правильное семейство тогда и только тогда, когда для любых наборов $a = (a_1, \ldots, a_n)$ из $\mathbb{F}_p^n$ семейство $g(a) = (x_1 + a_1 g_1, \ldots, x_n + a_n g_n)$ является регулярным.*

Доказательство. Пусть $g = (g_1, \ldots, g_n)$ — правильное семейство и набор $a = (a_1, \ldots, a_n)$ из $\mathbb{F}_p^n$ фиксирован. Тогда, по определению, для любой пары различных наборов $z' = (z'_1, \ldots, z'_n)$ и $z'' = (z''_1, \ldots, z''_n)$ существует $\alpha \in \overline{1,n}$, такое, что выполнено $z'_\alpha \neq z''_\alpha$ и $g_\alpha(z') = g_\alpha(z'')$. Следовательно,

$$g_\alpha(a, z') = z'_\alpha + a_\alpha g_\alpha(z') \neq z''_\alpha + a_\alpha g_\alpha(z'') = g_\alpha(a, z''),$$

что означает регулярность семейства функций $g(a)$. Пусть для любого набора $a \in \mathbb{F}_p^n$ семейство $g(a)$ регулярно, но семейство g не является правильным. Это означает, что существует пара различных наборов z' и z'', такая, что для всех $\alpha \in \overline{1,n}$, таких, что $z'_\alpha \neq z''_\alpha$ имеем $g_\alpha(z') \neq g_\alpha(z'')$. Выберем набор $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$ следующим образом:

положим

$$\begin{aligned} &a_\alpha = 0, && \text{если } \ z'_\alpha = z''_\alpha \\ &a_\alpha = \frac{z''_\alpha - z'_\alpha}{g_\alpha(z') - g_\alpha(z'')}, && \text{если } \ z'_\alpha \neq z''_\alpha. \end{aligned} \tag{9}$$

Определение набора a корректно в силу предположения о наборах z' и z''.

Для выбранных $(a_1, \dots, a_n) \in \mathbb{F}_p^n$ имеем

$$z'_\alpha + a_\alpha g_\alpha(z') = z''_\alpha + a_\alpha g_\alpha(z'') \quad \text{для всех} \quad \alpha \in \overline{1,n}.$$

Следовательно, семейство $g(a)$ не является регулярным, что противоречит условию.

Таким образом, для проверки правильности семейства функций p-значной логики могут быть использованы критерии регулярности семейства. Согласно [2], семейство функций g p-значной логики регулярно тогда и только тогда, когда для любых ненулевых наборов $(t_1, \dots, t_n) \in \mathbb{F}_p^n$ функция $t_1 g_1 + \dots + t_n g_n$ имеет равномерный обобщенный вес, то есть вес $(p^{n-1}, \dots, p^{n-1})$. Отсюда получаем

Следствие 1. *Семейство функций p-значной логики $g = (g_1, \dots, g_n)$ правильно тогда и только тогда, когда для любых двух наборов $a = (a_1, \dots, a_n) \in \mathbb{F}_p^n$ и $t = (t_1, \dots, t_n) \in \mathbb{F}_p^n$, причем $(t_1, \dots, t_n) \neq (0, \dots, 0)$ функция $t_1 x_1 + \dots + t_n x_n + t_1 a_1 g_1 + \dots + t_n a_n g_n$ имеет равномерный обобщенный вес.*

6°. Рассмотрим теперь вопрос о конструктивном построении классов правильных семейств функций, поскольку проверка условий правильности конкретного семейства может быть трудоемкой. Ясно, что правильными семействами будут семейства, которые перенумерацией индексов приводятся к виду

$$\begin{aligned} g_1 &= c \\ g_2(x_1) & \\ &\dots \\ g_n(x_1, \dots, x_{n-1}). & \end{aligned} \tag{10}$$

Правильными будут такие семейства $g = (g_1, \dots, g_n)$, у которых для всех $i \in \overline{1,n}$ переменная x_i не является существенной для g_i и при этом $g_i \cdot g_j \equiv 0$ при $i \neq j$. Укажем один рекуррентный способ построения правильных семейств функций. Пусть имеем семейство функций

