Матрицы и графы существенной зависимости правильных семейств функций*

А. А. КОЗЛОВ
Московский государственный университет им. М. В. Ломоносова

В. А. НОСОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vnosov40@mail.ru

А. Е. ПАНКРАТЬЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: apankrat@shade.msu.ru

УДК 519.1+519.7

Ключевые слова: латинский квадрат, булева матрица, граф существенной зависимости семейства функций, правильное семейство функций.

Аннотация

В работе исследуются правильные семейства функций, применяемые при функциональном задании латинских квадратов большого порядка над множеством n-мерных булевых векторов. Правильные семейства функций изучаются с точки зрения структуры соответствующих графов существенной зависимости и их матриц инцидентности. Выведены различные необходимые и достаточные условия, при которых булева матрица реализуется как матрица существенной зависимости некоторого правильного семейства функций. Рассмотрены преобразования матриц, сохраняющие указанное свойство. Показано, что любой ориентированный граф без петель и кратных рёбер можно достаточно экономно вложить в качестве вершинного подграфа в граф существенной зависимости правильного семейства функций. При этом функции получаемого правильного семейства наследуют свойства семейства функций, реализующего исходный граф.

Abstract

A. A. Kozlov, V. A. Nosov, A. E. Pankratiev, Matrices and graphs of essential dependence of proper families of functions, Fundamentalnaya i prikladnaya matematika, vol. 14 (2008), no. 4, pp. 137—149.

This paper considers proper families of functions, which are used in functional specification of Latin squares of large size over the set of n-dimensional binary vectors. Proper families of functions are studied from the viewpoint of the intrinsic structure of the corresponding graphs of essential dependence and their adjacency matrices. Various necessary

*Работа поддержана Советом при Президенте РФ по поддержке ведущих научных школ, грант № НШ-1983.2008.1.

Фундаментальная и прикладная математика, 2008, том 14, № 4, с. 137—149.

and sufficient conditions for a binary matrix to be treated as the adjacency matrix of the graph of essential dependence of a proper family of functions are derived. Also, transformations of matrices are considered, under which the indicated property is preserved. It is demonstrated that any directed graph without loops and multiple edges can be embedded as an induced subgraph into the graph of essential dependence of some proper family of functions. Moreover, such embedding is reasonably economical and the functions of the resulting proper family inherit properties of the functions that realize the original graph as the graph of essential dependence.

Памяти Евгения Васильевича Панкратьева

1. Введение

Настоящая работа посвящена изучению свойств правильных семейств функций. Такие семейства функций применяются при построении больших латинских квадратов, широко используемых в различных областях математики и кибернетики: теории кодирования, планировании эксперимента, защите информации [9]. В своей фундаментальной теоретической работе [8], посвящённой 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.

Применяемые в области защиты информации латинские квадраты могут иметь достаточно большие размеры, что делает затруднительным поэлементное хранение в памяти компьютера всего квадрата целиком. Возникает потребность в разработке конструктивных методов задания латинских квадратов. Широкое распространение получило аналитическое задание латинских квадратов при помощи функции двух переменных, определяющей элемент квадрата по его координатам (номеру строки и столбца). Свойства возникающих при этом функций и составляют предмет настоящего исследования.

Напомним, что латинским квадратом порядка n называется матрица размера $n \times n$, заполненная элементами некоторого n-элементного множества Ω таким образом, что в каждой её 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 задаётся формулой $L(x,y) = x + y$, где x и y — «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 $L(x,y) = x + y$

задаёт латинский квадрат над абелевой группой $\mathbb{Z}_n$). Произвольный латинский квадрат порядка n над группой $\mathbb{Z}_n$ задаётся 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 задавать их более наглядно и удобно с вычислительной точки зрения.

В [2,3] вводится и изучается конструкция, обобщающая формулу (1). Функция $f(x,y)$ рассматривается как вектор-функция или семейство булевых функций. В терминах свойств этого семейства функций формулируются необходимые и достаточные условия того, что матрица, задаваемая формулой (1), является латинским квадратом. В дальнейшем эта конструкция была перенесена на функции p-значной логики [4] (т. е. на множество n-мерных векторов над простым полем $\mathbb{F}_p$) и далее на множество n-мерных векторов над произвольной абелевой группой [5,6]. Настоящая работа продолжает указанные исследования.

