

УДК 519.1+512.5

О ВЗАИМНО ОДНОЗНАЧНОМ СООТВЕТСТВИИ МЕЖДУ ПРАВИЛЬНЫМИ СЕМЕЙСТВАМИ БУЛЕВЫХ ФУНКЦИЙ И РЁБЕРНЫМИ ОРИЕНТАЦИЯМИ БУЛЕВЫХ КУБОВ

К. Д. Царегородцев

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

Доказывается факт взаимно однозначного соответствия между правильными семействами булевых функций и рёберными 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 длины $n \geq 5$ и показать, что задача распознавания правильности семейства является coNP-полной.

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

DOI 10.17223/20710410/48/2

ONE-TO-ONE CORRESPONDENCE BETWEEN PROPER FAMILIES OF BOOLEAN FUNCTIONS AND UNIQUE SINK ORIENTATIONS OF CUBES

K. D. Tsaregorodtsev

*Moscow State University, Moscow, Russia***E-mail:** kirill94_12@mail.ru

In the paper, we study the relationship between proper families of Boolean functions and unique sink orientations of Boolean cubes. A family of Boolean functions $F = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ is called proper if for every two binary vectors α, β , $\alpha \neq \beta$, the following condition holds:

$$\exists i (\alpha_i \neq \beta_i \ \& \ f_i(\alpha) = f_i(\beta)).$$

Unique sink orientation of Boolean cube $\mathbb{E}_n$ is such an orientation of edges of $\mathbb{E}_n$ that any subcube of $\mathbb{E}_n$ has a unique sink, i.e., a unique vertex without outgoing edges. The existence of one-to-one correspondence between two classes of objects is proved, and various properties are derived for proper families. The following boundary for the number $T(n)$ of proper families of given size n is obtained: there exist two numbers B and A , $B \geq A > 0$, such that $n^{A2^n} \leq T(n) \leq n^{B2^n}$ for $n \geq 2$. Also, coNP-completeness of the problem of recognizing properness is derived.

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

Введение

Работа посвящена изучению соответствия между правильными семействами булевых функций и рёберными ориентациями с единственным стоком на графах булевых кубов. Правильные семейства функций применяются при построении латинских

квадратов, которые используются в различных областях математики и кибернетики: теории кодирования, планировании эксперимента, криптографии [1, 2]. Применяемые в области защиты информации латинские квадраты имеют достаточно большие размеры, что делает затруднительным поэлементное хранение в памяти компьютера всего квадрата целиком. Из этих соображений в работах [3, 4] предложен метод задания латинского квадрата при помощи семейства булевых функций, которое определяет элемент квадрата по его координатам (номеру строки и столбца).

Рёберные ориентации с единственным стоком изучаются в работах [5, 6] в связи с задачами линейного и квадратичного программирования. Оказывается, что по правильному семейству можно задать ориентацию рёбер на графе булева куба таким образом, что полученный объект будет рёберной ориентацией с единственным стоком, и наоборот, каждая такая ориентация задаёт некоторое правильное семейство. Доказательство этого факта, а также некоторые следствия для правильных семейств приведены в данной работе.

1. Предварительные сведения

1.1. Графы булева куба и одностокковые ориентации

Определение 1. Графом булева куба $\mathbb{E}_n$ размерности n будем называть граф на 2^n вершинах с метками $(\alpha_1, \dots, \alpha_n)$, $\alpha_i \in \{0, 1\}$, где рёбра проведены между вершинами, расстояние Хэмминга между которыми равно 1.

Определение 2. Подкубом булева куба размерности $(n-m)$ будем называть подграф, порождённый вершинами с фиксированными значениями некоторых координат $i_1, \dots, i_m \in \{1, \dots, n\}$.

В частности, подкубами размерности 1 являются рёбра графа $\mathbb{E}_n$, подкубами размерности 2 — его двумерные грани куба и так далее.

Определение 3. Стоком в ориентированном графе будем называть вершину, в которую входят и из которой не исходят рёбра.

Определение 4. Рёберной ориентацией с единственным стоком на графе булева куба $\mathbb{E}_n$ называется ориентация всех рёбер графа $\mathbb{E}_n$ с тем свойством, что в каждом подкубе размерностей $d = 1, 2, \dots, n$ существует ровно один сток.

Для краткости будем в дальнейшем называть такие ориентации одностокковыми. Примеры одностокковых ориентаций кубов приведены на рис. 1.

