Оценка числа правильных семейств функций k-значной логики

А. В. Галатенко[1]

Правильные семейства функций являются удобным средством для задания больших параметрических классов квазигрупп и d-квазигрупп. К. Д. Царегородцевым было установлено, что в булевом случае правильные семейства находятся в естественном взаимно-однозначном соответствии с одностоковыми ориентациями булева куба. Число таких ориентаций было оценено И. Матоушеком. В работе представлено обобщение нижней оценки Матоушека на случай логики произвольной значности, некоторые следствия из этого обобщения, а также показано, что свойство правильности является редким — доля правильных семейств размера n в классе всех семейств из n n-арных функций, для которых одноименная переменная фиктивна, стремится к 0 при $n \to \infty$.

Ключевые слова: правильные семейства функций, функции k-значной логики, гиперграф, паросочетание

1. Введение

Правильные семейства булевых функций были введены В. А. Носовым в работе [1]. В работе [2] было показано, что с помощью правильных семейств булевых функций размера n можно задавать параметрические классы квазигрупп порядка 2^n. В работе [3] В. А. Носов и А. Е. Панкратьев обобщили понятие правильного семейства на случай функций k-значной логики при $k \geq 3$. И. А. Плаксина показала, что с помощью правильных семейств можно задавать не только квазигруппы, но и d-квазигруппы при $d \geq 3$ [4]. В работе [5] конструкция Плаксиной была дополнительно усилена. Обзор результатов по правильным семействам приведен в статье [6].

Обозначим через $T_k(n)$ число правильных семейств размера n в k-значной логике. Известно, что $T_2(n) \geq n^{A \cdot 2^n}$, где A — некоторая положительная вещественная константа. Этот результат был получен следующим способом. К. Д. Царегородцев установил, что между правильными семействами булевых функций размера n и так называемыми одностоковыми ориентациями n-мерного булева куба существует взаимно однозначное соответствие [7]. Таким образом, в качестве нижней оценки на число

[1] *Галатенко Алексей Владимирович* — доцент каф. МаТИС мех.-мат. ф-та МГУ, e-mail: agalat@msu.ru.

Galatenko Alexei Vladimirovich — associate professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, MaTIS chair

правильных семейств булевых функций можно использовать оценку на число одностоковых ориентаций, полученную И. Матоушеком [8]. Приведенное ниже обобщение конструкции Матоушека на k-значный случай позволяет получить нижнюю оценку $T_k(n)$ для произвольного $k \geq 3$. Затем мы покажем, что свойство правильности является редким — доля правильных семейств среди всех семейств функций, фиктивно зависящих от одноименной переменной, стремится к 0.

Дальнейшее изложение имеет следующую структуру. В разделе 2 вводятся необходимые определения. В разделе 3 представлены основные результаты работы. Раздел 4 является заключением.

2. Основные определения и обозначения

Пусть $E_k = \{0, 1, \dots, k-1\}$. Множество всех n-местных функций на E_k обозначим через P_k^n.

Определение 1. *Пусть $k, n \in \mathbb{N}$, $k \geq 2$. Семейство функций $(f_1, \dots, f_n)$, $f_i \in P_k^n$, $i = 1, \dots, n$, называется правильным, если для любых наборов $\alpha, \beta \in E_k^n$, $\alpha = (a_1, \dots, a_n)$, $\beta = (b_1, \dots, b_n)$, $\alpha \neq \beta$, найдется индекс i, $1 \leq i \leq n$, такой что $a_i \neq b_i$, но $f_i(\alpha) = f_i(\beta)$.*

Легко увидеть, что если семейство $(f_1, \dots, f_n)$ является правильным, то переменная x_i фиктивна для функции $f_i(x_1, \dots, x_n)$, $i = 1, \dots, n$.

