ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 1**

УДК 621.391.15

© 2020 г. **Н.Л. Манев**

О РАСПРЕДЕЛЕНИИ РАССТОЯНИЙ ОРТОГОНАЛЬНЫХ ТАБЛИЦ[1]

Ортогональные таблицы играют важную роль в статистике и планировании эксперимента. Как и для других комбинаторных конструкций, наиболее важными и хорошо изученными задачами являются вопросы их существования и классификации. Существенным шагом в направлении решения таких задач является определение распределений расстояний Хэмминга ортогональной таблицы с заданными параметрами. Предлагается алгоритм для вычисления возможных распределений расстояний ортогональной таблицы с произвольными параметрами относительно произвольного вектора пространства. Возможные распределения расстояний – это все неотрицательные целочисленные решения специальных линейных систем с целыми коэффициентами. Предлагаемый алгоритм сводит задачу к проверке знаков лишь $t+1$ координат векторов в некотором подмножестве целочисленных решений системы.

Ключевые слова: ортогональные таблицы, распределение расстояний Хэмминга, неотрицательные целые решения линейной системы.

DOI: 10.31857/S0555292320010052

§ 1. Введение

Определение 1. Пусть $\mathcal{A}$ – алфавит из q символов. *Ортогональной таблицей* $\mathrm{OA}(M,n,q,t)$ *силы* t *с* M *строками*, n *столбцами* ($n \geqslant t$) *и* q *уровнями* называется $(M \times n)$-матрица (таблица) с элементами из $\mathcal{A}$, такая что каждая ее $(M \times t)$-подматрица содержит в качестве строки каждый из q^t возможных наборов длины t одинаковое число (скажем, λ) раз.

Также для $\mathrm{OA}(M,n,q,t)$ часто используются другие обозначения – $\mathrm{OA}(M,q^n,t)$ и t-(q,n,λ), где $\lambda = M/q^t$ называется *индексом*.

Тривиальным примером ортогональной таблицы является $\mathrm{OA}(\lambda q^t,t,q,t)$: каждый элемент $\mathcal{A}^t$ повторен λ раз. Вот еще один простой пример, $\mathrm{OA}(4,3,2,2)$:

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0. \end{matrix}$$

Ортогональные таблицы, также известные как *дробные факториальные дизайны*, играют важную роль в статистике и планировании эксперимента. Введенные Рао в 1946 г., они явились объектом интенсивного изучения для многих исследователей из самых разных научных областей. Есть множество статей и обзоров по этой теме,

[1] Работа выполнена при частичной финансовой поддержке Министерства образования и науки Болгарии (грант D01-271/16.12.2019, Национальный центр высокопроизводительных и распределенных вычислений).

но в качестве наиболее всестороннего источника сведений об ортогональных таблицах следует упомянуть монографию [1]. В частности, в ней подробно обсуждается взаимосвязь между ортогональными таблицами и теорией кодирования.

Здесь мы приведем лишь те основные свойства ортогональных таблиц, которые понадобятся нам для описания цели настоящей статьи и ее места в данной научной области.

Как и для других комбинаторных структур, основными вопросами в теории ортогональных таблиц являются вопрос о том, какие параметры допустимы, а также классификация с точностью до изоморфизма ортогональных таблиц с такими параметрами. В [1] были введены следующие функции.

Пусть $n \geqslant t \geqslant 2$, $q \geqslant 2$, $M = \lambda q^t$. Положим

$$f(M,q,t) \stackrel{\text{def}}{=} \max\bigl\{n : \text{существует } \mathrm{OA}(M,n,q,t),\ \text{т.е. } t\text{-}(q,n,\lambda)\bigr\},$$

$$F(n,q,t) \stackrel{\text{def}}{=} \min\bigl\{M : \text{существует } \mathrm{OA}(M,n,q,t),\ \text{т.е. } t\text{-}(q,n,M/q^t)\bigr\}.$$

Величины $f(M,q,t)$ и $F(n,q,t)$ связаны между собой следующим образом:

$$F(n,q,t) = \min\{M \mid f(M,q,t) \geqslant n\},$$
$$f(M,q,t) \leqslant \max\{n \mid F(n,q,t) \leqslant M\}.$$

Заметим, что определить значение $F(n,q,t)$ означает найти минимальный индекс λ, для которого существует $\mathrm{OA}(\lambda q^t, n, q, t)$. Таблицу наименьших известных индексов для различных значений q можно найти в [1]. Улучшения этой таблицы публикуются онлайн (см. [2,3]).

