

# Построение латинских квадратов в булевой 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 построения классов латинских квадратов сколь угодно больших размеров. В данной работе изучаются конструкции, позволяющие строить параметрические классы латинских квадратов в булевой 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  $(f_1, \dots, f_n)$ , где  $f_i = f_i(x_1, \dots, x_n)$ , обладает свойством *правильности* (или является *правильным*), если выполнены следующие условия:

$$\text{Для любых наборов } (x'_1, \dots, x'_n) \neq (x''_1, \dots, x''_n) \text{ существует } \alpha \in \overline{1, n}, \text{ такое, что } x'_\alpha \neq x''_\alpha, f_\alpha(x'_1, \dots, x'_n) = f_\alpha(x''_1, \dots, x''_n). \quad (1)$$

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:



## Список литературы

- [1] Носов В. А. О построении латинских квадратов в булевой 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 булевой параметризации. *Дипломная работа*. 2004.