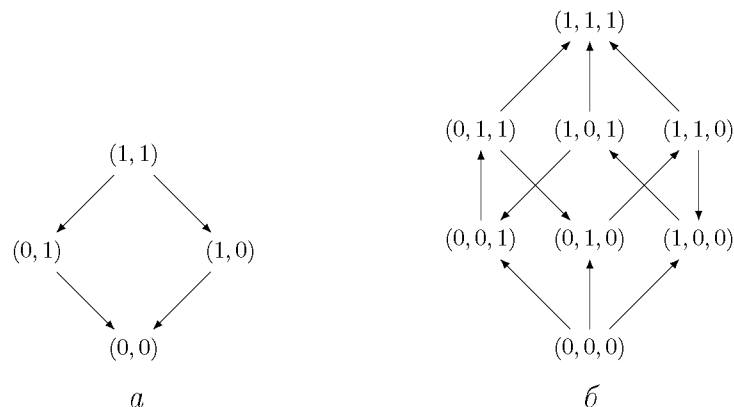


Рис. 1. Одностокковая ориентация двумерного (*a*) и трёхмерного (*б*) кубов

1.2. Правильное семейство булевых функций

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

Определение 5. Семейство булевых функций

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

называется правильным, если для любых двух двоичных наборов $\alpha = \alpha_1 \dots \alpha_n$, $\beta = \beta_1 \dots \beta_n$, $\alpha \neq \beta$, выполняется следующее условие:

$$\exists i (\alpha_i \neq \beta_i \ \& \ f_i(\alpha) = f_i(\beta)).$$

Правильные семейства используются для построения латинских квадратов, а именно верна

Теорема 1 [3]. Пусть $x, y \in \{0, 1\}^n$, $F = (f_1, \dots, f_n)$ — семейство булевых функций. Рассмотрим следующую операцию на множестве $\{0, 1\}^n$:

$$\begin{aligned} x \circ y &= x \oplus y \oplus f^\pi(x, y), \\ f^\pi(x, y) &= (f_1(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)), \dots, f_n(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))); \\ \pi_i : \{0, 1\}^2 &\rightarrow \{0, 1\}, \ i = 1, \dots, n, \text{ — произвольные булевы функции.} \end{aligned}$$

Тогда операция $\circ : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ задаёт структуру квазигруппы на $\{0, 1\}^n$ для любых функций π_i тогда и только тогда, когда F — правильное семейство. Таблица Кэли полученной квазигруппы является латинским квадратом.

2. Связь между одностокowymi ориентациями $\mathbb{E}_n$ и правильными семействами

Определение 6. Для заданного семейства булевых функций

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

размера n , где функция f_i не зависит существенно от x_i , $i = 1, \dots, n$, введём следующий граф семейства Γ_F .

Вершинами графа являются все двоичные наборы длины n . Рёбра проводятся между вершинами, расстояние Хэмминга между которыми равно 1. Ориентация ребра задается следующим образом: пусть (v, w) — смежные вершины в $\mathbb{E}_n$, различающиеся в i -м бите. Рассмотрим значения функции f_i на этих двух наборах. Поскольку она не зависит существенно от x_i , то $f_i(v) = f_i(w)$. Если $f_i(v) = v_i$, то ребро ориентируется от w к v , в противном случае ($f_i(v) = w_i$) — от v к w .

Замечание 1. Соответствие между семействами $F = (f_1, \dots, f_n)$ булевых функций (где f_i не зависит существенно от x_i) и ориентированными графами булевых кубов $\mathbb{E}_n$ является взаимно однозначным:

- 1) по семейству однозначно задаётся (указанным способом) ориентация на графе булева куба;
- 2) по ориентированному графу булева куба $\mathbb{E}_n$ можно восстановить значения всех функций семейства на любом $x \in \mathbb{E}_n$: рассмотрим вершину с меткой x и все смежные с ней рёбра. Если ребро, ведущее из вершины x в вершину, отличную от x в i -й координате, выходит из x , то $f_i(x) = \overline{x_i}$, иначе $f_i(x) = x_i$. В полученном семействе f_i не зависит существенно от x_i , поскольку ни одно ребро не ориентировано в две стороны.

Замечание 2. Нетрудно заметить, что вершина v является стоком в данной ориентации тогда и только тогда, когда v — неподвижная точка отображения $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$. Действительно, $F(v) = v$ тогда и только тогда, когда $f_i(v) = v_i$ для каждого $i = 1, \dots, n$, что, в свою очередь, равносильно тому, что v является стоком в данной ориентации.

Докажем два вспомогательных утверждения.