Обычно в качестве алфавита $\mathcal{A}$ выбирается коммутативное кольцо с единицей. В настоящей статье будем предполагать, что $\mathcal{A}$ – кольцо $\mathbb{Z}_q$ целых чисел по модулю q или конечное поле $GF(q)$ из q элементов.

Расстоянием Хэмминга $d(\boldsymbol{x},\boldsymbol{y})$ между двумя векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\mathcal{A}^n$ называется число позиций, в которых они различаются:

$$d(\boldsymbol{x},\boldsymbol{y}) \stackrel{\text{def}}{=} |\{i \mid x_i \neq y_i\}|.$$

Весом Хэмминга $\mathrm{wt}(\boldsymbol{c})$ вектора $\boldsymbol{c} \in \mathcal{A}^n$ называется число ненулевых элементов этого кодового слова. Очевидно, $\mathrm{wt}(\boldsymbol{c}) = d(\boldsymbol{c},\boldsymbol{0})$, где $\boldsymbol{0}$ – вектор из всех нулей.

Пусть C – подмножество (в общем случае – мультиподмножество) в $\mathcal{A}^n$, и пусть $\boldsymbol{x} \in \mathcal{A}^n$ – фиксированный вектор. Множество неотрицательных целых чисел $\boldsymbol{p}(\boldsymbol{x}) = (p_0, p_1, \ldots, p_n)$ вида

$$p_i = |\{\boldsymbol{u} \in C \mid d(\boldsymbol{x},\boldsymbol{u}) = i\}|$$

называется *распределением расстояний множества* C *относительно* $\boldsymbol{x}$.

Знание распределения расстояний множества C относительно точек из $\mathcal{A}^n$ важно при изучении кодов и ортогональных таблиц. В работах [4–6] знание возможных значений $\boldsymbol{p}(\boldsymbol{x})$ было использовано для доказательства несуществования ортогональных таблиц с заданными параметрами, чтобы определить минимально возможный индекс. Распределение $\boldsymbol{p}(\boldsymbol{x})$ вычислялось как неотрицательное целочисленное решение линейной системы с матрицей (t_j^i), где $t_j = 1 - \dfrac{2j}{n}$. Это свойство распределения $\boldsymbol{p}(\boldsymbol{x})$ является следствием результата Левенштейна из [7].

К сожалению, упомянутая линейная система с рациональными коэффициентами дает мало информации. Действительно, нужно проверить все $(M+1)^{n+1}$ возможных неотрицательных наборов целых чисел длины $(n+1)$ на предмет того, удовлетворяют ли они этой системе, что делает такую задачу почти невыполнимой.

В настоящей статье мы покажем, как можно получить много линейных систем с целыми коэффициентами, которым удовлетворяет $\boldsymbol{p}(\boldsymbol{x})$. Это позволит нам

- во-первых, понизить границы сверху для всех p_i, что значительно уменьшит число потенциальных кандидатов на $\boldsymbol{p}(\boldsymbol{x})$;
- во-вторых, избежать проверки того, является ли данный вектор решением системы, заменяя это проверкой лишь знаков некоторых $t+1$ координат этого вектора.

В § 2 представлены необходимые понятия и результаты. В § 3 описывается наш алгоритм для эффективного вычисления распределений расстояний ортогональных таблиц. В заключительном параграфе обрисованы идеи того, как можно использовать найденные распределения расстояний.

§ 2. Предварительные сведения

2.1. Многочлены Кравчука. Здесь мы приведем хорошо известные результаты о многочленах Кравчука (см., например, [7–10]).

Пусть $\mathcal{R}_n$ – линейное пространство многочленов степени не выше n над полем вещественных чисел $\mathbb{R}$. Пусть $q \geqslant 2$ – целое число. Нетрудно проверить, что билинейное отображение

$$\langle f, g\rangle \stackrel{\text{def}}{=} \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(i)g(i) \tag{1}$$

удовлетворяет аксиомам скалярного произведения.