Пример 1 ([3, пример 2]). *Пусть семейство $F = (f_1, \dots, f_n)$ таково, что переменные $x_i, \dots, x_n$ фиктивны для функции $f_i(x_1, \dots, x_n)$, $i = 1, \dots, n$. Тогда это семейство является правильным. Для доказательства правильности достаточно рассмотреть первую позицию, на которой наборы α и β отличаются. Рассмотрим произвольную перестановку $\sigma \in S_n$ и применим ее к семейству F. Результат обозначим через $G = (g_1, \dots, g_n)$, $g_i(x_1, \dots, x_n) = f_{\sigma(i)}(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. Легко увидеть, что семейство G также является правильным. Такие семейства называются треугольными.*

Пример 2 ([6, замечание 1]). *Пусть семейство $F = (f_1, \dots, f_n)$ удовлетворяет следующим условиям. Во-первых, переменная x_i фиктивна для функции $f_i(x_1, \dots, x_n)$, $i = 1, \dots, n$. Во-вторых, существует элемент $a \in E_k$, такой что для любого набора $\alpha \in E_k^n$ и любых i, j, $1 \leq i < j \leq n$, по крайней мере одно из значений $f_i(\alpha)$, $f_j(\alpha)$ равно a. Тогда семейство F правильное. Если во втором условии в качестве элемента a выбрать 0, получится аналог условия ортогональности, поэтому семейства такого вида мы будем называть обобщенно ортогональными.*

Значительное число других примеров можно найти в работе [6].

В завершение раздела приведем ряд определений из области теории графов, которые потребуются для доказательства утверждений.

Определение 2. *Гиперграфом называется пара (V, E), где V — конечное множество вершин, E — конечное множество гиперребер, элементами которого являются подмножества вершин. Если число вершин во всех гиперребрах равно одной и той же константе r, гиперграф называется r-однородным или просто однородным.*

Определение 3. *Пусть $H = (V, E)$ — некоторый гиперграф, $v \in V$ — вершина этого гиперграфа. Степенью вершины $d(v)$ называется число гиперрребер, содержащих v. Если для всех вершин степень равна одной и той же константе d, гиперграф называется d-регулярным или просто регулярным.*

Определение 4. *Паросочетанием в гиперграфе $H = (V, E)$ называется подмножество попарно непересекающихся гиперребер $M \subseteq E$.*

Пусть $H = (V, E)$ — гиперграф, $u, v \in V$, $u \neq v$. Через $d(u, v)$ обозначим число гиперребер, содержащих вершины u и v.

3. Основные результаты

Теорема 1. *Существует константа $A \in \mathbb{R}$, $A > 0$, такая что*

$$T_k(n) \geq n^{A \cdot k^n}.$$

Доказательство. Сперва построим взаимно однозначное соответствие между семействами функций $F_n = (f_1, \dots, f_n)$, где $f_i \in P_k^n$, причем переменная x_i фиктивна для f_i, $i = 1, \dots, n$, и классом нагруженных гиперграфов следующего вида. В качестве множества вершин выберем множество E_k^n. Содержательно каждая вершина соответствует набору значений переменных. Каждое подмножество вершин вида

$$\{(a_1, \dots, a_{i-1}, c, a_{i+1}, \dots, a_n) \mid c \in E_k\} \tag{1}$$

образуем гиперребро. Содержательно гиперребрами соединяются все наборы, отличающиеся ровно в одной заданной позиции. Дополнительно каждое гиперребро снабжается пометкой из множества E_k. В булевом случае роль пометок играла ориентация ребер.

Для определения отображения из множества семейств функций в множество гиперграфов достаточно задать правило, задающее значение меток гиперребер. Сделаем это следующим образом. Пусть F_n —

некоторое семейство. Тогда гиперребро (1) снабжается меткой, равной $f_i(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n)$. Заметим, что в силу фиктивной зависимости f_i от переменной x_i константа 0 может быть заменена на любую другую, при этом значение метки не изменится. Легко увидеть, что построенное соответствие является биекцией, так как разные семейства переходят в разные гиперграфы и любая комбинация меток реализуется как образ некоторого семейства.

Рассмотрим правильное семейство, такое что все функции тождественно равны константе $k-1$, и гиперграф H_n, соответствующий этому семейству. Метки всех гиперребер H_n равны $k-1$. Рассмотрим произвольное паросочетание M в H_n. Произвольным образом поменяем значения меток для гиперребер из M, выбрав для каждого гиперребра новое значение из множества $E_k \setminus \{k-1\}$. Обозначим получившийся гиперграф через H'_n, а прообраз этого гиперграфа относительно введенного соответствия через $F'_n = (f'_1, \ldots, f'_n)$. Покажем, что он является образом правильного семейства функций. Возможны следующие случаи.

