Секция «Дискретная математика и математическая кибернетика»

Классификация правильных семейств функций малых размерностей

Плаксина Инесса Андреевна

Аспирант

Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории
интеллектуальных систем, Москва, Россия

E-mail: inesenok@gmail.com

Развитие и внедрение новых информационных технологий во всех сферах человеческой деятельности приводит к тому, что защита информации становится все более актуальной и сложной проблемой. В связи с этим появляется необходимость в использовании шифров, которые бы удовлетворяли современным требованиям безопасности. В работе [5] введено понятие шифров совершенной секретности, которые могут быть построены с помощью латинских квадратов. В работе [1] приводится способ задания латинских квадратов с помощью семейств функций, обладающих свойством правильности. Семейство функций $f = (f_1, \dots, f_n)$ от переменных $x_1, \dots, x_n$ называется *правильным*, если для любых двух различных наборов переменных $x' = (x'_1, \dots, x'_n)$, $x'' = (x''_1, \dots, x''_n)$ существует такое $i \in \{1, \dots, n\}$, что выполняются условия $x'_i \neq x''_i$, $f_i(x') = f_i(x'')$. Важную роль при изучении правильных семейств функций играют графы существенной зависимости. *Графом существенной зависимости* семейства функций $f = (f_1, \dots, f_n)$ от переменных $x_1, \dots, x_n$ называется $G_f = (V, E)$, где $V = 1, 2, \dots, n$, а ребро $(i, j) \in E$ тогда и только тогда, когда f_j зависит от x_i существенно. В работах [2]-[4] был рассмотрен вопрос о влиянии циклов графа G_f семейства функций на правильность этого семейства для булевых функций, функций p-значной логики и функций над абелевыми группами. В данной работе продолжается исследование правильных семейств функций с использованием информации о графе существенной зависимости. Перечислены все графы для $n = 4$ с точностью до изоморфизма, которые являются графами существенной зависимости для некоторых правильных семейств. Приведена классификация правильных семейств функций для $n = 4$ с учетом информации о цикловой структуре соответствующих им графов существенной зависимости.

Источники и литература

1) Носов В.А. О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. Т.4, вып. 3-4. 1999. С . 307-320.

2) Носов В.А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. Т.8, вып. 1-4. 2004. С. 517-528.

3) Носов В.А. , Панкратьев А.Е. Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. Т. 12, ќ3. 2006. С. 65-71.

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

5) Shannon C. Communication Theory of Secrecy Systems // Bell System Techn. J.28, №4.1949. P.656-715.

Слова благодарности

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