О соответствии между правильными семействами и реберными ориентациями булевых кубов

Царегородцев К.Д.[1]

В работе рассматривается соответствие между правильными семействами булевых функций и реберными ориентациями с единственным стоком на булевых кубах. Данное соответствие позволяет перенести часть результатов, полученных для указанных ориентаций, на язык правильных семейств: получить оценки на число правильных семейств порядка $n \geq 5$ и показать, что задача распознавания правильности семейства является coNP-полной.

Ключевые слова: правильные семейства булевых функций, реберные ориентации с единственным стоком.

1. Введение

Настоящая работа посвящена изучению соответствия между правильными семействами булевых функций и реберными ориентациями с единственным стоком на булевых кубах. Правильные семейства функций применяются при построении больших латинских квадратов, которые используются в различных областях математики и кибернетики: теории кодирования, планировании эксперимента, защите информации [1, 2]. В работах [3, 4] был предложен функциональный метод задания латинского квадрата при помощи семейства булевых функций.

Реберные ориентации с единственным стоком изучались в работах [5, 6] в связи с задачами линейного и квадратичного программирования. По правильному семейству можно задать ориентацию ребер на булевом кубе таким образом, что полученный объект будет реберной ориентацией

[1] *Царегородцев Кирилл Денисович* — аспирант каф. алгебры мех.-мат. ф-та МГУ имени М.В.Ломоносова, e-mail: kirill94_12@mail.ru.

Tsaregorodtsev Kirill Denisovich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Algebra.

с единственным стоком, и наоборот, каждой такой ориентации можно сопоставить некоторое правильное семейство.

2. Предварительные сведения

Наделим булев куб E_2^n размерности n структурой графа, соединив (неориентированными) ребрами пары точек, находящихся на расстоянии Хэмминга 1. Вершинам сопоставим метки $(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \{0, 1\}$. Будем называть такой граф графом булева куба.

Подкубом размерности $n - m$ будем называть подграф графа булева куба E_2^n, индуцированный вершинами, имеющими фиксированные значения некоторых координат $i_1, \ldots, i_m \in \{1, \ldots, n\}$.

Реберной ориентацией с единственным стоком на графе булева куба E_2^n называется такая ориентация всех его ребер, что в каждом подкубе размерности $d = 1, 2, \ldots, n$ существует ровно 1 сток. Для краткости будем в дальнейшем называть такие ориентации одностоковыми.

Следуя работам [3, 4, 7], введем понятие правильности семейства булевых функций.

Семейство булевых функций

$$F = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$

называется правильным, если для любых двух двоичных наборов α, β, $\alpha \neq \beta$, выполняется следующее условие:

$$\exists i : \alpha_i \neq \beta_i, \;\; f_i(\alpha) = f_i(\beta)$$

О способах построения латинских квадратов по правильным семействам можно прочитать в работе [3].

Семейству функций $F = (f_1, \ldots, f_n)$ от n переменных с тем свойством, что f_i не зависит от x_i, $i = 1, \ldots, n$, сопоставим реберную ориентацию на графе n-мерного булева куба следующих образом. Пусть (v, w) — смежные вершины в E_2^n, $v_i \neq w_i$. По свойству семейства F имеем $f_i(v) = f_i(w)$. Если $f_i(v) = v_i$, то ребро ориентируется от w к v, в противном случае $(f_i(v) = w_i)$ ребро ориентируется от v к w. Построенный таким образом по семейству F граф обозначим за G_F.

Вершина v является стоком в данной ориентации тогда и только тогда, когда v — неподвижная точка отображения $f : E_2^n \to E_2^n$, задаваемого семейством F.

3. Связь между одностоковыми ориентациями и правильными семействами

Для правильных семейств верны следующие два утверждения, которые представляют самостоятельный интерес и играют ключевую роль в доказательстве основного результата (теорема 3).