1. $n = 1$. Тогда H'_n имеет ровно одно гиперребро с пометкой $c \in E_k$ и соответствует семейству, состоящему из одной функции, тождественно равной c, то есть является правильным.

2. $n = 2$. Тогда гиперграф H'_n имеет форму квадрата, а все гиперребра из множества M идут в одном направлении (любые два гиперребра, идущих разных направлениях, то есть одно горизонтальное и одно вертикальное, пересекаются). Рассмотрим подслучай, когда ребра в M вертикальные, что соответствует вариации второй компоненты набора. Тогда семейство F'_n имеет вид $((k-1), f(x_1))$, то есть является треугольным и, как следствие, правильным. Второй подслучай рассматривается полностью аналогично.

3. $n \geq 3$. В этом случае завершим доказательство индукцией по n. Рассмотрим пару входных наборов $\alpha = (a_1, \ldots, a_n)$, $\beta = (b_1, \ldots, b_n)$, $\alpha \neq \beta$. Если найдется такой индекс i, $1 \leq i \leq n$, что $a_i = b_i$, то рассмотрим семейство F^i_n, полученное из F'_n подстановкой значения a_i вместо переменной x_i и вычеркиванием функции f'_i. Семейству F^i_n соответствует гиперграф H^i_n, являющийся подграфом H'_n, порожденным множеством вершин, для которых компонента номер i равна a_i; этот подграф может быть получен из H_{n-1} и паросочетания, в которое входят те и только те гиперребра из M, для которых координата номер i фиксирована и равна a_i. По индуктивному предположению семейство F^i_n правильное, значит, найдется индекс j, такой что $a_j \neq b_j$, но $f'_j(\alpha) = f'_j(\beta)$. Пусть теперь все компоненты наборов α и β различны. Так как вершины, соответствующие наборам α и β, принадлежат не более чем одному гиперребру из M, а $n \geq 3$, найдется такой индекс i, что гиперребра, содержащие α и β и полученные вариацией компоненты номер i, не лежат в M, то есть в H'_n

оба этих ребра сохраняют пометку $k-1$. Значит, $f_i(\alpha) = f_i(\beta) = k-1$. Таким образом, семейство F'_n правильное по определению.

Легко увидеть, что семейства, являющиеся прообразами гиперграфов для различных паросочетаний, различны. Таким образом, число паросочетаний в графе H_n является нижней оценкой числа правильных семейств размера n.

Для завершения доказательства воспользуемся оценкой из работы А. С. Асратяна и Н. Н. Кузюрина [9]. Пусть r фиксированная константа, $H^n = (V^n, E^n)$ — , r-однородный и $d(n)$-регулярный гиперграф, такой что для каждой пары $u, v \in V$, $u \neq v$, выполнено $d(u,v) = o(n)$, $n \to \infty$. Тогда число паросочетаний $N(H^n)$ оценивается снизу следующим образом:

$$N(H^n) \geq d(n)^{(n-o(n))/r}, \quad n \to \infty. \tag{2}$$

Заметим, что в гиперграфе $H(n)$ степень каждой вершины равна n, каждое ребро состоит из k вершин, а пара различных вершин принадлежит не более чем одному гиперребру. Таким образом, можно применить оценку (2) с параметрами $r = k$, $d = n$, $n = n^k$, и получить следующее асимптотическое неравенство:

$$T_k(n) \geq n^{\frac{1}{k}\left(n^k - o\left(n^k\right)\right)}, \quad n \to \infty,$$

из которого вытекает справедливость теоремы. □

Замечание 1. *Так как нижняя оценка построена с помощью паросочетания, для любого входного набора α не более, чем одна функция нового семейства примет значение, отличное от $k-1$, откуда следует, что это семейство является обобщенно ортогональным.*

Используем полученную оценку для доказательства того, что семейства из примеров 1 составляют бесконечно малую долю в множестве всех правильных семейств.