Лемма 1. Рассмотрим ограничение правильного семейства $F = (f_1, \dots, f_n)$ на подкуб графа $\mathbb{E}_n$: зафиксируем позиции $x_{i_1} = a_1, \dots, x_{i_m} = a_m$, $a_i \in \{0, 1\}^n$, и рассмотрим подкуб, порождённый фиксацией данных координат:

$$(x_1, \dots, x_{i_1-1}, a_1, x_{i_1+1}, \dots, x_{i_m-1}, a_m, x_{i_m+1}, \dots, x_n).$$

Исключим из правильного семейства $(f_1, \dots, f_n)$ функции с номерами $i_1, \dots, i_m$ и поставим в оставшихся функциях константы $a_1, \dots, a_m$ вместо соответствующих переменных $x_{i_1}, \dots, x_{i_m}$. Полученное семейство функций также является правильным.

Доказательство. Следует из определения правильности семейства: рассмотрим два произвольных набора $(\alpha_1, \dots, \alpha_n)$ и $(\beta_1, \dots, \beta_n)$, где $\alpha \neq \beta$, $\alpha_{i_k} = a_k = \beta_{i_k}$. По определению правильности существует индекс j , такой, что $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$. Из первого условия следует, что $j \notin \{i_1, \dots, i_m\}$. Следовательно, ограничение семейства F на подкуб удовлетворяет условию правильности. ■

Лемма 2. У правильного семейства всегда существует единственная неподвижная точка.

Доказательство. Индукция по размеру правильного семейства.

По определению семейство размера $n = 1$ — это константа $a_1 \in \{0, 1\}$. У такого семейства, очевидно, имеется единственная неподвижная точка a_1 .

Рассмотрим семейство $F = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ размера n и его ограничения на подкубы, задаваемые фиксацией координат $x_n = 0$ и $x_n = 1$.

По предположению индукции для ограничений семейств в каждом подкубе существует единственная неподвижная точка $\alpha = (\alpha_1, \dots, \alpha_{n-1}, 0)$ и $\beta = (\beta_1, \dots, \beta_{n-1}, 1)$ соответственно, то есть $f_1(\alpha) = \alpha_1, \dots, f_{n-1}(\alpha) = \alpha_{n-1}$, $f_1(\beta) = \beta_1, \dots, f_{n-1}(\beta) = \beta_{n-1}$. Рассмотрим $f_n(\alpha)$ и $f_n(\beta)$. Так как семейство $F = (f_1, \dots, f_n)$ — правильное, то найдётся индекс $j \in \{1, \dots, n\}$, такой, что $\alpha_j \neq \beta_j$, $f_j(\alpha) = f_j(\beta)$. Из приведённых рассуждений видно, что единственный случай, когда данное условие может быть выполнено, — это $j = n$. В таком случае, если $f_j(\alpha) = 0$, то единственной неподвижной точкой является α , иначе — β . ■

Докажем основное утверждение.

Теорема 2. Граф семейства Γ_F является одностокковой ориентацией $\mathbb{E}_n$ тогда и только тогда, когда f — правильное семейство.

Доказательство. Как отмечено в замечании 2, стоки в графе Γ_F соответствуют неподвижным точкам ограничения отображения F на соответствующий подкуб куба $\mathbb{E}_n$.

Д о с т а т о ч н о с т ь. Пусть F — правильное семейство. Тогда по лемме 1 любое ограничение семейства F на любой подкуб $\mathbb{E}_n$ также является правильным. По лемме 2 такое ограничение имеет единственную неподвижную точку в данном подкубе, т.е. данный подкуб имеет единственный сток. Следовательно, граф Γ_F для правильного семейства F является одностокковой ориентацией.

Необходимость. Пусть Γ_F — одностоковая ориентация. Покажем индукцией по размеру F , что в таком случае F является правильным семейством.

База: $n = 1$. Нетрудно убедиться, что существует ровно две одностоковые ориентации на двух вершинах, соответствующих семействам $\{f = (0)\}$, $\{f = (1)\}$.

Индуктивный переход: пусть $\alpha \neq \beta$. По определению правильного семейства нужно показать, что тогда существует индекс i , такой, что $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$.

Если найдётся индекс k , такой, что $\alpha_k = \beta_k$, то задача может быть сведена к задаче меньшей размерности: рассматриваем ограничение на подкуб $x_k = \alpha_k$ и используем индуктивное предположение.