Теорема 1. *Пусть $F = (f_1, \ldots, f_n)$ — правильное семейство булевых функций. Рассмотрим ограничение семейства F на подкуб E_2^n вида $x_{i_1} = a_1, \ldots, x_{i_m} = a_m$. Исключим из семейства F функции с номерами $i_1, \ldots, i_m$ и подставим в оставшиеся функции константы $a_1, \ldots, a_m$ вместо соответствующих переменных $x_{i_1}, \ldots, x_{i_m}$. Тогда полученное семейство функций также будет правильным.*

Теорема 2. *У отображения $E_2^n \to E_2^n$, задаваемого правильным семейством, всегда существует единственная неподвижная точка.*

Данные утверждения позволяют доказать основное утверждение про взаимосвязь правильных семейств и одностоковых ориентаций.

Теорема 3. *Граф G_F семейства $F = (f_1, \ldots, f_n)$, является одностоковой ориентацией на графе булева куба E_2^n тогда и только тогда, когда F — правильное семейство.*

Данное соответствие позволяет перенести часть результатов из теории, развитой в работах [6, 8, 9], на правильные семейства. В частности, верны следующие утверждения:

Следствие 1 ([8], [10])**.** *Пусть семейство булевых функций задано в виде конъюнктивной нормальной формы. Тогда задача распознавания правильности семейства является $coNP$-полной.*

Обозначим за $T(n)$ количество правильных семейств порядка n.

Следствие 2 ([6])**.** $T(n) \geq 4(T(n-1))^2$

Следствие 3 ([9])**.** *Существуют константы $B \geq A > 0$, такие что для $n \geq 2$ выполняются неравенства:*

$$n^{A \cdot 2^n} \leq T(n) \leq n^{B \cdot 2^n}$$

Автор выражает признательность своему научному руководителю А. Е. Панкратьеву и с.н.с. А. В. Галатенко за оказанную помощь при написании настоящей статьи.

Список литературы

[1] Keedwell, D., and Dénes, J., *Latin Squares and their Applications, 2nd Edition*, North Holland, 2015, 438 pp.

[2] Глухов, М. М., “О применениях квазигрупп в криптографии”, *ПДМ*, 2008, 28–32.

[3] 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)*, **4**:3–4 (1999), 307–320.

[4] Носов, В. А., “Построение параметрического семейства латинских квадратов в векторной базе данных”, *Интеллектуальные системы. Теория и приложения (ранее: Интеллектуальные системы по 2014, № 2, ISSN 2075-9460)*, **8** (2006), 517–529.

[5] Szabo, T., and Welzl, E., “Unique Sink Orientations of Cubes”, *Proceedings of the 42nd IEEE Symposiumon Foundations of Computer Science (FOCS)*, 2001, 547–555.

[6] Schurr, I. A., *Unique sink orientations of cubes*, ETH Zurich, 2004.

[7] Носов, В. А., Панкратьев, А. Е., “О функциональном задании латинских квадратов”, *Фундамент. и прикл. матем.*, **15**:4 (2009), 177–187.

[8] Gärtner, B. and Thomas, A., “The Complexity of Recognizing Unique Sink Orientations”, *Leibniz International Proceedings in Informatics, LIPIcs*, **30** (2015).

[9] Matoušek, J., “The Number Of Unique-Sink Orientations of the Hypercube”, *Combinatorica*, **26** (2006), 91–99.

[10] Носов, В. А., “Критерий регулярности булевского неавтономного автомата с разделенным входом”, **3** (1998), 269–280.

On the relationship between proper families and edge orientations of Boolean cubes

Tsaregorodtsev K.D.

This paper is devoted to the study of relationship between proper families of Boolean functions and unique sink orientations of cubes. A one-to-one correspondence between these two objects is established, a number of properties are carried over from unique sink orientations to proper families. These results include an upper bound for the number of proper families of given size and coNP-completeness of the problem of recognizing properness.

Keywords: proper families of Boolean functions, unique sink orientations.