$g = (g_{10}, \dots, g_{n0})$ от переменных $x_{10}, \dots, x_{n0}$. Пусть $s_1, \dots, s_n$ — набор натуральных чисел. Определим семейство функций $f = (f_{ij})$, $i \in \overline{1,n}$, $j \in \overline{0,s_i}$ от переменных (x_{ij}), $i \in \overline{1,n}$, $j \in \overline{0,s_i}$ соотношениями для всех $i \in \overline{1,n}$:

$$\begin{aligned} f_{i1} &= F_{i1}(g_{i0}) \\ f_{i2} &= F_{i2}(g_{i0}, x_{i1}) \\ &\dots \\ f_{is_i} &= F_{is_i}(g_{i0}, x_{i1}, \dots, x_{is_i-1}) \\ f_{i0} &= F_{i0}(g_{i0}, x_{i1}, \dots, x_{is_i}), \end{aligned} \tag{11}$$

где F_{ij} — некоторые функции от указанных переменных. Легко убедиться, что справедлива

Теорема 4. *Если семейство функций $g = (g_{10}, \dots, g_{n0})$ правильно, то семейство функций $f = (f_{ij})$, $i \in \overline{1,n}$, $j \in [0, s_i]$ правильно при любых функциях $F_{i1}, \dots, F_{is_i}$, $i \in \overline{1,n}$.*

Укажем теперь в явном виде некоторые классы правильных семейств функций p-значной логики.

Пусть $\varphi(x)$ — произвольный перестановочный многочлен над $\mathbb{F}_p$. Рассмотрим следующее семейство функций $f = (f_1, \dots, f_n)$, где

$$\begin{aligned} f_1 &= \varphi(x_2 + 1) \dots \varphi(x_2 + p - 1) \cdot \varphi(x_3) \\ f_2 &= \varphi(x_3 + 1) \dots \varphi(x_3 + p - 1) \cdot \varphi(x_4) \\ &\dots \\ f_n &= \varphi(x_1 + 1) \dots \varphi(x_1 + p - 1) \cdot \varphi(x_2). \end{aligned} \tag{12}$$

Справедлива

Теорема 5. *Семейство функций f правильно тогда и только тогда, когда n нечетно.*

Доказательство. Пусть n четно. Поскольку $\phi(x)$ — перестановочный многочлен, то существуют z'_2 и z'_3, такие, что $f_1(z'_2, z'_3) \neq 0$. Далее, существуют z'_4, z'_5, такие, что $f_3(z'_4, z'_5) \neq 0$, …, z'_n, z'_1, такие, что $f_{n-1}(z'_n, z'_1) \neq 0$. Пусть $z' = (z'_1, \dots, z'_n)$ — полученный набор. Ему

соответствует $f_1(z'), \ldots, f_n(z')$, у которого элементы на нечетных местах отличны от нуля. Согласно (12), если $f_\alpha(z) \neq 0$, то $f_{\alpha-1}(z) = f_{\alpha+1}(z) = 0$ (индексы по модулю n) в силу перестановочности φ. Аналогично предыдущему, существуют z''_3, z''_4, такие, что $f_2(z''_3, z''_4) \neq 0$, $\ldots$, z''_1, z''_2, такие, что $f_n(z''_1, z''_2) \neq 0$. Пусть $z'' = (z''_1, \ldots, z''_n)$ — соответствующий набор. Ему соответствует $f_1(z''), \ldots, f_n(z'')$, у которого на четных местах стоят элементы, отличные от нуля. Теперь замечаем, что для пары z', z'' свойство правильности семейства $f = (f_1, \ldots, f_n)$ не выполняется.