2. Задание латинских квадратов правильными семействами булевых функций

Рассмотрим множество $\Omega = E^n$ двоичных векторов длины n и квадратную матрицу L размера $2^n \times 2^n$, элементами которой являются n-мерные двоичные векторы. «Занумеруем» строки и столбцы квадрата L элементами множества E^n и будем считать, что 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 $y = (y_1,\ldots,y_n)$, определяется 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 от $2n$ переменных $x_1,\ldots,x_n,y_1,\ldots,y_n$.

Используя известные результаты о регулярности системы булевых функций [1], можно показать [3], что семейство n булевых функций $G = \{g_1,g_2,\ldots,g_n\}$ от $2n$ переменных $x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n$ задаёт латинский квадрат с помощью формул (2) тогда и только тогда, когда во всех произведениях $g_{i_1}\ldots g_{i_k}$, $1 \leqslant i_1 < \ldots < i_k \leqslant n$, $k < n$, в полиноме Жегалкина нет членов, содержащих вхождения $x_1\ldots x_n$ или $y_1\ldots y_n$, а произведение $g_1\ldots g_n$ содержит оба таких члена и не содержит других членов, их содержащих.

Приведём параметрический способ задания семейства латинских квадратов [3]. Пусть дано семейство булевых функций $F = \{f_i\}_{i=1}^n$, $f_i = f_i(z_1,\ldots,z_n)$, и пусть $\pi_1(x_1,y_1),\ldots,\pi_n(x_n,y_n)$ — семейство булевых функций от двух переменных. Определим систему функций $G = \{g_1,\ldots,g_n\}$ от $2n$ переменных $x_1,\ldots,x_n$, $y_1,\ldots,y_n$ соотношениями

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

Условие, при котором семейство функций $G = \{g_1, g_2, \ldots, g_n\}$ вида (3) определяет с помощью формул (2) латинский квадрат, можно сформулировать в терминах следующего свойства.

Определение. Семейство булевых функций $F = \{f_i\}_{i=1}^n$, $f_i = f_i(z_1, \ldots, z_n)$, является правильным, если для любых различных наборов значений аргументов $z' = (z'_1, z'_2, \ldots, z'_n)$ и $z'' = (z''_1, z''_2, \ldots, z''_n)$ найдётся такой индекс $\alpha \in \overline{1,n}$, что

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

Теорема 1 [3]. *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 1 позволяет при помощи любого правильного семейства функций $F = \{f_1, f_2, \ldots, f_n\}$ получать различные латинские квадраты, варьируя систему функций-параметров $\pi_1, \pi_2, \ldots, \pi_n$.

Замечание. Используя известные результаты о регулярности семейства функций p-значной логики [7], можно обобщить введённые выше определения и утверждение теоремы 1 на случаи n-мерных векторов над простым полем [4] и n-мерных векторов с коэффициентами из любой конечной абелевой группы [5].

Для некоторых классов функций можно привести эффективный критерий правильности семейства в терминах цикловой структуры соответствующего графа существенной зависимости.

Определение. Графом существенной зависимости семейства функций $F = \{f_i\}_{i=1}^n$, $f_i = f_i(z_1, \ldots, z_n)$, называется такой ориентированный граф $G_F = (V, E)$ на множестве вершин $V = \{1, 2, \ldots, n\}$, что $(i, j) \in E$, если и только если f_j существенно зависит от x_i.

Теорема 2 [5]. *Семейство линейных функций $F = \{f_1, f_2, \ldots, f_n\}$ является правильным в том и только в том случае, если его граф существенной зависимости G_F не содержит циклов.*

Класс функций, для которого правильность семейств равносильна отсутствию циклов в графах существенной зависимости, можно существенно расширить [6].

Приведём теперь пример правильного семейства функций, имеющего полный граф существенной зависимости.

Булевы функции $f = f(x_1, \ldots, x_n)$ и $g = g(x_1, \ldots, x_n)$ будем называть *ортогональными*, если для любого $x = (x_1, \ldots, x_n) \in E^n$ выполнено условие $f(x) \cdot g(x) = 0$, т. е. функция fg тождественно равна нулю.

Лемма 1. *Пусть $n \geqslant 3$ и семейство $F = \{f_1, f_2, \ldots, f_n\}$ попарно ортогональных булевых 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 $F = \{f_1, f_2, \ldots, f_n\}$.

Приведём 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. Определим функции f_i формулами

$$\begin{aligned} f_1 &= \bar{x}_2 x_3 \ldots x_{n-1} x_n, \\ f_2 &= \bar{x}_3 x_4 \ldots x_n x_1, \\ &\ldots \\ f_n &= \bar{x}_1 x_2 \ldots x_{n-2} x_{n-1}. \end{aligned}$$

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 (так как оно удовлетворяет условию леммы) и имеет полный граф существенной зависимости G_F.

