О функциональном задании латинских квадратов

В. А. Носов, А. Е. Панкратьев*

В работе исследуются функциональные способы задания латинских квадратов над множествами n-мерных булевых векторов, n-мерных векторов над произвольным простым конечным полем и произвольной конечной абелевой группой. Также приводится конструкция, задающая классы негрупповых латинских квадратов.

Введение

Латинские квадраты широко используются в различных областях математики и кибернетики: теории кодирования, планировании эксперимента, защите информации [1]. В своей фундаментальной теоретической работе [2], посвященной связи в секретных системах, К. Шеннон показал, что шифры, построенные на латинских квадратах, обладают так называемым свойством совершенной секретности. Это свойство обуславливает применение латинских квадратов в алгоритмах и стандартах шифрования.

При практическом применении латинские квадраты могут иметь достаточно большие размеры, что делает затруднительным хранение в памяти всего квадрата целиком (всех элементов). Поэтому необходимо использовать конструктивные методы задания латинских квадратов. Широкое распространение получило аналитическое задание

*Работа второго автора поддержана Советом при Президенте РФ по поддержке ведущих научных школ, грант № НШ–5666.2006.1

латинских квадратов при помощи функции двух переменных, определяющей элемент квадрата по его координатам (номеру строки и столбца). Свойствам таких функций и получаемых латинских квадратов и посвящена настоящая работа, являющаяся продолжением и обобщением работ [4], [5], [6].

Напомним, что латинским квадратом порядка n называется матрица размера $n \times n$, заполненная элементами некоторого множества Ω, $|\Omega| = n$, таким образом, что в каждой ее строке и в каждом столбце все элементы различны. Простейшим примером латинского квадрата порядка n является матрица

$$L = \begin{pmatrix} 0 & 1 & \cdots & n-2 & n-1 \\ 1 & 2 & \cdots & n-1 & 0 \\ \vdots & & \ddots & & \vdots \\ n-2 & n-1 & \cdots & n-4 & n-3 \\ n-1 & 0 & \cdots & n-3 & n-2 \end{pmatrix}.$$

Этот латинский квадрат задается формулой $L(x, y) = x + y$, где x и y суть «номера» строки и столбца квадрата, $x, y \in \Omega = \{0, 1, \ldots, n-1\}$, и под сложением понимается сложение по модулю n (можно сказать, что формула $L(x, y) = x + y$ задает латинский квадрат над абелевой группой $\mathbb{Z}_n$). Произвольный латинский квадрат порядка n над группой $\mathbb{Z}_n$ задается формулой

$$L(x, y) = x + y + f(x, y), \tag{1}$$

где f — некоторая функция $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$. Заметим, что латинские квадраты определяются над любым множеством из n элементов, однако часто специфика групповой структуры позволяет их задавать более наглядно и удобно с вычислительной точки зрения.

В данной работе приводится конструкция, обобщающая формулу (1). Фигурирующая в этой формуле функция $f(x, y)$ рассматривается как вектор-функция или семейство функций. В терминах свойств этого семейства функций формулируются необходимые и достаточные условия того, что матрица, задаваемая формулой (1), является латинским квадратом.

1. Латинские квадраты, задаваемые семействами булевых функций

Рассмотрим квадраты, заданные над множеством $\Omega = E_n$, то есть множеством всех двоичных наборов длины n. Такие квадраты имеют порядок $m \times m$, где $m = |E_n| = 2^n$. «Занумеруем» строки и столбцы квадрата L элементами множества E_n и определим элемент $L(x, y) = (z_1, \ldots, z_n)$, стоящий на пересечении строки с номером $x = (x_1, \ldots, x_n)$ и столбца с номером $y = (y_1, \ldots, y_n)$, формулами

$$z_i = g_i(x_1, \ldots, x_n, y_1, \ldots, y_n), \quad i = 1, \ldots, n, \tag{2}$$

где g_i являются булевыми функциями $2n$ переменных $x_1, \ldots, x_n$, $y_1, \ldots, y_n$.