Определение 2. *Многочленом Кравчука* называется многочлен вида

$$K_k(x;n,q) = \sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j}, \quad k = 0,1,\ldots,n.$$

Многочлен $K_k(x;n,q)$ имеет степень k по x и старший коэффициент $(-q)^k/k!$. Обычно q и n фиксированы заранее или их значения известны из контекста. Поэтому для простоты мы часто будем опускать n и q и писать просто $K_k(x)$.

Для фиксированных q и n многочлены Кравчука $K_0(x), K_1(x), \ldots, K_n(x)$ удовлетворяют равенствам

$$\langle K_k, K_\ell\rangle = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_k(i)K_\ell(i) = \binom{n}{k}(q-1)^k\delta_{k\ell} \tag{2}$$

при $k,\ell = 0,1,\ldots,n$, где $\delta_{k\ell}$ – символ Кронекера. Таким образом, они образуют *ортогональный базис* пространства $\mathcal{R}_n$ в соответствии с (1).

Используя равенство

$$(q-1)^i\binom{n}{i}K_k(i) = (q-1)^k\binom{n}{k}K_i(k), \tag{3}$$

из (2) можно вывести так называемое *второе соотношение ортогональности*

$$\sum_{i=0}^{n}K_k(i)K_i(\ell) = q^n\delta_{k\ell}. \tag{4}$$

Следующая теорема является следствием того факта, что многочлены $K_0(x)$, $K_1(x), \ldots, K_n(x)$ образуют ортогональный базис пространства $\mathcal{R}_n$.

Теорема 1. *Для любого многочлена $f(x) \in \mathbb{R}[x]$ степени $\leqslant n$ имеется единственное разложение*

$$f(x) = \sum_{k=0}^{n} f_k K_k(x),$$

где

$$f_k = \frac{1}{q^n \binom{n}{k} (q-1)^k} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) K_k(i) = \frac{1}{q^n} \sum_{i=0}^{n} f(i) K_i(k).$$

Действительно, $f_k = \langle f(x), K_k(x)\rangle / \langle K_k(x), K_k(x)\rangle$. Второе равенство вытекает из соотношения (3).

2.2. Основные свойства ортогональных таблиц.

Теорема 2 [1]. *Для любого* $\mathrm{OA}(M, n, q, t)$ *имеют место следующие свойства*:

(i) *Перестановка строк или столбцов в* $\mathrm{OA}(M, n, q, t)$ *приводит к ортогональной таблице с теми же параметрами*;

(ii) *Перестановка символов в любом столбце* $\mathrm{OA}(M, n, q, t)$ *приводит к ортогональной таблице с теми же параметрами*;

(iii) *Любая подтаблица размера* $M \times k$ *в* $\mathrm{OA}(M, n, q, t)$ *является* $\mathrm{OA}(M, k, q, t')$, *где* $t' = \min\{t, k\}$;

(iv) *Если* $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \end{pmatrix}$ *является* $\mathrm{OA}(M, n, q, t)$, *где* $\boldsymbol{A}_1$ – $\mathrm{OA}(M_1, n, q, t_1)$, *то* $\boldsymbol{A}_2$ *является* $\mathrm{OA}(M - M_1, n, q, t_2)$ *с* $t_2 \geqslant \min\{t, t_1\}$.

Напомним, что в данной статье алфавит $\mathcal{A}$ – это либо кольцо $\mathbb{Z}_q$ целых чисел по модулю q, либо конечное поле $GF(q)$ из q элементов. Следующие два результата принадлежат Дельсарту [11–13].