Замечание. Приведённый выше пример можно обобщить на случай n-мерных векторов с коэффициентами из произвольной конечной абелевой группы.

3. Представление правильных семейств функций матрицами существенной зависимости

Определение. Назовём булеву матрицу *правильной*, если она является матрицей существенной зависимости (т. е. матрицей инцидентности графа существенной зависимости) некоторого правильного семейства функций.

В качестве примера правильной матрицы можно взять любую нижнетреугольную матрицу (такие матрицы соответствуют так называемым треугольным семействам функций, которые являются правильными [5]).

В данном разделе мы приведём свойства правильных и неправильных булевых матриц и укажем некоторые преобразования матриц, при которых свойство правильности (или неправильности) сохраняется.

Теорема 3. *Пусть A — правильная матрица размера $n \times n$. Тогда матрица $\bar{A}$, полученная из матрицы A обнулением любой строки, также является правильной.*

Доказательство. Пусть $F = \{f_i(x_1, \ldots, x_n)\}_{i=1}^n$ — соответствующее матрице A правильное семейство функций. Будем считать, что матрица $\bar{A}$ получена из матрицы A обнулением k-й строки.

Рассмотрим семейство функций $\bar{F} = \{\bar{f}_i(x_1, \ldots, x_n)\}_{i=1}^n$, где $f_k = \mathrm{const}$ и $\bar{f}_i(x_1, \ldots, x_n) = f_i(x_1, \ldots, x_n)$, $1 \leqslant i \leqslant n$, $i \neq k$. Обратим внимание на то, что

при $i \neq k$ функция $\bar{f}_i$ существенно зависит от тех же аргументов, что и функция f_i. Очевидно также, что матрица существенной зависимости семейства $\bar{F}$ равна $\bar{A}$.

Покажем теперь, что семейство $\bar{F}$ является правильным. Возьмём произвольные различные наборы $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$.

В силу правильности семейства F найдётся индекс i, $1 \leqslant i \leqslant n$, такой что $a_i \neq b_i$ и $f_i(a) = f_i(b)$. Но тогда по построению семейства $\bar{F}$ имеем $\bar{f}_i(a) = \bar{f}_i(b)$ (так как $\bar{f}_k = \mathrm{const}$, а при $i \neq k$ функции f_i и $\bar{f}_i$ совпадают: $\bar{f}_i(a) = f_i(a) = f_i(b) = \bar{f}_i(b)$).

Таким образом, доказана правильность семейства $\bar{F}$, а вместе с ней и правильность матрицы $\bar{A}$. □

Теорема 4. *Пусть некоторый (для определённости k-й) столбец булевой матрицы A размера $n \times n$ полностью состоит из нулей. Тогда матрица $\bar{A}$ размера $(n-1) \times (n-1)$, получающаяся из A удалением k-го столбца и k-й строки, является правильной, если и только если матрица A является правильной.*

Доказательство. Достаточность. Пусть матрица A размера $n \times n$ является правильной и $F = \{f_i(x_1, \ldots, x_n)\}_{i=1}^n$ — соответствующее ей правильное семейство функций. Без ограничения общности считаем, что $k = n$, т. е. фигурирующий в условии теоремы нулевой столбец матрицы A имеет номер n (такое допущение корректно, поскольку правильность семейства функций инвариантна относительно согласованной перестановки индексов, см. [5]). Это означает, что никакая функции семейства F не зависит существенно от переменной x_n.

Рассмотрим семейство функций $\bar{F} = \{\bar{f}_i(x_1, \ldots, x_{n-1})\}_{i=1}^{n-1}$ от $n-1$ переменной $x_1, \ldots, x_{n-1}$, определяемых равенствами

$$\bar{f}_i(x_1, \ldots, x_{n-1}) = f_i(x_1, \ldots, x_{n-1}, 0).$$

Обратим внимание на то, что для любого i, $1 \leqslant i \leqslant n-1$, функция $\bar{f}_i$ существенно зависит от тех же аргументов, что и функция f_i. Очевидно также, что матрица существенной зависимости семейства $\bar{F}$ совпадает с $\bar{A}$.