Теорема 2. *Пусть $k \in \mathbb{N}$, $k \geq 3$. Тогда доля треугольных семейств размера n в множестве всех правильных семейств размера n стремится к 0 при $n \to \infty$.*

Доказательство. Сперва оценим сверху мощность множества треугольных семейств $(f_1, \ldots, f_n)$, таких что переменные $x_i, \ldots, x_n$ фиктивны для функции $f_i(x_1, \ldots, x_n)$, $i = 1, \ldots, n$. Из предположения на вид функции f_i следует, что она может быть выбрана $k^{k^{i-1}}$ способами. Значит, общее число треугольных семейств такого вида оценивается сверху следующим образом:

$$k^{k^0} \cdot k^{k^1} \cdot \ldots \cdot k^{k^{n-1}} = k^{\sum_{i=0}^{n-1} k^i} = k^{\frac{k^n - 1}{k-1}} \leq k^{k^n}.$$

В результате согласованной перенумерации мощность вырастет не более, чем в $n!$ раз. Следовательно, доля треугольных семейств в множестве всех правильных семейств оценивается сверху величиной

$$\frac{n! \cdot k^{k^n}}{n^{A \cdot k^n}}. \tag{3}$$

Логарифм по основанию k отношения (3) в свою очередь оценивается величиной

$$\log_k (n!) + k^n - Ak^n \cdot \log_k n \leq n \cdot \log_k n + k^n - Ak^n \cdot \log_k n,$$

которая стремится к $-\infty$ при $n \to \infty$. Значит, искомое отношение стремится к 0. $\square$

Следствие 1. *Отношение числа треугольных семейств размера n к числу обобщенно ортогональных семейств размера n стремится к 0 при $n \to \infty$.*

Замечание 2. *Аналог теоремы 2 для булева случая был установлен К. Д. Царегородцевым (см. [10, Теорема 6]). Следствие 1 в булевом случае также имеет место.*

Теперь покажем, что свойство правильности является редким: доля правильных семейств размера n среди всех семейств размера n, в которых функции фиктивно зависят от одноименной переменной, стремится к 0.

Теорема 3. *Пусть $k \in \mathbb{N}$, $k \geq 3$. Тогда*

$$\lim_{n\to\infty} \frac{T_k(n)}{N_k(n)} = 0, \tag{4}$$

где $N_k(n)$ — число семейств $(f_1, \ldots, f_n)$, $f_i \in P_k^n$, таких что переменная x_i фиктивна для функции $f_i(x_1, \ldots, x_n)$.

Доказательство. Функцию от n переменных, для которой заданная переменная фиктивна, очевидным образом можно выбрать $k^{k^{n-1}}$ способом, откуда следует равенство $N_k(n) = k^{n \cdot k^{n-1}}$.

Оценим сверху величину $T_k(n)$. Разделим функции семейства на пары: (f_1, f_2), (f_3, f_4), … Если n четно, последняя пара имеет вид (f_{n-1}, f_n), в противном случае последняя пара имеет вид (f_{n-2}, f_{n-1}), а последняя функция остается без пары. Оценим число вариантов для выбора пары (f_i, f_{i+1}). Сгруппируем входные наборы так, что в одну группу попадают все наборы, отличающихся только в позициях i или j. В каждой группе окажется k^{n-2} набора. На каждой группе пару (f_i, f_j) можно рассматривать как семейство функций от двух переменных x_i, x_j. Используя утверждение о сохранении правильности при подстановке константы вместо переменной с удалением одноименной функции (см., например, [11, лемма 1]) легко показать, что это семейство правильное. Известно, что правильные семейства размера 2 являются треугольными (см., например, [11, утверждение 1]). Значит, на рассматриваемой группе входных наборов либо f_i является константой, а f_j есть функция от одной переменной x_i, либо наоборот. Значит, имеется не более $2 \cdot k \cdot k^k$ способов задать значения пары функций (f_i, f_j) на каждой группе входов, а общее число способов выбора (f_i, f_j) оценивается сверху величиной

$$\left(2 \cdot k \cdot k^k\right)^{k^{n-2}} \leq \left(k^{k+2}\right)^{k^{n-2}} = k^{(k+2)k^{n-2}}.$$