Известные результаты о регулярности системы булевых функций [7] позволяют сформулировать следующий критерий.

Теорема 1. *[4] Семейство n булевых функций $G = \{g_1, g_2, \ldots, g_n\}$ от $2n$ переменных $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ задает латинский квадрат с помощью формул (2) тогда и только тогда, когда во всех произведениях $g_{i_1} \cdot \cdots \cdot g_{i_k}$, $1 \leqslant i_1 < \cdots < i_k \leqslant n$, $k < n$, в полиноме Жегалкина нет членов, содержащих вхождения $x_1 \ldots x_n$ либо $y_1 \ldots y_n$, а произведение $g_1 \cdot \cdots \cdot g_n$ содержит оба таких члена и не содержит других членов, их содержащих.*

Можно предложить параметрический способ задания семейства латинских квадратов. Пусть дано семейство булевых функций $F = \{f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n)\}$ от n переменных $z_1, \ldots, z_n$. Пусть $\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)$ — семейство булевых функций от двух переменных. Определим систему булевых функций $G = \{g_1, \ldots, g_n\}$ от $2n$ переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$ соотношениями

$$\begin{aligned} g_1 &= x_1 + y_1 + f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ g_2 &= x_2 + y_2 + f_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ &\ldots \\ g_n &= x_n + y_n + f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)). \end{aligned} \tag{3}$$

Будем говорить, что семейство булевых функций $F = \{f_1, f_2, \ldots, f_n\}$ является правильным, если для любых различных наборов переменных $z' = (z'_1, z'_2, \ldots, z'_n)$ и $z'' = (z''_1, z''_2, \ldots, z''_n)$ существует $\alpha \in \overline{1,n}$ такое, что выполнено

$$z'_\alpha \neq z''_\alpha, \quad f_\alpha(z'_1, \ldots, z'_n) = f_\alpha(z''_1, \ldots, z''_n). \tag{4}$$

Теорема 2. *[4] Семейство булевых функций $G = \{g_1, g_2, \ldots, g_n\}$ вида* (3) *определяет с помощью формул* (2) *латинский квадрат для любых функций $\pi_1, \pi_2, \ldots, \pi_n$ в том и только том случае, когда семейство функций $F = \{f_1, f_2, \ldots, f_n\}$ является правильным.*

Замечание. Теорема 2 позволяет при помощи любого правильного семейства функций $F = \{f_1, f_2, \ldots, f_n\}$ получать различные латинские квадраты, варьируя систему функций-параметров $\pi_1, \pi_2, \ldots, \pi_n$.

Введем некоторые определения. Пусть $f(x_1, x_2, \ldots, x_n)$ — булева функция от n переменных и $I \subseteq [1, n]$. Множество переменных $x_I = (x_i)$, $i \in I$, где для определенности возьмем $I = [1, s]$, $1 \leqslant s \leqslant n$, будем называть существенным для функции f, если

$$\sum_{\alpha_1, \ldots, \alpha_s} f(\alpha_1, \ldots, \alpha_s, x_{s+1}, \ldots, x_n) \not\equiv 0 \pmod 2 \tag{5}$$

При $s = 1$ определение существенного множества переменных сводится к известному свойству существенной зависимости функции от соответствующего переменного. При $s = n$ утверждение о существенности множества переменных (x_i), $i \in [1, n]$ равносильно нечетности веса f.

Следующий результат позволяет свести проверку правильности семейства функций к проверке существенной зависимости произведений функций от подмножеств их аргументов.