Возьмём теперь произвольные различные наборы $\bar{a} = (a_1, \ldots, a_{n-1})$ и $\bar{b} = (b_1, \ldots, b_{n-1})$. В силу правильности семейства F для наборов $a = (a_1, \ldots, a_{n-1}, 0)$ и $b = (b_1, \ldots, b_{n-1}, 0)$ найдётся индекс i, $1 \leqslant i \leqslant n-1$, такой что $a_i \neq b_i$ и $f_i(a) = f_i(b)$. Но тогда по построению семейства $\bar{F}$ имеем $\bar{f}_i(\bar{a}) = f_i(a) = f_i(b) = \bar{f}_i(\bar{b})$. Тем самым доказана правильность семейства $\bar{F}$, а вместе с ней и правильность матрицы $\bar{A}$.

Необходимость. Пусть матрица $\bar{A}$ размера $(n-1) \times (n-1)$ является правильной и $\bar{F} = \{\bar{f}_i(x_1, \ldots, x_{n-1})\}_{i=1}^{n-1}$ — соответствующее ей правильное семейство функций. Без ограничения общности можно считать, что матрица A получена из матрицы $\bar{A}$ добавлением n-го столбца, состоящего полностью из нулей, и n-й строки $(\alpha_1 \alpha_2, \ldots, \alpha_{n-1}, 0)$.

Рассмотрим семейство функций $F = \{f_i(x_1, \ldots, x_n)\}_{i=1}^n$ от n переменных $x_1, \ldots, x_n$, где функции f_i, $1 \leqslant i \leqslant n-1$, определяются равенствами

$$f_i(x_1, \ldots, x_n) = \bar{f}_i(x_1, \ldots, x_{n-1}) \quad \text{при любом значении аргумента } x_n,$$

а f_n — произвольная функция, удовлетворяющая условию существенной зависимости, определяемому выбранной n-й строкой $(\alpha_1, \ldots, \alpha_{n-1}, 0)$. Обратим внимание на то, что для любого i, $1 \leqslant i \leqslant n-1$, функция f_i существенно зависит от тех же аргументов, что и функция $\bar{f}_i$. Очевидно также, что матрица существенной зависимости семейства F совпадает с A.

Возьмём произвольные различные наборы $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$. Если они различаются только по n-й компоненте, то имеем $f_n(a) = f_n(b)$, так как функция f_n не зависит существенно от аргумента x_n.

Если наборы a и b различаются не только по n-й компоненте, то наборы $\bar{a} = (a_1, \ldots, a_{n-1})$ и $\bar{b} = (b_1, \ldots, b_{n-1})$ также различны и в силу правильности семейства $\bar{F} = \{\bar{f}_i(x_1, \ldots, x_{n-1})\}_{i=1}^{n-1}$ найдётся индекс i, $1 \leqslant i \leqslant n-1$, такой что $a_i \neq b_i$ и $\bar{f}_i(\bar{a}) = \bar{f}_i(\bar{b})$. Тогда по построению семейства F имеем $f_i(a) = f_i(b)$.

В обоих случаях для различных наборов a и b найдётся индекс i, такой что $a_i \neq b_i$ и $f_i(a) = f_i(b)$. Тем самым доказана правильность семейства функций F, а вместе с ней и правильность матрицы A. □

Соберём вместе свойства правильных матриц. Если булева матрица A размера $n \times n$ является правильной, то

1) матрица A имеет нулевую главную диагональ;
2) матрица, полученная из A применением одной и той же перестановки к наборам строк и столбцов, является правильной;
3) матрица, полученная из A обнулением любой строки, является правильной;
4) если некоторый (для определённости i-й) столбец матрицы A состоит из нулей, то матрица, полученная из A вычёркиванием i-го столбца и i-й строки, является правильной;
5) матрица размера $(n+1)\times(n+1)$, полученная добавлением к A произвольной $(n+1)$-й строки и нулевого $(n+1)$-го столбца, является правильной.

Приведём теперь некоторые условия, при которых булева матрица заведомо не может быть правильной.

Теорема 5.

1. *Если булева матрица $A = \{a_{ij}\}$ содержит пару строк (с индексами i и j), для которых $a_{ij} = a_{ji} = 1$ и не существует $k \in \overline{1,n}$, такого что $a_{ik} = a_{jk} = 1$, то матрица A не является правильной.*
2. *Если каждая строка булевой матрицы A содержит ровно одну единицу, то матрица A не является правильной (в частности, перестановочная матрица не может быть правильной).*

Доказательство.

1. Пусть матрица A реализуется как матрица существенной зависимости некоторого семейства функций $F = \{f_i\}_{i=1}^n$. Покажем, что семейство F не может быть правильным.