Если n четно, число пар равно $n/2$, поэтому число правильных семейств размера n оценивается сверху величиной

$$\left(k^{(k+2)k^{n-2}}\right)^{n/2};$$

если n нечетно, замечаем, что оставшаяся без пары функция f_n имеет фиктивную переменную x_n и поэтому может быть выбрана не более, чем $k^{k^{n-1}}$ способом, поэтому верхняя оценка принимает вид

$$\left(k^{(k+2)k^{n-2}}\right)^{(n-1)/2} \cdot k^{k^{n-1}}.$$

Поделим полученные оценки на $N_k(n)$ и прологарифмируем по основанию k. В первом случае с учетом неравенства $k \geq 3$ возникает следующая цепочка:

$$\frac{n}{2} \cdot (k+2) \cdot k^{n-2} - n \cdot k^{n-1} = \left(\frac{nk}{2} - kn + n\right) k^{n-2} = \\ = (2-k)\frac{n}{2} \cdot k^{n-2} \to -\infty, n \to \infty.$$

Во втором случае имеем

$$\frac{n-1}{2} \cdot (k+2) \cdot k^{n-2} + k^{n-1} - n \cdot k^{n-1} = \left(\frac{kn}{2} - \frac{k}{2} + n - 1 + k - nk\right) k^{n-2} = \\ = \left((2-k)\frac{n-1}{2}\right) k^{n-2} \to -\infty, n \to \infty.$$

Обе подпоследовательности сходятся к $-\infty$, откуда следует, что исходное отношение стремится к 0 при $n \to \infty$. □

Замечание 3. *Справедливость формулы (4) для случая $k = 2$ является очевидным следствием верхней оценки $T_2(n) \leq n^{B \cdot 2^n}$, полученной И. Матоушеком в работе [8]; здесь B — некоторая положительная вещественная константа.*

4. Заключение

В булевом случае в работе И. Матоушека [8] получены оценки мощности множества одностоковых ориентаций n-мерного булева куба. Из результатов К. Д. Царегородцева [7] вытекает, что эти оценки одновременно являются оценками мощности множества правильных семейств булевых функций размера n. В нашей работе изучается мощность множества правильных семейств функций k-значной логики при $k \geq 3$. В качестве нижней оценки предлагается прямое обобщение оценки Матоушека. Интересно, что она достигается на множестве обобщенно ортогональных правильных семейств, тогда как доля треугольных семейств размера n в классе всех правильных семейств размера n стремится к 0 при $n \to \infty$; более того, отношение мощности множества треугольных семейств размера n и мощности множества обобщенно ортогональных правильных семейств также стремится к 0.

Из определения правильности следует, что для каждой функции семейства одноименная переменная должна быть фиктивной. В качестве верхней оценки в работе показано, что доля правильных семейств размера n в классе всех семейств $(f_1, \ldots, f_n)$, где $f_i \in P_k^n$ и x_i фиктивна для $f_i(x_1, \ldots, x_n)$, $i = 1, \ldots, n$, стремится к 0 при $n \to \infty$. По всей видимости, верно и более сильное утверждение: $T_k(n) \leq n^{B \cdot k^n}$ для некоторой вещественной константы B. Доказательство этой гипотезы является направлением дальнейших исследований.

Автор благодарит К. Д. Царегородцева и А. Е. Панкратьева за плодотворные обсуждения и полезные замечания.

Список литературы

[1] В. А. Носов, “Критерий регулярности булевского неавтономного автомата с разделенным входом”, *Интеллектуальные системы*, **3**:3–4 (1998), 269–280.

[2] В. А. Носов, “Построение классов латинских квадратов в булевой базе данных”, *Интеллектуальные системы*, **4**:3–4 (1999), 307–320.

[3] В. А. Носов, А. Е. Панкратьев, “Латинские квадраты над абелевыми группами”, *Фундаментальная и прикладная математика*, **12**:3 (2006), 65–71.