Теорема 3. *[3] Семейство булевых функций $F = \{f_1, f_2, \ldots, f_n\}$ от переменных $x_1, x_2, \ldots, x_n$ является правильным тогда и только тогда, когда для любого подмножества $I \subseteq \{1, 2, \ldots, n\}$ произведение функций $\prod\limits_{i \in I} f_i$ не зависит существенно от множества переменных $x_I = \{x_i\}$, $i \in I$.*

2. Латинские квадраты, задаваемые семействами функций p-значной логики

Рассмотрим теперь квадраты над $\mathbb{F}_p^n$, то есть множеством n-мерных векторов над простым полем $\mathbb{F}_p$. Зададим квадрат L над множеством $\mathbb{F}_p^n$ при помощи системы n функций p-значной логики от $2n$ переменных:

$$\begin{aligned} &g_1(x_1,\dots,x_n,y_1,\dots,y_n)\\ &g_2(x_1,\dots,x_n,y_1,\dots,y_n)\\ &\vdots\\ &g_n(x_1,\dots,x_n,y_1,\dots,y_n). \end{aligned} \tag{6}$$

Здесь, как и в булевом случае, набор $x = (x_1,\dots,x_n)$ задает номер строки, набор $y = (y_1,\dots,y_n)$ — номер столбца, а значения функций $(g_1,\dots,g_n)$ определяют соответствующий элемент $L(x,y) = (z_1,\dots,z_n)$ квадрата L.

Используя результаты о регулярности семейства функций p-значной логики [8] можно получить критерии того, что семейство (6) задает латинский квадрат.

Теорема 4. *[5] Семейство функций p-значной логики $G = \{g_1, g_2, \dots, g_n\}$ от $2n$ переменных $x_1,\dots,x_n,y_1,\dots,y_n$ определяет латинский квадрат тогда и только тогда, когда во всех произведениях $g_{i_1}^{\alpha_1}\dots g_{i_k}^{\alpha_k}$ кроме $g_1^{p-1}\dots g_k^{p-1}$, 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 $g_1^{p-1}\dots g_n^{p-1}$ соответствующие коэффициенты равны 1.*

Аналогично критерию, сформулированному в Теореме 1 данный критерий не дает эффективного способа построения нужных семейств функций, но позволяет получать достаточные условия путем выделения классов функций.

Приведём конструкцию, обобщающую сформулированные выше результаты о булевых функциях на случай функций p-значной логики.

Пусть задано семейство функций p-значной логики $F = \{f_1, f_2, \ldots, f_n\}$ от n переменных $z_1, z_2, \ldots, z_n$. 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 $G = \{g_1, g_2, \ldots, g_n\}$ от переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$ соотношениями

$$\begin{aligned} g_1 &= H_1(x_1, y_1, f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \\ g_2 &= H_2(x_2, y_2, f_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \\ &\ldots \\ g_n &= H_n(x_n, y_n, f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))), \end{aligned} \tag{7}$$

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

Будем говорить, что функция $H : \mathbb{F}_p^3 \to \mathbb{F}_p$ является латинской, если в уравнении $H(x, y, z) = t$ над $\mathbb{F}_p$ для любых фиксированных трёх величин однозначно определена четвертая.

Заметим также, что определение правильного семейства булевых функций, введенное в пункте 1, можно дословно перенести на случай функций p-значной логики.

Теорема 5. *[5] Для латинских функций трех переменных H_i, $i \in \overline{1, n}$ семейство функций $G = \{g_1, g_2, \ldots, g_n\}$ вида (7) определяет латинский квадрат при любых функциях $\pi_1, \ldots, \pi_n$ в том и только том случае, когда семейство функций $F = \{f_1, f_2, \ldots, f_n\}$ является правильным.*

Ясно, что класс латинских функций включает 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. [9]).

Приведем критерий, позволяющий свести проверку выполнения условия правильности для семейства функций p-значной логики к проверке условия регулярности для ассоциированного семейства.