Обозначим множества переменных, от которых существенным образом зависят функции f_i и f_j, через $S = \{x_{s_1}, \ldots, x_{s_k}\}$ и $T = \{x_{t_1}, \ldots, x_{t_m}\}$ соответственно. По условию теоремы $x_j \in S$, $x_i \in T$ и эти множества не пересекаются: $S \cap T = \varnothing$.

Покажем теперь, что можно выбрать различные наборы $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ таким образом, чтобы они отличались только по переменным x_i, x_j и обе функции f_i, f_j принимали на этих наборах различные значения. По определению существенной зависимости функции f_i от переменной x_j можно выбрать значения $\{\bar{x}_1, \ldots, \bar{x}_{j-1}, \bar{x}_{j+1}, \ldots, \bar{x}_n\}$ всех остальных аргументов так, чтобы выполнялось неравенство

$$f_i(\bar{x}_1, \ldots, \bar{x}_{j-1}, 0, \bar{x}_{j+1}, \ldots, \bar{x}_n) \neq f_i(\bar{x}_1, \ldots, \bar{x}_{j-1}, 1, \bar{x}_{j+1}, \ldots, \bar{x}_n).$$

Заметим, что при этом значения всех аргументов, не входящих в множество S, можно выбрать произвольным образом. В частности, значения аргументов из множества $T \setminus \{x_i\}$ можно выбрать так, чтобы выполнялось неравенство

$$f_j(\bar{x}_1, \ldots, \bar{x}_{i-1}, 0, \bar{x}_{i+1}, \ldots, \bar{x}_n) \neq f_j(\bar{x}_1, \ldots, \bar{x}_{i-1}, 1, \bar{x}_{i+1}, \ldots, \bar{x}_n).$$

Теперь определим наборы

$$x' = (\bar{x}_1, \ldots, \bar{x}_{i-1}, 0, \bar{x}_{i+1}, \ldots, \bar{x}_{j-1}, 0, \bar{x}_{j+1}, \ldots, \bar{x}_n),$$
$$x'' = (\bar{x}_1, \ldots, \bar{x}_{i-1}, 1, \bar{x}_{i+1}, \ldots, \bar{x}_{j-1}, 1, \bar{x}_{j+1}, \ldots, \bar{x}_n).$$

Очевидно, что наборы x', x'' отличаются только по переменным x_i, x_j, но обе функции f_i, f_j принимают на них различные значения. Это противоречит определению правильности семейства функций.

2. Пусть, как и выше, матрица A реализуется как матрица существенной зависимости некоторого семейства функций $F = \{f_i\}_{i=1}^n$. Покажем, что семейство F не может быть правильным.

Рассмотрим наборы $x' = (0, 0, \ldots, 0)$ и $x'' = (1, 1, \ldots, 1)$. По условию каждая функция зависит существенным образом ровно от одной переменной. Поэтому $f_i(x') \neq f_i(x'')$, $i \in \overline{1, n}$. □

Замечание. Утверждение 2 теоремы 5 можно усилить следующим образом. Пусть матрица A приводится согласованной перестановкой строк и столбцов к блочному виду

$$A = \begin{pmatrix} B & 0 \\ C & D \end{pmatrix},$$

где B — квадратная булева матрица, содержащая ровно одну единицу в каждой строке. Тогда матрица A не может быть правильной.

В самом деле, достаточно рассмотреть наборы x', x'', различающиеся по всем аргументам, соответствующим «номерам» строк подматрицы B, и совпадающие по всем остальным аргументам.

Замечание. Правильность булевой матрицы может быть нарушена

1) при несогласованной перестановке её строк и столбцов;
2) при транспонировании.

Приводимый ниже результат будет переформулирован и доказан в следующем разделе в терминах графа существенной зависимости семейства функций.

Теорема 6. *Любую булеву матрицу размера $n \times n$ с нулевой диагональю можно расширить* (*добавлением новых строк и столбцов*) *до правильной матрицы размера не более чем* $(n + \lceil \log_2 n \rceil) \times (n + \lceil \log_2 n \rceil)$.

В заключение настоящего раздела сформулируем некоторые проблемы, возникающие при исследовании правильных семейств функций с точки зрения свойств их матриц существенной зависимости.

1. Классификация булевых матриц на правильные и неправильные.
2. Нахождение правильного семейства функций с заданной правильной матрицей существенной зависимости.
3. Нахождение критериев того, что данная правильная матрица может соответствовать семействам, определяющим различные (неизоморфные, неизотопные) латинские квадраты.
4. Приведение заданной матрицы к правильной матрице путём изменения наименьшего количества элементов.
5. Нахождение классов матриц, из которых можно получить правильную матрицу путём присоединения малого числа строк и столбцов (в частности, одной строки и одного столбца).