Пусть $\alpha_k \neq \beta_k$, $k = 1, \dots, n$. Будем считать, что α — сток, то есть $f_k(\alpha) = \alpha_k$, $k = 1, \dots, n$. Если это не так, то перейдём к новому семейству $g_k = f_k \oplus 1$, таким образом изменив направление всех рёбер между подкубами для $x_k = 0$ и $x_k = 1$. Данная смена направлений рёбер не разрушает свойство ориентации быть одностоковой. Нетрудно убедиться, что $F = (f_1, \dots, f_n)$ является правильным семейством тогда и только тогда, когда $F \oplus \alpha = (f_1 \oplus \alpha_1, \dots, f_n \oplus \alpha_n)$ является правильным для любого фиксированного набора $\alpha \in \{0, 1\}^n$. Таким образом, можно без ограничения общности считать, что вершина α является стоком. Но в таком случае если $f_k(\alpha) \neq f_k(\beta)$, $k = 1, \dots, n$, то $f_k(\beta) = \beta_k$, $k = 1, \dots, n$, то есть вершина β также является стоком, что противоречит одностоковости. Следовательно, должен найтись какой-либо индекс k , для которого $f_k(\alpha) = f_k(\beta)$, что и требовалось доказать. ■

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

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

Обозначим через $T(n)$ количество правильных семейств размера 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 следующие неравенства:

$$n^{A2^n} \leq T(n) \leq n^{B2^n}.$$

Заключение

Каждому правильному семейству булевых функций можно поставить во взаимно однозначное соответствие ориентацию на рёбрах булева куба таким образом, что данная ориентация оказывается ориентацией с единственным стоком. Это соответствие позволяет перенести часть результатов с геометрического языка ориентаций на свойства правильных семейств.

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

ЛИТЕРАТУРА

1. *Keedwell A. and Denes J.* Latin Squares and their Applications, 2nd Ed. North Holland, 2015. 438 p.
2. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.

3. *Носов В. А.* Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. 1999. Т. 4. Вып. 3–4. С. 307–320.
4. *Носов В. А.* Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. 2006. Т. 8. Вып. 1–4. С. 517–529.
5. *Szabo T. and Welzl E.* Unique sink orientations of cubes // Proc. 42nd IEEE Symp. FOCS. Newport Beach, CA, USA, 2001. P. 547–555.
6. *Schurr I.* Unique Sink Orientations of Cubes. Doctoral Thesis. ETH Zurich, 2004.
7. *Носов В. А., Панкратьев А. Е.* О функциональном задании латинских квадратов // Интеллектуальные системы. 2008. Т. 12. Вып. 1–4. С. 317–332.
8. *Gärtner B. and Thomas A.* The complexity of recognizing unique sink orientations // Leibniz Intern. Proc. Informatics (LIPIcs). 2015. V. 30. P. 341–353.
9. *Matousek J.* The number of unique-sink orientations of the hypercube // Combinatorica. 2006. V. 26. P. 91–99.

REFERENCES

1. *Keedwell A. and Denes J.* Latin Squares and their Applications, 2nd Edition. North Holland, 2015. 438 p.
2. *Glukhov M. M.* O primeneniya kh kvazigrupp v kriptografii [Some applications of quasigroups in cryptography]. Prikladnaya Diskretnaya Matematika, 2008, no. 2(2), pp. 28–32. (in Russian)
3. *Nosov V. A.* Postroyeniye klassov latinskikh kvadratov v bulevoy baze dannykh [Constructing classes of Latin squares in the Boolean database]. Intelligent Systems, 1999, vol. 4, no. 3–4, pp. 307–320. (in Russian)
4. *Nosov V. A.* Postroyeniye parametricheskogo semeystva latinskikh kvadratov v vektornoy baze dannykh [Constructing a parametrical families of Latin squares in a vector database]. Intelligent Systems, 2006, vol. 8, no. 1–4, pp. 517–529. (in Russian)
5. *Szabo T. and Welzl E.* Unique sink orientations of cubes. Proc. 42nd IEEE Symp. FOCS, Newport Beach, CA, USA, 2001, pp. 547–555.
6. *Schurr I.* Unique Sink Orientations of Cubes. Doctoral Thesis, ETH Zurich, 2004.
7. *Nosov V. A. and Pankratyev A. E.* O funktsionalnom zadanii latinskikh kvadratov [On functional representation of Latin squares]. Intelligent Systems, 2008, vol. 12, no. 1–4, pp. 317–332. (in Russian)
8. *Gärtner B. and Thomas A.* The complexity of recognizing unique sink orientations. Leibniz Intern. Proc. Informatics (LIPIcs), 2015, vol. 30, pp. 341–353.
9. *Matousek J.* The number of unique-sink orientations of the hypercube. Combinatorica, 2006, vol. 26, pp. 91–99.