Секция «Математика и механика»

Построение параметрического семейства многомерных латинских квадратов над абелевыми группами

Плаксина Инесса Андреевна
Аспирант
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: inesenok@gmail.com

Латинским квадратом порядка n называют матрицу размера $n \times n$, заполненную элементами множества Ω, $|\Omega| = n$, таким образом, что в каждой из строк и каждом из столбцов ее элементы различны. Для практической применимости в сфере защиты информации требуются латинские квадраты достаточно больших размеров, что не позволяет хранить их в памяти поэлементно. Поэтому используется аналитический метод задания латинских квадратов с помощью функций, определяющих значение элемента квадрата по номеру строки и номера столбца. В данной работе обобщается конструкция параметрического семейства латинских квадратов над прямым произведением абелевых групп [2]-[4], на многомерный случай с целью увеличения количества параметров. Дается критерий реализуемости данной конструкции, использующий свойство функций, называемое правильностью [1].

Пусть G — абелева группа. Рассмотрим прямое произведение n ее копий:

$$H = G^n = \underbrace{G \times G \times \ldots \times G}_{n}.$$

Зададим над группой H латинский квадрат L следующим образом. "Проиндексируем" каждое измерение L элементами группы H. Пусть $x^1,\ x^2,\ \ldots,\ x^m$, где $x^i = (x_1^i,\ x_2^i, \ldots, x_n^i)$, $i \in \overline{1,m}$, — элементы группы H. Тогда элемент $L(x^1, x^2, \ldots, x^m) = (z_1, \ldots, z_n)$ квадрата L определим формулами:

$$\begin{aligned} z_1 &= x_1^1 + \ldots + x_1^m + f_1(p_1(x_1^1, \ldots, x_1^m), \ldots, p_n(x_n^1, \ldots, x_n^m)) \\ z_2 &= x_2^1 + \ldots + x_2^m + f_2(p_1(x_1^1, \ldots, x_1^m), \ldots, p_n(x_n^1, \ldots, x_n^m)) \\ &\vdots \\ z_n &= x_n^1 + \ldots + x_n^m + f_n(p_1(x_1^1, \ldots, x_1^m), \ldots, p_n(x_n^1, \ldots, x_n^m)), \end{aligned} \tag{1}$$

где $p_1, p_2, \ldots, p_n$ - функции из G^m в G, $f_1, f_2, \ldots, f_n$ - функции из G^n в G.

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

Как следствие теоремы 1, общее число латинских квадратов размерности 2, которые можно получить при помощи любого правильного семейства функций $f_1, f_2, \ldots, f_n$, составляет $\frac{1}{2}m(m-1)|G|^{2n+n|G|^m}$. Применение данной конструкции в шифровании позволяет увеличить число ключей при прежнем размере шифруемого текста, либо увеличить размер текста, оставив неизменным число ключей.

Также в работе рассматривается вопрос о связи правильности и циклов в графе существенной зависимости, исследуемый ранее в [2], [3], [5], и получен следующий результат для функций над кольцами вычетов.

Теорема 2 Пусть семейство функций $f = f_1, \ldots, f_n$ вида $f_i = \prod_{j=1}^{k} \left(\sum_{i=1}^{n} S_i(x) \right)$, где $S_i(x)$ — биективны, правильно. Тогда для любого простого элементарного цикла C в графе существенной зависимости G_f выполнено

$$\prod_{i \in C} f_i(x_1, \ldots, x_n) \equiv 0.$$

Литература

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

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, №3. 2006. С. 65-71.

5. Носов В.А., Панкратьев А.Е. О функциональном задании латинских квадратов // Интеллектуальные системы. Т.12, вып. 1-4. 2008. С. 317-332.

Слова благодарности

Автор выражает благодарность своему научному руководителю к.ф.-м.н. Носову В.А. за участие в обсуждении работы.