4. Представление правильных семейств функций графами существенной зависимости

Выше мы видели, что любому (не обязательно правильному) семейству функций можно поставить в соответствие ориентированный граф, называемый графом существенной зависимости данного семейства функций. В связи с этим естественно задать вопрос: какие ориентированные графы являются графами существенной зависимости правильных семейств функций?

Замечание. Граф существенной зависимости правильного семейства функций не содержит петель.

Замечание. Любой граф без (ориентированных) циклов является графом существенной зависимости правильного семейства функций.

Из существования правильных семейств функций с полным графом существенной зависимости [6] вытекает очевидное свойство, что любой ориентированный граф G без петель и кратных рёбер можно вложить в граф, реализуемый в виде графа существенной зависимости некоторого правильного семейства функций. Однако при таком вложении исходный граф G может пополниться большим количеством новых рёбер. Более того, предъявленное в [6] правильное семейство функций, реализующее полный граф существенной зависимости, может иметь мало общего с семейством функций, реализующим исходный граф G.

В связи с этим возникает естественный вопрос: можно ли вложить исходный граф G в некоторый больший граф G', реализуемый в виде графа существенной зависимости некоторого правильного семейства функций $F' = \{f'_i\}$, таким образом, чтобы сохранилась структура графа G? Это особенно важно, если исходный граф G возник как граф существенной зависимости некоторого заданного семейства функций $F = \{f_i\}$. В этом случае желательно, чтобы функции f'_i были максимально «похожи» на исходные функции f_i в том смысле, что для некоторого фиксированного набора значений вновь добавленных аргументов функции f'_i полностью совпадали бы с функциями f_i как функции от исходных аргументов. Оказывается, что такое вложение возможно и количество вершин, которые требуется добавить, мало по сравнению с размерами исходного графа.

Перед тем как сформулировать основной результат, докажем следующее вспомогательное утверждение.

Лемма 2. *Пусть $G(V, E)$ — ориентированный граф без петель, являющийся графом существенной зависимости некоторого семейства функций $F = \{f_i\}_{i=1}^{n}$. Пусть граф $G'(V', E')$ получен добавлением к графу $G(V, E)$ некоторого множества $\bar{V}$ новых вершин и рёбер, начинающихся в новых вершинах и оканчивающихся в вершинах из множества V. При этом добавленные рёбра разделены на две группы E_0, E_1 так, что в каждый ориентированный цикл исходного графа G входят два ребра, исходящие из одной и той же новой вершины и принадлежащие разным группам. Тогда граф $G'(V', E')$ реализуется в виде графа существенной зависимости некоторого правильного семейства функций $F' = \{f'_i\}_{i=1}^{n'}$, причём для каждого i, $1 \leqslant i \leqslant n$, существует набор значений аргументов $x_{n+1}, \ldots, x_{n'}$, при которых f'_i как функция от n аргументов $x_1, \ldots, x_n$ совпадает с f_i.*

Доказательство. Определим функции $f'_i = f'_i(x_1, \ldots, x_{n'})$, $i \in \overline{1, n'}$ следующим образом. При $i = \overline{n+1, n'}$ возьмём $f'_i = \mathrm{const}$, а при $i \leqslant n$ положим

$$f'_i(x_1, \ldots, x_{n'}) \stackrel{\text{def}}{=} f_i(x_1, \ldots, x_n) \cdot x_{s_1} \cdot \ldots \cdot x_{s_k} \cdot \bar{x}_{t_1} \cdot \ldots \cdot \bar{x}_{t_m},$$

где $\{s_1, \ldots, s_k\}$ и $\{t_1, \ldots, t_m\}$ — множества новых вершин, из которых в вершину i проведены рёбра, принадлежащие соответственно группам E_0 и E_1 (т. е. $s_j, t_l \in V' \setminus V$ и $(s_j, i) \in E_0$, $(t_l, i) \in E_1$, $j \in \overline{1, k}$, $l \in \overline{1, m}$).

Покажем, что определённое таким образом семейство функций $F' = \{\bar{f}_i\}_{i=1}^{n'}$ является правильным. Рассмотрим два различных набора значений аргументов $x' = (x'_1, \ldots, x'_{n'})$ и $x'' = (x''_1, \ldots, x''_{n'})$. Если они различаются по какой-нибудь переменной с индексом $i \geqslant n+1$, то соответствующая функция f'_i, будучи константой, принимает на этих наборах одно и то же значение.

