Мальцевские чтения
Новосибирск (2006)
Тезисы докладов

Семейства функций, задающие латинские квадраты над абелевыми группами

В. А. Носов, А. Е. Панкратьев

Напомним, что латинским квадратом порядка k называется матрица размера $k \times k$, заполненная элементами некоторого множества Ω, $|\Omega| = k$, таким образом, что в каждой ее строке и в каждом столбце все элементы различны [**1**]. Простейший латинский квадрат задается формулой $L(x, y) = x + y$, где $L(x, y)$ — элемент квадрата, стоящий на пересечении строки и столбца с "номерами" x и y, соответственно, $x, y \in \Omega = \mathbb{Z}_k$, и сложение понимается как сложение по модулю k. В данной работе изучаются свойства функций $f(x, y) : \Omega \times \Omega \to \Omega$, задающих латинские квадраты при помощи формулы $L(x, y) = x + y + f(x, y)$ в том случае, когда Ω является абелевой группой.

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

$$H = G^n = \underbrace{G \times G \times \cdots \times G}_{n}. \tag{1}$$

Над группой H зададим латинский квадрат L порядка $|H| = |G|^n$ следующим образом. Сначала "проиндексируем" строки и столбцы квадрата L элементами группы H. Пусть $x = (x_1, x_2, \dots, x_n)$ и $y = (y_1, y_2, \dots, y_n)$ суть элементы группы H. Элемент $L(x, y) = (z_1, z_2, \dots, z_n)$ квадрата L, находящийся на пересечении строки x и столбца y, определим формулами

$$\begin{aligned} z_1 &= x_1 + y_1 + f_1(p_1(x_1, y_1), \dots, p_n(x_n, y_n)) \\ z_2 &= x_2 + y_2 + f_2(p_1(x_1, y_1), \dots, p_n(x_n, y_n)) \\ &\vdots \\ z_n &= x_n + y_n + f_n(p_1(x_1, y_1), \dots, p_n(x_n, y_n)). \end{aligned} \tag{2}$$

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

Будем говорить, что функции $f_1, f_2, \dots, f_n$ от переменных $p_1, p_2, \dots, p_n$ образуют *правильное* семейство [**2, 3, 4**], если для любых различных наборов $p' = (p'_1, p'_2, \dots, p'_n)$ и $p'' = (p''_1, p''_2, \dots, p''_n)$ найдется индекс α, $1 \le \alpha \le n$, такой, что $p'_\alpha \ne p''_\alpha$ и $f_\alpha(p') = f_\alpha(p'')$.

Теорема 1 ([**4**]). *Формулы (2) определяют латинский квадрат для любых функций $p_1, p_2, \ldots, p_n$ тогда и только тогда, когда семейство функций $\{f_1, f_2, \ldots, f_n\}$ является правильным.*

Замечание 1. Теорема 1 позволяет при помощи любого правильного семейства функций $\{f_1, f_2, \ldots, f_n\}$ получать различные латинские квадраты, варьируя систему функций-параметров $p_1, p_1, \ldots, p_n$. Нетрудно также видеть, что систему параметров можно выбрать $|H|^{n|H|}$ способами.

Понятие правильности семейства функций тесно связано с понятием регулярности, т.е. со свойством семейства функций осуществлять биективное отображение на множестве всех входных наборов.

Теорема 2 ([**4**]). *Функции $f_1, f_2, \ldots, f_n$ образуют правильное семейство тогда и только тогда, когда для любого набора функций $\psi_1, \psi_2, \ldots, \psi_n$ (здесь $\psi_i : G \to G$) семейство функций $\{x_1 + \psi_1(f_1(x)), x_2 + \psi_2(f_2(x)), \ldots, x_n + \psi_n(f_n(x))\}$ является регулярным.*

Для широкого класса функций проверку правильности семейства $F = \{f_1, f_2, \ldots, f_n\}$ можно свести к проверке отсутствия циклов в ориентированном *графе существенной зависимости* $G_F = (V, E)$ семейства F, который определяется на множестве вершин $V = \{1, 2, \ldots, n\}$ по правилу

$$(i, j) \in E \Leftrightarrow \{f_j \text{ существенно зависит от } x_i\}.$$

Для фиксированного элемента $g \in G$ функцию $f(x_1, \ldots, x_n)$ вида $G^n \to G$ назовем g-функцией, если для любой переменной x_i, от которой она зависит существенным образом, выполнено условие $f(g, \ldots, g, x_i, g, \ldots, g) \neq \mathrm{const}$. Заметим, что константы являются g-функциями для любого $g \in G$.

Замечание 2. Можно показать, что при $|G| \to \infty$, $|G|/n \to \infty$, доля g-функций среди всех функций n переменных стремится к 1.

Теорема 3. *Семейство g-функций $F = \{f_1, f_2, \ldots, f_n\}$ правильно в том и только том случае, если его граф существенной зависимости G_F не содержит циклов.*

С другой стороны, за рамками широкого класса g-функций существуют правильные семейства с богатой цикловой структурой в графе существенной зависимости.

Будем говорить, что функции f и g вида $G^n \to G$ *ортогональны*, 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, $1 \leq i \leq n$, функция f_i не зависит от x_i существенным образом. Тогда семейство F является правильным.*

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 (разумеется, за исключением петель (i, i)).

Возьмем произвольное собственное подмножество $L \subset H$, $\emptyset \neq L \neq H$, 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 функций $F = \{f_1, f_2, \dots, f_n\}$ 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 $g_1, g_2, \dots, g_n$ суть произвольные элементы группы G, а коэффициенты перед ними суть произведения характеристических функций.

Нетрудно видеть, что полученное семейство $F = \{f_1, f_2, \dots, f_n\}$, являющееся правильным в силу леммы, имеет полный граф существенной зависимости G_F.

Таким образом, для любого фиксированного числа переменных доля функций, для которых правильность семейств равносильна отсутствию циклов в графах существенной зависимости, стремится к 1 с ростом порядка группы. С другой стороны, приведено простое достаточное условие построения правильных семейств функций, графы которых имеют богатую цикловую структуру.

Список литературы

[1] Dénes J. and Keedwell A., *Latin Squares and their Applications*, Budapest, (1974).

[2] Носов, В. А., *О построении классов латинских квадратов в булевой базе данных*, Интеллектуальные системы, т. 4, вып. 3–4, (1999), с. 307–320.

[3] Носов, В. А., *Построение параметрического семейства латинских квадратов в векторной базе данных*, Интеллектуальные системы, т. 8, вып. 1–4, (2004), с. 517–528.

[4] Носов, В. А., Панкратьев, А. Е., *Латинские квадраты над абелевыми группами*, Фундаментальная и прикладная математика, т. 12, вып. 3, 2006, с. 65–71.

Московский государственный университет, механико-математический факультет, кафедра математической теории интеллектуальных систем

E-mail: apankrat@shade.msu.ru