Теорема 6. *[5] Функции p-значной логики* $F = \{f_1, f_2, \ldots, f_n\}$ *от переменных* $x_1, x_2, \ldots, x_n$ *образуют правильное семейство тогда и только тогда, когда для любого набора* $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$ *семейство функций* $F(a) = \{x_1 + a_1 f_1, x_2 + a_2 f_2, \ldots, x_n + a_n f_n\}$ *является регулярным.*

3. Латинские квадраты над абелевыми группами

Всюду в дальнейшем мы будем работать с латинскими квадратами, заданными над абелевыми группами. При этом будем использовать аддитивную запись группы и через 0 обозначать нейтральный элемент.

Рассмотрим прямое произведение нескольких (n) копий конечной абелевой группы G:

$$H = G^n = \underbrace{G \times G \times \cdots \times G}_{n}. \tag{8}$$

Зададим над группой H латинский квадрат порядка $|H|$. Сначала «занумеруем» строки и столбцы квадрата элементами группы H. Пусть $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ суть элементы группы H. Определим элемент квадрата $L(x, y) = (z_1, z_2, \ldots, z_n)$, стоящий на пересечении строки, соответствующей элементу x, и столбца, соответствующего элементу y, формулами

$$\begin{aligned} z_1 &= x_1 + y_1 + f_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) \\ z_2 &= x_2 + y_2 + f_2(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) \\ &\vdots \\ z_n &= x_n + y_n + f_n(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)). \end{aligned} \tag{9}$$

Здесь $p_1, p_2, \ldots, p_n$ — функции $G \times G \to G$; $f_1, f_2, \ldots, f_n$ — функции $G^n \to G$.

Очевидно, формулы (9) не всегда задают латинский квадрат. Например, набор $f_1 = -y_1, f_2 = -y_2, \ldots, f_n = -y_n$ задает квадрат с

одинаковыми столбцами. Приведем условия на функции $f_1, f_2, \ldots, f_n$, при выполнении которых квадрат $L = L(x, y)$ является латинским для любых функций $p_1, p_2, \ldots, p_n$.

Заметим, что определение правильного семейства функций, введенное выше для булевых функций и функций k-значной логики, дословно переностися и на случай функций над абелевыми группами.

Теорема 7. *[6] Квадрат, элементы которого задаются формулами* (9)*, является латинским при любых $p_1, p_2, \ldots, p_n$ тогда и только тогда, когда семейство функций $f_1, f_2, \ldots, f_n$ является правильным.*

Замечание. Аналогично случаю булевых функций и функций k-значной логики, теорема 7 позволяет при помощи любого правильного семейства функций $f_1, f_2, \ldots, f_n$ получать различные латинские квадраты, варьируя систему функций-параметров $p_1, p_2, \ldots, p_n$. Нетрудно также видеть, что систему параметров можно выбрать $|H|^{n|H|}$ способами.

Теорема 8. *[6] Функции $f_1, f_2, \ldots, f_n$ образуют правильное семейство тогда и только тогда, когда для любого набора функций $\psi_1, \psi_2, \ldots, \psi_n$ вида $G \to G$ семейство функций $\{x_1 + \psi_1(f_1),\ x_2 + \psi_2(f_2), \ldots, x_n + \psi_n(f_n)\}$ является регулярным (определяет биекцию $G^n \to G^n$).*

Замечание. Теорема 8 позволяет свести проверку правильности семейства функций к проверке регулярности семейства ассоциированных отображений, а для проверки регулярности системы существуют многочисленные алгоритмы, основанные на различных способах задания этих функций [8].

Для семейств линейных функций можно привести эффективный критерий правильности в терминах цикловой структуры графа.