Теперь рассмотрим наборы x', x'', различающиеся по переменным $x_{\alpha_1}, \ldots, x_{\alpha_k}$, где никакой индекс α_j не превосходит n. Если вершинный подграф графа $G(V, E)$, соответствующий множеству вершин $\Omega = \{\alpha_1, \ldots, \alpha_k\}$, не содержит ориентированных циклов, то в нём найдётся вершина α_j, в которую не входит

ни одно ребро, начинающееся в Ω. Это означает, что соответствующая функция f'_{α_j} не зависит существенным образом от переменных из множества Ω и, следовательно, принимает одно и то же значение на наборах x', x''.

Остаётся рассмотреть случай, когда соответствующий вершинный подграф содержит ориентированный цикл C. Без ограничения общности можно считать, что $C = \alpha_1\alpha_2\ldots\alpha_m$, $m \leqslant k$. По условию леммы в графе $G'(V', E')$ найдётся вершина s, $s \geqslant n+1$, из которой выходят два ребра, оканчивающиеся в вершинах цикла и принадлежащие разным группам E_0, E_1. Пусть $(s, \alpha_p) \in E_0$, $(s, \alpha_q) \in E_1$. Тогда обе функции f'_{α_p}, f'_{α_q} зависят существенным образом от переменной x_s и по построению семейства F' имеем

$$f'_{\alpha_p}(x') = f'_{\alpha_p}(x'') = 0 \quad \text{при} \quad x'_s = x''_s = 0,$$
$$f'_{\alpha_q}(x') = f'_{\alpha_q}(x'') = 0 \quad \text{при} \quad x'_s = x''_s = 1.$$

Итак, во всех случаях найдётся такой индекс i, что $x'_i \neq x''_i$, но $f'_i(x') = f'_i(x'')$. Тем самым правильность семейства F' доказана. Тот факт, что функции f'_i можно ограничить на переменные $x_1, \ldots, x_n$ таким образом, чтобы они совпали с функциями f_i, следует непосредственно из построения семейства F'. Лемма доказана. □

Теорема 7. *Пусть $G(V, E)$ — произвольный ориентированный граф без петель и кратных рёбер на n вершинах $V = \{1, 2, \ldots, n\}$. Тогда существует граф $G'(V', E')$ на $n' \leqslant n + \lceil \log_2 n \rceil$ вершинах $V' = \{1, 2, \ldots, n'\}$, реализуемый в виде графа существенной зависимости некоторого правильного семейства функций и такой, что его вершинный подграф на подмножестве $V \subseteq V'$ совпадает с G. Более того, для любого семейства функций $F = \{f_i\}_{i=1}^n$, реализующего исходный граф G, найдётся правильное семейство функций $F' = \{f'_i\}_{i=1}^{n'}$, реализующее граф G' и такое, что для каждого i, $1 \leqslant i \leqslant n$, существует набор значений аргументов $x_{n+1}, \ldots, x_{n'}$, при которых f'_i как функция от n аргументов $x_1, \ldots, x_n$ совпадает с f_i.*

Доказательство. Покажем, что к графу $G(V, E)$ на n вершинах можно добавить не более $\lceil \log_2 n \rceil$ новых вершин и провести рёбра так, чтобы полученный граф $G'(V', E')$ удовлетворял условиям леммы 2.

В самом деле, достаточно, чтобы для каждой пары вершин $i, j \in V$ можно было указать новую вершину $n + k$, из которой бы исходили рёбра $(n + k, i)$ и $(n + k, j)$, принадлежащие разным группам.

Будем последовательно добавлять к графу по одной вершине, соединять её рёбрами с вершинами исходного множества V и разбивать получающиеся рёбра на две группы.

На первом шаге исходное множество вершин V разобьём на два равномощных (или почти равномощных) подмножества $V = V_0 \sqcup V_1$, $|V_0| = \lfloor |V|/2 \rfloor$, $|V_1| = \lceil |V|/2 \rceil$. Затем, добавив новую вершину $n + 1$, соединим её со всеми вершинами множества V и разобьём новые рёбра на две группы E_0 и E_1 так, что $(n + 1, i) \in E_0$ при $i \in V_0$ и $(n + 1, i) \in E_1$ при $i \in V_1$. Тем самым для любой пары вершин i, j исходного графа, принадлежащих разным подмножествам

($i \in V_0$, $j \in V_1$), имеется новая вершина $n+1$, из которой исходят рёбра $(n+1, i)$ и $(n+1, j)$, принадлежащие разным группам E_0, E_1.