Пусть теперь n нечетно. Предположим, что семейство f не является правильным. Это значит, что существует пара различных наборов z' и z'', такая, что для всех α, таких, что $z'_\alpha \neq z''_\alpha$ имеем $f_\alpha(z') \neq f_\alpha(z'')$. В силу нечетности n и в силу того, что в наборе $(f_1(z), \ldots, f_n(z))$ для любого z каждый ненулевой элемент окаймлен нулями, получаем, что для наборов z' и z'' и соответствующих $(f_1(z'), \ldots, f_n(z'))$ и $(f_1(z''), \ldots, f_n(z''))$ найдется $\alpha \in \overline{1,n}$, для которого $f_\alpha(z') = f_\alpha(z'') = 0$. Следовательно, должно быть $z'_\alpha = z''_\alpha$. Если $\varphi(z'_\alpha) = \varphi(z''_\alpha) = 0$, то из (12) получаем $f_{\alpha-2}(z') = f_{\alpha-2}(z'') = 0$ и тогда имеем $z'_{\alpha-2} = z''_{\alpha-2}$. Если $\varphi(z'_\alpha) = \varphi(z''_\alpha) \neq 0$, то в силу перестановочности φ имеем $\varphi(z'_\alpha + 1) \ldots \varphi(z'_\alpha + p - 1) = 0$ и тогда $f_{\alpha-1}(z') = f_{\alpha-1}(z'') = 0$ и должно быть $z'_{\alpha-1} = z''_{\alpha-1}$. Используя (12), снова получаем, что $f_{\alpha-2}(z') = f_{\alpha-2}(z'')$ и тогда $z'_{\alpha-2} = z''_{\alpha-2}$. Таким образом, во всех случаях из равенства $z'_\alpha = z''_\alpha$ следует $z'_{\alpha-2} = z''_{\alpha-2}$. В силу нечетности n получаем $z' = z''$, что противоречит условию на их выбор.

7°. Для семейства функций $f = (f_1, \ldots, f_n)$ от переменных $x_1, \ldots, x_n$ определим граф существенной зависимости $G_f = (V, E)$, где $V = \{1, 2, \ldots, n\}$. Пара $(i, j) \in E \Leftrightarrow$ если f_j зависит от x_i существенно. Рассмотрим вопрос, как влияют циклы графа G_f семейства функций f на правильность этого семейства.

Теорема 6. *Пусть $f = (f_1, \ldots, f_n)$ — семейство функций p-значной логики, G_f — его граф существенной зависимости переменных.*

Пусть для любого простого элементарного цикла C графа G_f выполнено

$$\prod_{i\in C} f_i \equiv 0. \tag{13}$$

Тогда семейство f является правильным.

Доказательство. Предположим, что семейство f не является правильным, но выполнено условие (13). Пусть $a = (a_1, \dots, a_n) \in \mathbb{F}_p^n$ — набор элементов из $\mathbb{F}_p$, такой, что семейство $f(a) = (x_1 + a_1 f_1, \dots, x_n + a_n f_n)$ не является регулярным. Согласно критерия регулярности из [3] должен существовать набор индексов $i_1, \dots, t_k$ и набор констант $\alpha_1, \dots, \alpha_k$, $1 \leqslant \alpha_i \leqslant p-1$, $1 \leqslant i_1 < \dots < i_k \leqslant n$, $k \in \overline{1,n}$, такой, что произведение $(x_{i_1} + a_{i_1} \cdot f_{i_1})^{\alpha_1} \dots (x_{i_k} + a_{i_k} \cdot f_{i_k})^{\alpha_k}$ в приведенном многочлене содержит член $x_1^{p-1} \dots x_n^{p-1}$, либо в произведении $(x_1 + a_1 f_1)^{p-1} \dots (x_n + a_n f_n)^{p-1}$ в приведенном многочлене коэффициент при $x_1^{p-1} \dots x_n^{p-1}$ отличен от 1. В первом случае существуют $\gamma_1 > 0, \dots, \gamma_k > 0$, $\beta_1, \dots, \beta_k$, где $\gamma_i + \beta_i = \alpha_i$, что произведение $x_{i_1}^{\beta_1} f_{i_1}^{\gamma_1} \dots x_{i_k}^{\beta_k} f_{i_k}^{\gamma_k}$ дает член $x_1^{p-1} \dots x_n^{p-1}$. Это означает, что в графе G_f имеются дуги, выходящие из каждой вершины $i_1, \dots, i_k$ и входящие в каждую вершину $i_1, \dots, i_k$. Значит, вершинный подграф G_f на вершинах $i_1, \dots, i_k$ содержит цикл C и согласно (13) получаем противоречие. Второй случай разбирается аналогично.