Теорема 9. *[6] Пусть $F = \{f_1, f_2, \ldots, f_n\}$ — семейство линейных функций $G^n \to G$, имеющее вид*

$$\begin{aligned} f_1(x_1,\dots,x_n) &= a_{11}x_1 + \cdots + a_{1n}x_n + c_1 \\ f_2(x_1,\dots,x_n) &= a_{21}x_1 + \cdots + a_{2n}x_n + c_2 \\ &\vdots \\ f_n(x_1,\dots,x_n) &= a_{n1}x_1 + \cdots + a_{nn}x_n + c_n \end{aligned} .$$

Здесь свободные члены $c_1, c_2, \dots, c_n$ — элементы группы G, а целочисленные коэффициенты a_{ij} приведены по модулю экспоненты группы G. Определим ориентированный граф $G_F = (V, E)$ (граф существенной зависимости) на множестве вершин $V = \{1, 2, \dots, n\}$, положив $(i, j) \in E \iff a_{ij} \neq 0$. Тогда семейство $F = \{f_1, f_2, \dots, f_n\}$ правильно в том и только в том случае, если граф G_F не содержит циклов.

Теорема 9 допускает значительное обобщение. Можно указать более широкий класс функций, для которого правильность семейств равносильна отсутствию циклов в соответствующих графах.

Для фиксированного элемента $g \in G$ будем говорить, что функция $f(x_1, \dots, x_n)$ вида $G^n \to G$ является *g-функцией*, если для любой переменной x_i, от которой она зависит существенным образом, выполнено условие $f(g, \dots, g, x_i, g, \dots, g) \not\equiv \text{const}$. Заметим, что константы являются g-функциями для любого $g \in G$.

Замечание. Можно показать, что при $|G| \to \infty$, $\frac{|G|}{n} \to \infty$, доля g-функций среди всех функций n переменных стремится к 1.

Обобщим также введенное выше понятие графа G_F, положив $(i, j) \in E$ если и только если f_j существенно зависит от x_i (очевидно, что граф, введенный в Теореме 9, удовлетворяет этому свойству). Назовем его *графом существенной зависимости* семейства функций $F = \{f_1, f_2, \dots, f_n\}$.

Теорема 10. *Семейство g-функций $F = \{f_1, f_2, \dots, f_n\}$ правильно в том и только том случае, если его граф существенной зависимости G_F не содержит циклов.*

Доказательство. Докажем необходимость. Допустим, что граф G_F содержит (ориентированные) циклы и рассмотрим кратчайший цикл

$i_1 i_2 \dots i_k$. Случай $k = 1$ соответствует ориентированной петле в вершине i_1. Но это означает, что функция f_{i_1} существенно зависит от переменной i_1, что противоречит правильности семейства F в силу Замечания 2 из работы [6].

Пусть теперь цикл $i_1 i_2 \dots i_k$ проходит по крайней мере через две вершины. Обозначим множество индексов этих вершин через $I = \{i_1, i_2, \dots, i_k\}$. Тогда для любого $j \in \overline{1,k}$ функция $f_{i_{j+1}}$ существенным образом зависит от x_{i_j} (под $f_{i_{k+1}}$ подразумевается f_{i_1}). Заметим, что для любого индекса $j \in I$ функция f_j существенно зависит в точности от одного переменного x_i, $i \in I$. В самом деле, при $k = 2$ наличие двух различных индексов $i_1, i_2 \in I$ таких, что функция f_j существенно зависит от переменных x_{i_1}, x_{i_2}, невозможно (так как в этом случае один из этих индексов совпадает с j и мы приходим к случаю петли, рассмотренному выше). Если же $k \geqslant 3$, то допустим, что (с точностью до циклической перестановки) существует индекс s, $1 \leqslant s \leqslant k-2$, такой, что f_{i_k} существенно зависит от x_{i_s}. Тогда граф G_F содержит ребро (i_s, i_k) и, следовательно, имеется более короткий цикл $i_1 i_2 \dots i_s i_k$, что противоречит выбору цикла $i_1 i_2 \dots i_k$.