На втором шаге каждое из множеств V_0, V_1 разобьём на два равномощных (или почти равномощных) подмножества $V_0 = V_{00} \sqcup V_{01}$, $V_1 = V_{10} \sqcup V_{11}$ и, добавив новую вершину $n+2$, соединим её рёбрами со всеми элементами исходного множества V. Добавленные рёбра отнесём к группам E_0 и E_1 по правилу

$$(n+2, i) \in E_0 \Longleftrightarrow i \in V_{00} \cup V_{10}, \quad (n+2, i) \in E_1 \Longleftrightarrow i \in V_{01} \cup V_{11}.$$

Далее на k-м шаге каждое из полученных ранее подмножеств $V_s \subset V$ (здесь s — двоичный вектор длины $k-1$) разбиваем на два (почти) равномощных подмножества $V_s = V_{s0} \sqcup V_{s1}$, добавляем новую вершину $n+k$, соединяем её со всеми вершинами множества V и относим полученные рёбра к группам E_0, E_1 по правилу

$$(n+k, i) \in E_0 \Longleftrightarrow i \in \cup V_{s0}, \quad (n+k, i) \in E_1 \Longleftrightarrow i \in \cup V_{s1}$$

(здесь объединение берётся по всем двоичным наборам s длины $k-1$).

Нетрудно убедиться, что после $\lceil \log_2 n \rceil$ шагов исходное множество разбито на одноэлементные подмножества и для каждой пары элементов $i, j \in V$ на некотором этапе была добавлена вершина $n+k$, соединённая с вершинами i, j рёбрами, принадлежащими разным группам E_0, E_1. Таким образом, выполнены условия леммы 2, из которой и следует утверждение теоремы. □

Замечание. Если множество V вершин исходного графа $G(V, E)$ можно разбить на два подмножества $V = V_0 \sqcup V_1$ так, чтобы любой ориентированный цикл графа $G(V, E)$ проходил через вершины обоих подмножеств V_0, V_1, то для построения графа $G'(V', E')$ в теореме 7 достаточно добавить только одну новую вершину.

Замечание. Сформулированные в предыдущем разделе проблемы, возникающие при изучении правильных семейств функций с точки зрения структуры матриц существенной зависимости, имеют естественные аналоги в терминах графов существенной зависимости.

5. Заключение

В работе исследуются правильные семейства функций, применяемые при функциональном задании латинских квадратов большого порядка над множеством n-мерных булевых векторов.

Правильные семейства функций изучаются с точки зрения структуры соответствующих графов существенной зависимости и их матриц инцидентности. Получаемые здесь результаты во многом параллельны: свойства, доказанные для матриц, могут быть переформулированы в терминах графов, и наоборот. Выведены различные необходимые и достаточные условия, при которых булева

матрица реализуется как матрица существенной зависимости некоторого правильного семейства функций. Рассмотрены преобразования матриц, сохраняющие указанное свойство.

В заключительной части работы изучаются свойства графов существенной зависимости правильных семейств функций. Показано, что любой ориентированный граф без петель можно вложить в качестве вершинного подграфа в некоторый граф, реализуемый в виде графа существенной зависимости правильного семейства функций. При этом вложение является достаточно экономным (в том смысле, что добавляется небольшое количество новых вершин) и функции получаемого правильного семейства наследуют свойства семейства функций, реализующего исходный граф.

Литература

[1] Клосс Б. М., Малышев В. А. Определение регулярности автомата по его каноническим уравнениям // ДАН СССР. — 1967. — Т. 172, №. 3. — С. 543—546.

[2] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделённым входом // Интеллект. сист. — 1998. — Т. 3, вып. 3-4. — С. 269—280.

[3] Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллект. сист. — 1999. — Т. 4, вып. 3-4. — С. 307—320.

[4] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллект. сист. — 2004. — Т. 8, вып. 1-4. — С. 517—528.

[5] Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Фундамент. и прикл. мат. — 2006. — Т. 12, вып. 3. — С. 65—71.

[6] Носов В. А., Панкратьев А. Е. О семействах функций, задающих латинские квадраты над абелевыми группами // Вестн. Моск. гос. ун-та леса — Лесной вестник. — 2007. — № 2 (51). — С. 141—144.

[7] Применко Э. А., Скворцов Э. Ф. Об условиях регулярности конечных автономных автоматов // Дискрет. мат. — 1990. — Т. 2, вып. 1. — С. 26—30.

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

[9] Denes J., Keedwell A. D. Latin Squares and Their Applications. — Budapest, 1974.