Представляет интерес, когда условия (13) являются необходимыми для правильности семейства функций f.

Будем говорить, что функция $f(x_1, \dots, x_n)$ p-значной логики обладает свойством Q, если для всякого существенного переменного x_k функции f выполнено: если $f(\alpha_1, \dots, \alpha_k, \dots, \alpha_n) \neq 0$, то существует $\alpha'_k \in \mathbb{F}_p$, такое, что $f(\alpha_1, \dots, \alpha'_k, \dots, \alpha_n) = 0$. (То есть на каждом ребре p-ичного куба есть нуль функции.)

Теорема 7. *Пусть каждая функция семейства $f = (f_1, \dots, f_n)$ функций p-значной логики обладает свойством Q. Тогда для правильности семейства f необходимо, чтобы выполнялось условие* (13) *для каждого простого элементарного цикла графа G_f.*

Доказательство. Пусть, напротив, существует цикл C графа G_f, для которого $\prod_{i\in C} f_i \not\equiv 0$. Это зачит, что существует набор значений

переменных $\alpha = (\alpha_1, \ldots, \alpha_n)$, такой, что $f_{i_1}(\alpha) \neq 0, \ldots, f_{i_k}(\alpha) \neq 0$, где $C = \{i_1, \ldots, i_k\}$. Ясно, что функция f_{i_1} зависит от x_{i_2} существенно и не зависит от $x_{i_1}, x_{i_3}, \ldots, x_{i_k}$. По свойству Q для функции f_{i_1} существует α'_{i_2}, такое, что $f_{i_1}(\alpha_1, \ldots, \alpha'_{i_2}, \ldots, \alpha_n) = 0$. Аналогично для функций $f_{i_2}, \ldots, f_{i_k}$. Для набора $\alpha' = (\alpha_1 \ldots \alpha'_{i_1} \ldots \alpha'_{i_k} \ldots \alpha_n)$ имеем

$$f_{i_1}(\alpha') = \cdots = f_{i_k}(\alpha') = 0.$$

Следовательно, семейство f не является правильным.

Укажем теперь класс функций p-значной логики, для которого введенное выше свойство Q выполнено. Пусть $\varphi_1(x), \ldots, \varphi_n(x)$ — перестановочные многочлены над $\mathbb{F}_p$. Нетрудно видеть, что функция $f(x_1, \ldots, x_n)$ вида

$$f(x_1, \ldots, x_n) = (a_{11}\varphi_1(x_1) + \cdots + a_{1n}\varphi_n(x_n))(a_{21}\varphi_1(x_1) + \ldots \\ \cdots + a_{2n}\varphi_n(x_n)) \ldots (a_{k1}\varphi_1(x_1) + \cdots + a_{kn}\varphi_n(x_n)),$$

где $a_{ij} \in \mathbb{F}_p$ обладает свойством Q (произведение линейных форм от перестановочных многочленов).

Замечание. Можно показать, что «почти все» правильные семейства функций p-значной логики при $p \to \infty$ приводятся к виду (10). Конструкции, предложенные в теоремах 4, 5, 6, приводят к семействам, вообще говоря, отличным от вида (10).

Список литературы

[1] Носов В.А. Построение классов латинских квадратов в булевой базе данных // Интелл. Системы. Т. 4. Вып. 3–4. 1999. С. 307–320.

[2] Применко В.А., Скворцов В.Ф. Об условиях регулярности конечных автономных автоматов // Дискретная математика. Т. 2. Вып. 1. 1990.

[3] Лидл Р., Нидеррайтер Т. Конечные поля. Т. 2. М.: Мир, 1968.

[4] Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М., 1963. С. 333–369.

[5] Denes J., Keedwell A. Latin aquares and their applications. Budapest, 1974.