Теперь возьмем $g' = (g, \dots, g)$ и выберем $g'' = (g_1, \dots, g_n)$ следующим образом. При $i \notin I$ положим $g_i = g$. Далее, поскольку f_{i_2} существенно зависит от x_{i_1}, то согласно определению g-функции можно выбрать значение переменной $x_{i_1} = g_{i_1}$ так, что $f_{i_2}(g, \dots, g, g_{i_1}, g, \dots, g) \neq f_{i_2}(g, \dots, g)$. Аналогично можно выбрать остальные g_i, $i \in I$, удовлетворяющие условиям

$$\begin{gathered} f_{i_1}(g, \dots, g, g_{i_k}, g, \dots, g) \neq f_{i_1}(g, \dots, g) \\ f_{i_2}(g, \dots, g, g_{i_1}, g, \dots, g) \neq f_{i_2}(g, \dots, g) \\ \vdots \\ f_{i_k}(g, \dots, g, g_{i_{k-1}}, g, \dots, g) \neq f_{i_k}(g, \dots, g) \end{gathered}$$

Но согласно доказанному ранее каждая из этих функций существенно зависит только от одной из переменных x_i, $i \in I$. Поэтому значения функций в левых частях системы равны значениям тех же функций на наборе $g'' = (g_1, \dots, g_n)$. Это противоречит определению правильности семейства $F = \{f_1, f_2, \dots, f_n\}$, поскольку все

функции семейства принимают различные значения на различных наборах $g' = (g, \ldots, g)$ и $g'' = (g_1, \ldots, g_n)$.

Докажем достаточность. Допустим, что семейство g-функций $F = \{f_1, f_2, \ldots, f_n\}$ не является правильным. Тогда найдутся различные наборы $g' = (g'_1, \ldots, g'_n)$ и $g'' = (g''_1, \ldots, g''_n)$ со свойством, что для любого индекса $\alpha \in \overline{1,n}$ из неравенства $g'_\alpha \neq g''_\alpha$ следует неравенство $f_\alpha(g') \neq f_\alpha(g'')$.

Рассмотрим множество $I = \{i_1, i_2, \ldots, i_k\}$ всех индексов, по которым отличаются наборы g' и g''. Возьмем какой-нибудь индекс $s_1 \in I$. Поскольку $f_{s_1}(g') \neq f_{s_1}(g'')$, функция f_{s_1} существенно зависит, по крайней мере, от одной из переменных $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$. Это означает, что граф G_F содержит, по крайней мере, одно ребро, заканчивающееся в вершине s_1. Пусть это ребро (s_2, s_1), где $s_2 \in I$. Точно так же находим индекс $s_3 \in I$, для которого граф G_F содержит ребро (s_3, s_2). Продолжая этот процесс, получаем последовательность индексов $s_1, s_2, \ldots$, принадлежащих множеству I и таких, что граф G_F содержит ребра (s_{j+1}, s_j), $j = 1, 2, \ldots$. В силу конечности множества I найдется индекс $s_q \in I$, равный некоторому полученному ранее индексу s_p. Это даёт цикл $s_p s_{p+1} \ldots s_{q-1}$ в графе G_F. Теорема доказана.

Теперь приведем класс правильных семейств функций, не удовлетворяющих условию Теоремы 10.

Будем называть функции f и g вида $G^n \to G$ *ортогональными*, если для любого $x \in G^n$ либо $f(x) = 0$ либо $g(x) = 0$.

Лемма. *Пусть семейство $F = \{f_1, f_2, \ldots, f_n\}$ попарно ортогональных функций таково, что для любого i, $1 \leqslant i \leqslant n$, функция f_i не зависит существенно от x_i. Тогда семейство F является правильным.*

Доказательство леммы осуществляется непосредственной проверкой выполнения условия правильности семейства $F = \{f_1, f_2, \ldots, f_n\}$.

Приведем пример семейства $F = \{f_1, f_2, \ldots, f_n\}$ попарно ортогональных функций, удовлетворяющего условию леммы и такого, что граф существенной зависимости G_F является полным.