[4] И. А. Плаксина, “Построение параметрического семейства многомерных латинских квадратов”, *Интеллектуальные системы. Теория и приложения*, **18**:2 (2014), 323–329.

[5] А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, К. Д. Царегородцев, “О порождении n-квазигрупп с помощью правильных семейств функций”, *Дискретная математика*, **35**:1 (2023), 35–53.

[6] A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev, “Proper families of functions and their applications”, *Матем. вопр. криптогр.*, **14**:2 (2023), 43–58.

[7] К. Д. Царегородцев, “О взаимно однозначном соответствии между правильными семействами булевых функций и реберными ориентациями булевых кубов”, *Прикладная дискретная математика*, 2020, № 48, 16–21.

[8] J. Matoušek, “The number of unique-sink orientations of the hypercube”, *Combinatorica*, **26** (2006), 91–99.

[9] A. S. Asratian, N. N. Kuzjurin, “On the number of nearly perfect matchings in almost regular uniform hypergraphs”, *Discrete Mathematics*, **207**:1–3 (1999), 1–8.

[10] К. Д. Царегородцев, “О свойствах правильных семейств булевых функций”, *Дискретная математиа*, **33**:1 (2021), 91–102.

[11] A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, “Latin squares over quasigroups”, *Lobachevskii Journal of Mathematics*, **41**:2 (2020), 194–203.

Bounds on the number of proper families of k-valued functions

Galatenko A.V.

Proper families of functions are a convenient apparatus for memory-efficient specification of large parametric families of quasigroups and d-quasigroups. K. D. Tsaregorodtsev proved that there exists a natural one-to-one correspondence between proper families of functions and unique sink orientations of a Boolean cube. The cardinality of such orientations was estimated by J. Matoušek. In our paper we extend Matoušek's lower bound to the case of k-valued logics for arbitrary $k > 2$, present a number of corollaries and prove that properness is a rare property, namely, the fraction of proper families of the size n in the class of all families of n-ary functions $(f_1, \dots, f_n)$ such that x_i is dummy for $f_i(x_1, \dots, x_n)$ tends to 0 as $n \to \infty$.

Keywords: proper families of functions, k-valued functions, hypergraph, matching.

References

[1] V. A. Nosov, "Regularity criterion for a non-autonomous Boolean automaton with split input", *Intellektualnye Systemy*, **3**:3–4 (1998), 269–280 (In Russian).

[2] V. A. Nosov, "Construction of classes of Latin squares in a Boolean database", *Intellektualnye Systemy*, **4**:3–4 (1999), 307–320 (In Russian).

[3] V. A. Nosov, A. E. Pankratiev, "Latin squares over Abelian groups", *Journal of Mathematical Sciences*, **149**:3 (2008), 1230–1234.

[4] I. A. Plaksina, "Construction of parametric families of multidimensional Latin squares", *Intellektualnye Systemy. Teoria i Prilojenia*, **18**:2 (2014), 323–329 (In Russian).

[5] A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev, "Generation of n-quasigroups by the means of proper families of functions", *Diskrentnaya Matematika*, **35**:1 (2023), 35–53 (In Russian).

[6] A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev, "Proper families of functions and their applications", *Matematicheskie Voprosy Kriptografii*, **14**:2 (2023), 43–58.

[7] K. D. Tsaregorodtsev, "One-to-one correspondence between proper families of Boolean functions and unique sink orientations of cubes", *Prikladnaya Diskrentnaya Matematika*, 2020, № 48, 16–21 (In Russian).

[8] J. Matoušek, "The number of unique-sink orientations of the hypercube", *Combinatorica*, **26** (2006), 91–99.

[9] A. S. Asratian, N. N. Kuzjurin, "On the number of nearly perfect matchings in almost regular uniform hypergraphs", *Discrete Mathematics*, **207**:1–3 (1999), 1–8.

[10] K. D. Tsaregorodtsev, "Properties of proper families of Boolean functions", *Discrete Mathematics and Applications*, **32**:5 (2022), 369–378.

[11] A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, "Latin squares over quasigroups", *Lobachevskii Journal of Mathematics*, **41**:2 (2020), 194–203.