Секция «Математическая логика, алгебра и теория чисел»

О взаимно-однозначном соответствии между правильными семействами булевых функций и реберных ориентаций с единственным стоком на булевых кубах.

Научный руководитель – Панкратьев Антон Евгеньевич

Царегородцев Кирилл Денисович

Аспирант

Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра высшей алгебры, Москва, Россия
E-mail: kirill94_12@mail.ru

Правильным семейством булевых функций [2] называется упорядоченный набор булевых функций $(f_1, \ldots, f_n)$ от переменных $x_1, \ldots, x_n$, такой что для любых двух различных двоичных наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$ найдется индекс i со свойством $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$. Правильные семейства были введены в [2] и изучались в [1, 3] применительно к построению параметрических семейств латинских квадратов для синтеза поточных шифров.

Ориентация рёбер булева куба $\mathbb{B}^n$ называется ориентацией с единственным стоком (unique sink orientation) [5, 6], если каждый подкуб в $\mathbb{B}^n$ имеет единственный сток.

С помощью семейства булевых функций $(f_1, \ldots, f_n)$ можно задавать ориентации на рёбрах булева куба, а именно: для каждой точки $\alpha \in \mathbb{B}^n$ рассмотрим её соседа $\alpha' \in \mathbb{B}^n$, где α' отличается от α только в i-той компоненте. Зададим ориентацию ребра $\alpha\alpha'$: если $f_i(\alpha') = \alpha_i$, то направим ребро от α' к α, иначе от α к α'. Если каждая из функций f_i не зависит существенно от x_i, то каждое ребро будет ориентировано единственным образом.

Оказывается, что при таком отображении правильным семействам $(f_1, \ldots, f_n)$ взаимно-однозначно соответствуют реберные ориентации кубов с единственным стоком. Данное свойство связано с неподвижными точками отображения $(x_1, \ldots, x_n) \to (f_1(x), \ldots, f_n(x))$ и позволяет получить дополнительные свойства для правильных семейств, в частности получить оценки на число правильных семейств длины $n \geq 5$ и показать, что задача распознавания правильности семейства является coNP-полной [4].

Источники и литература

1) Козлов А. А., Носов В. А., Панкратьев А. Е. Матрицы и графы существенной зависимости правильных семейств функций // Фундаментальная и прикладная математика. — 2008. — Т. 14, № 4. — С. 137–149.

2) Носов В. А. Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. Теория и приложения (ранее: Интеллектуальные системы по 2014, № 2, ISSN 2075-9460). — 1999. — Т. 4, № 3-4. — С. 307–320.

3) Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. — 2006. — Т. 12, № 3. — С. 65–71.

4) Gärtner, Bernd & Thomas, Antonis. (2015). The Complexity of Recognizing Unique Sink Orientations. Leibniz International Proceedings in Informatics, LIPIcs. 30. 10.4230/LIPIcs.STACS.2015.341.

5) Ingo A. Schurr. Unique sink orientations of cubes. PhD thesis, ETH Zurich,2004.

6) Szabó, Tibor; Welzl, Emo (2001), "Unique sink orientations of cubes", 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), IEEE Computer Soc., Los Alamitos, CA, pp. 547–555