Возьмем произвольное собственное подмножество $L \subset H$, $\varnothing \neq L \neq H$, и рассмотрим соответствующую характеристическую функцию вместе с ее отрицанием:

$$L(x) = \begin{cases} 1, & x \in L \\ 0, & x \notin L \end{cases} \qquad \overline{L}(x) = \begin{cases} 0, & x \in L \\ 1, & x \notin L \end{cases}$$

Определим семейство $F = \{f_1, f_2, \ldots, f_n\}$ формулами

$$\begin{aligned} f_1 &= \overline{L}(x_2)L(x_3)\cdots L(x_{n-1})L(x_n)g_1 \\ f_2 &= \overline{L}(x_3)L(x_4)\cdots L(x_n)L(x_1)g_2 \\ &\vdots \\ f_n &= \overline{L}(x_1)L(x_2)\cdots L(x_{n-2})L(x_{n-1})g_n \end{aligned}$$

Здесь $g_1, g_2, \ldots, g_n$ — произвольные элементы группы G, а коэффициенты перед ними суть произведения характеристических функций. Нетрудно видеть, что для любого i, $1 \leqslant i \leqslant n$, функция f_i зависит существенным образом от всех переменных кроме x_i.

Полученное семейство $F = \{f_1, f_2, \ldots, f_n\}$ является правильным, удовлетворяет условию леммы и имеет полный граф существенной зависимости G_F.

Замечание. Приведенные в предыдущих разделах результаты для случаев булевских функций и функций k-значной логики являются важными частными случаями ($G = \mathbb{Z}_2$ и $G = \mathbb{Z}_p$, соответственно) настоящей конструкции над абелевыми группами.

4. Негрупповые латинские квадраты

Еще одной важной задачей является построение латинских квадратов, не являющихся таблицей умножения конечной группы. Очевидно, что таблица умножения (таблица Кэли) любой конечной группы является латинским квадратом. Обратное, вообще говоря, неверно: не всегда на элементах латинского квадрата можно ввести бинарную операцию так, чтобы данный латинский квадрат представлял со-

бой таблицу умножения полученной алгебраической структуры. Ниже приводится целый класс таких латинских квадратов, полученный Л. Э. Будагяном в его дипломной работе.

Рассмотрим частный случай случай квадратов над циклической группой $\mathbb{Z}_n$. Для $x, y \in \mathbb{Z}$ определим элемент $L(x, y)$ квадрата формулой

$$L(x, y) = \pi(x + y) + x \tag{10}$$

или формулой

$$L(x, y) = \pi(x + y) - x, \tag{11}$$

где π — произвольное отображение множества $\mathbb{Z}_n$ в себя. Обозначим через π^+ (π^-) класс отображений π, задающих латинский квадрат по формуле (10) (соответственно, по формуле (11)).

Теорема 11. *[10]*

1) *Отображение $\pi = \pi(x)$ принадлежит классу π^+ (π^-) тогда и только тогда, когда, во-первых, π является перестановкой и, во-вторых, $\sigma(x) = \pi(x) + x$ (соответственно, $\sigma(x) = \pi(x) - x$) также является перестановкой.*
2) *Классы π^+ и π^- пусты при чётных n и непусты при нечётных n.*
3) *Классы π^+ и π^- равномощны, но не совпадают. В случае нечётного n их мощность нечётна и делится на n.*

Рассмотрим простое поле $\mathbb{F}_p$ порядка $p > 5$. При таких p всегда имеется разложение $p - 1 = l \cdot m$, $l > 2$, $m \geqslant 2$. Зафиксируем образующий s мультипликативной группы $\mathbb{F}_p^*$ (он имеет порядок $p - 1$). Обозначим $k = s^m$. Тогда любой элемент $x \in \mathbb{F}_p^*$ можно представить в виде произведения $x = s^\alpha \cdot k^\beta$, $0 \leqslant \alpha \leqslant m-1$, $0 \leqslant \beta \leqslant l$. Перестановка $\pi(x) = kx$ принадлежит классу π^+ и имеет следующую цикловую структуру:

$$\pi = (0)(1\ k\ k^2\ \ldots\ k^{l-1})(s\ sk\ sk^2\ \ldots\ sk^{l-1})\ldots \\ \ldots(s^{m-1}\ s^{m-1}k\ s^{m-1}k^2\ \ldots\ s^{m-1}k^{l-1}).$$

