Секция «Математика и механика»

О правильных семействах функций, используемых для задания латинских квадратов

Рыков Дмитрий Олегович
Аспирант
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: dorykov@gmail.com

В современном мире проблемы защиты информации становятся все более актуальными. Появляются новые методы криптографического анализа, компьютеры с каждым годом становятся все более мощными. В этой связи появляется необходимость в использовании шифров совершенной секретности, которые могут быть реализованы с помощью латинских квадратов (см. [6]). Латинский квадрат представляет собой таблицу Кэли (таблицу умножения) квазигруппы, алгебраической системы с бинарной операцией, в которой допускается деление (квазигруппа является некоторым обобщением группы). В работе [2] приводится способ построения параметрического семейства латинских квадратов с помощью семейства булевых функций, обладающего свойством правильности. Семейство функций $f = (f_1, f_2, \ldots, f_n)$ от переменных $x_1, x_2, \ldots, x_n$ называется правильным, если для любых двух различных наборов значений переменных $x' = (x'_1, x'_2, \ldots, x'_n)$ и $x'' = (x''_1, x''_2, \ldots, x''_n)$ существует $\alpha \in \overline{1,n}$ такое, что выполнено

$$x'_\alpha \neq x''_\alpha, \quad f_\alpha(x') = f_\alpha(x'').$$

Понятие правильности семейства функций впервые возникло в работе [1] в связи с вопросом о регулярности некоторого булевского автомата. Возможность построения обширного класса латинских квадратов, заданного параметрически, с помощью правильных семейств делает актуальным изучение свойств, способов построения и распознавания правильных семейств. Этому посвящены работы [1,2,3,4], а также работа автора [5]. В работе [1] предложен критерий правильности семейства булевых функций, сводящий проверку правильности семейства $f = (f_1, f_2, \ldots, f_n)$ к проверке наличия в полиномах Жегалкина произведений функций вида $\prod\limits_{i\in I} f_i$ членов, содержащих $\prod\limits_{i\in I} x_i$, где $I \subset [1,n]$. В работе [2] введено понятие графа существенной зависимости семейства функций и доказан критерий правильности для семейств мультиаффинных функций: семейство мультиаффинных функций $f = (f_1, f_2, \ldots, f_n)$ правильно тогда и только тогда,когда $\forall C$ – простого элементарного цикла графа существенной зависимости $\prod\limits_{i\in C} f_i \equiv 0$. Также показано, что семейство линейных функций может быть правильным только в случае отсутсвия циклов в графе существенной зависимости, а также что любое семейство функций с ацикличным графом существенной зависимости - правильное. Таким образом, было замечено, что структура графа существенной зависимости (в описанных выше случаях - именно цикловая структура) имеет большое значение для свойства правильности. В работах [3,4] предыдущие результаты были во многом обобщены на случаи p-значной логики (p-простое число). Имеющиеся результаты о связи правильности с цикловой структурой графа существенной зависимости в

случае функций определенных классов навели на идею использования структуры этого графа в случае произвольных функций. В работе автора [5] эта идея была реализована. Показано, что граф существенной зависимости может быть использован для проверки правильности в случае произвольных булевых функций, а именно, проверка правильности сводится к проверке правильности семейств функций, возникающих на сильных компонентах этого графа. Тем не менее, если граф не допускает разложения на сильные компоненты, добиться снижения сложности проверки правильности по сравнению с прямым перебором этим методом не удается. В той же работе приводится алгоритм проверки правильности семейства булевых монотонных функций, который позволяет существенно снизить время, необходимое для проверки правильности, по сравнению с прямым перебором.

Все известные до сих пор способы проверки правильности либо недостаточно эффективны (например, в случае, если граф не допускает разложение на сильные компоненты), либо применимы для ограниченного класса функций. Цель данной работы - использовать структуру графа существенной зависимости для построения еще более эффективного способа проверки правильности для случая произвольных функций.

В работе показано, что в случае, когда граф допускает разложение на сильные компоненты и, в дальнейшем, на блоки, проверка правильности сводится к проверке правильности семейств, возникающих на этих компонентах и блоках компонент. Также решается задача упрощения правильного семейства в случае, если граф семейства содержит некоторый "тривиальный"путь - в этом случае все внутренние точки пути можно заменить на одну. При этом изменении семейства и его графа функция, соответствующая новой точке, наследует функцию одной из точек графа и свойство правильности семейства не меняется. Полученные в данной работе результаты справедливы для правильных семейств функций k-значной логики, где $k \geq 2$. Таким образом, результат работы автора [5] был обобщен и улучшен.

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. О функциональном задании латинских квадратов // Интеллектуальные системы. Т.12, вып. 1-4. 2008. С. 317-332.

5. Рыков Д.О. Об алгоритмах проверки правильности семейств функций // Интеллектуальные системы. Т.14, вып. 1-4. 2010. С. 261-276.

6. Shannon C. Communication Theory of Secrecy Systems // Bell System Techn. J. 28, № 4. 1949. P. 656-715

Слова благодарности

Автор выражает благодарность Носову В.А. за научное руководство и постановку задачи.