Построение латинских квадратов в булевской параметризации

Д. В. Алашкевич

Латинские квадраты исследуются очень давно и нашли применение в различных областях математики и защиты информации. Согласно Шеннону, они представляют собой так называемый совершенный шифр.

Возникает задача построениях классов латинских квадратов сколь угодно больших размеров. В данной работе изучаются конструкции, позволяющие строить параметрические классы латинских квадратов в булевской параметризации.

В работе [1] был предложен способ построения параметрических классов латинских квадратов размера $2^n \times 2^n$ над множеством булевских векторов длины n. Данная конструкция реализуется с использованием семейств булевых функций, обладающих свойством *правильности*.

Определение. Семейство булевых функций $(f_1, \ldots, f_n)$, где $f_i = f_i(x_1, \ldots, x_n)$, обладает свойством *правильности* (или является *правильным*), если выполнены следующие условия:

$$\begin{array}{c}\text{Для любых наборов } (x'_1, \ldots, x'_n) \neq (x''_1, \ldots, x''_n) \text{ существует} \\ \alpha \in \overline{1,n}, \text{ такое, что } x'_\alpha \neq x''_\alpha,\ f_\alpha(x'_1, \ldots, x'_n) = f_\alpha(x''_1, \ldots, x''_n).\end{array} \tag{1}$$

Известны классы правильных семейств булевых функций. Однако нет эффективных алгоритмов для проверки этого свойства.

Удалось установить, что для некоторых семейств функций свойства правильности и регулярности (биективности) взаимосвязаны. Получены следующие результаты:

1°. Для систем булевых функций вида

$$\begin{cases} f_1 = x_1 + x_2^{\alpha_1} \cdots x_{k+1}^{\alpha_k} \\ f_2 = x_2 + x_3^{\alpha_1} \cdots x_{k+2}^{\alpha_k} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ f_n = x_n + x_1^{\alpha_1} \cdots x_k^{\alpha_k} \end{cases} \tag{2}$$

и

$$\begin{cases} \Delta_1 = x_2^{\alpha_1} \cdots x_{k+1}^{\alpha_k} \\ \Delta_2 = x_3^{\alpha_1} \cdots x_{k+2}^{\alpha_k} \\ \cdots\cdots\cdots\cdots\cdots \\ \Delta_n = x_1^{\alpha_1} \cdots x_k^{\alpha_k}, \end{cases} \tag{3}$$

где $2 \leqslant k \leqslant n-1$, $(\alpha_1, \ldots, \alpha_k) \in \{0,1\}^k$ доказана

Теорема 1. *Семейство булевых функций $(f_1, \ldots, f_n)$ является регулярным тогда и только тогда, когда семейство булевых функций $(\Delta_1, \ldots, \Delta_n)$ является правильным.*

Найдены достаточные условия, когда семейство (3) является правильным. Отдельно разобран случай $k = n-1$. Получен критерий и подсчитано количество удовлетворящих наборов $(\alpha_1, \cdots, \alpha_k)$.

Для семейств булевых функций из известных классов исследован вопрос правильности.

2°. Исследован вопрос задания латинских квадратов семействами булевых функций. Для «треугольных» семейств булевых функций получен критерий. Найдены необходимые и достаточные условия для того, чтобы семейства линейных функций задавали латинский квадрат. Исследован вопрос ортогональности двух латинских квадратов, заданных семействами линейных функций. Приведена конструкция, позволяющая строить тройки попарно ортогональных латинских квадратов.

Таким образом, в работе построены различные конструкции параметрических классов латинских квадратов в булевской параметризации.

Автор выражает признательность своему научному руководителю к.ф.-м.н. Носову В. А. за постановку задачи, участие в обсуждении работы и конструктивные замечания.

Список литературы

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

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

[3] Алашкевич Д. В. Построение латинских квадратов в булевской параметризации. *Дипломная работа.* 2004.