Можно показать, что перестановка, полученная из π заменой любых циклов на обратные, также принадлежит классу π^+. Пусть $\epsilon = (\epsilon_0, \ldots, \epsilon_{m-1})$, где $\epsilon_0 = 1$, $\epsilon_i = \pm 1$, $i = 1, \ldots, m-1$. Обозначим через π_ϵ перестановку, полученную из π обращением циклов с номерами i такими, что $\epsilon_i = -1$.

Теорема 12. *[10] Если $\epsilon \neq (1, \ldots, 1)$, то формула $L(x, y) = \pi_\epsilon(x + y) + x$ определяет негрупповой (не изоморфный таблице умножения никакой конечной группы) латинский квадрат.*

5. Заключение

В работе исследуются функциональные способы задания латинских квадратов над множествами n-мерных булевых векторов, n-мерных векторов над произвольным простым конечным полем и произвольной конечной абелевой группой.

В булевом случае приведены критерии того, что семейство функций от $2n$ переменных определяет латинский квадрат. В теореме 1 условия сформулированы в терминах свойств полиномов Жегалкина. В теореме 2 задача сводится к проверке свойства правильности семейства функций. Теорема 3 устанавливает взаимосвязь между правильностью семейства функций и существенной зависимостью произведений этих функций от подмножеств их аргументов.

Далее эти результаты обобщаются на случай p-значной логики (когда элементы квадрата являются n-мерными векторами над произвольным простым конечным полем).

Следующим обобщением являются квадраты над произвольными конечными абелевыми группами. Помимо аналогов результатов о семействах булевых функций и функций k-значной логики в случае абелевых групп получен критерий правильности семейства линейных функций в терминах отсутствия циклов в графа существенной зависимости. Этот критерий затем обобщён на более широкий класс g-функций (для любого фиксированного числа переменных доля g-функций стремится к 1 с ростом порядка группы). Также приведено простое достаточное условие построения правильных семейств

функций над абелевыми группами с богатой цикловой структурой в графе существенной зависимости.

Наконец, в заключительной части работы приводится конструкция функционального задания класса негрупповых латинских квадратов (то есть латинских квадратов, не являющихся таблицей умножения конечной группы).

Список литературы

[1] Shannon C. Communication Theory of Secrecy Systems // Bell System Techn. J. **28**, № 4. 1949. P. 656–715. [Имеется перевод: Шеннон К. Теория связи в секретных системах // В сб.: К. Шеннон. Работы по теории информации и кибернетике. М., 1963. С. 333–369.]

[2] Denes J., Keedwell A. D. Latin squares and their applications. Budapest, 1974.

[3] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. Т. 3, вып. 3–4. 1998. С. 269–280.

[4] Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. Т. 4, вып. 3–4. 1999. С. 307–320.

[5] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. Т. 8, вып. 1–4. 2004. С. 517–528.

[6] Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. Т. 12, вып. 3. 2006. С. 65–71.

[7] Клосс Б. М., Малышев В. А. Определение регулярности автомата по его каноническим уравнениям // Доклады АН СССР. Т. 172. №. 3. 1967. С. 543–546.

[8] Применко Э. А., Скворцов Э. Ф. Об условиях регулярности конечных автономных автоматов // Дискретная математика. Т. 2, вып. 1. 1990. С. 26–30.

[9] Lidl R., Niederreiter H. Finite Fields. Reading, Massachusetts, Addison-Wesley, 1983. [Имеется перевод: Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.]

[10] Будагян Л. Э. Построение негрупповых латинских квадратов произвольно больших порядков // В сб.: Математика и безопасность информационных технологий. Материалы конференции в МГУ 23–24 октября 2003 г. М., 2004. С. 410–412.