Лемма 1. *Пусть* C – $\mathrm{OA}(M, n, q, t)$, *и пусть* $\boldsymbol{x} \in \mathbb{F}_q^n$. *Если* C *имеет распределение расстояний* $\boldsymbol{p}(\boldsymbol{x}) = (p_0, p_1, \ldots, p_n)$ *относительно* $\boldsymbol{x}$, *то*

$$\sum_{i=0}^{n} p_i K_k(i) = 0 \quad \text{для } k = 1, \ldots, t. \tag{5}$$

Пусть C – (мульти)подмножество $\mathcal{A}^n$. Последовательность рациональных чисел $\{A_i\}$, $i = 0, 1, \ldots, n$, вида

$$A_i \stackrel{\text{def}}{=} \frac{1}{|C|} \left|\{(\boldsymbol{x}, \boldsymbol{y}) \in C^2 \mid d(\boldsymbol{x}, \boldsymbol{y}) = i\}\right|$$

называется *распределением расстояний* (мульти)множества C. Очевидно, $\{A_i\}$ является средним значением $\boldsymbol{p}(\boldsymbol{x})$ по всем $\boldsymbol{x} \in C$.

Лемма 2. *Пусть* C – $\mathrm{OA}(M, n, q, t)$, *и пусть* $\{A_i\}$, $i = 0, 1, \ldots, n$, – *распределение расстояний* C. *Тогда*

$$\sum_{i=0}^{n} A_i K_k(i) \geqslant 0$$

для любого $k = 0, 1, \ldots, n$.

§ 3. Как эффективно вычислять распределения расстояний

Теорема 3. *Пусть C является* $\mathrm{OA}(M,n,q,t)$, *и пусть* $\boldsymbol{v}\in\mathbb{F}_q^n$. *Если* $\boldsymbol{p}(\boldsymbol{v})=(p_0,p_1,\ldots,p_n)$ – *распределение расстояний C относительно* $\boldsymbol{v}$, *то для любого многочлена* $f(x)$ *степени* $\deg f\leqslant t$ *справедливо*

$$\sum_{i=0}^{n}p_if(i)=f_0M,\quad f_0=\frac{1}{q^n}\sum_{i=0}^{n}f(i)K_i(0)=\frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^if(i),\tag{6}$$

где $f(x)=f_0+\sum\limits_{j=1}^{t}f_jK_j(x)$.

Доказательство. Подставляя $x=i$ в $f(x)$ и умножая $f(i)$ на p_i, получаем

$$p_if(i)=f_0p_i+\sum_{j=1}^{t}f_jp_iK_j(i)\quad\text{для } i=0,1,\ldots,n.$$

Суммируя по i, получаем

$$\sum_{i=0}^{n}p_if(i)=f_0\sum_{i=0}^{n}p_i+\sum_{j=1}^{t}\biggl(f_j\sum_{i=0}^{n}p_iK_j(t_i)\biggr)=f_0M+\sum_{j=1}^{t}\biggl(f_j\sum_{i=0}^{n}p_iK_j(i)\biggr).$$

Поскольку C имеет силу t, по лемме 1 имеем

$$\sum_{i=0}^{n}p_iK_j(i)=0\quad\text{для } j=1,\ldots,t.$$

Следовательно,

$$\sum_{i=0}^{n}p_if(i)=f_0M.$$

Значение f_0 дается теоремой 1. ▲

Это простое следствие леммы 1 Дельсарта дает очень полезный инструмент для изучения ортогональных таблиц и, в частности, их распределений расстояний. Ее важность обусловлена большой свободой при выборе многочлена $f(x)$.

В дальнейшем мы будем применять теорему 3 с многими различными многочленами, но вначале проиллюстрируем ее важность, приведя альтернативное доказательство хорошо известного свойства, указанного в [14] (хотя и сформулированного там в ином виде). Оригинальное доказательство основано на комбинаторных рассуждениях и содержится также в [1, лемма 2.7].

Теорема 4. *Пусть C является* $\mathrm{OA}(M,n,q,t)$, *и пусть* $\boldsymbol{v}\in\mathcal{A}^n$. *Если* $\boldsymbol{p}(\boldsymbol{v})=(p_0,p_1,\ldots,p_n)$ – *распределение расстояний ортогональной таблицы C относительно* $\boldsymbol{v}$, *то при* $k=0,1,\ldots,t$

$$\sum_{i=0}^{n}\binom{n-i}{k}p_i=\frac{M}{q^k}\binom{n}{k}=\lambda q^{t-k}\binom{n}{k}.\tag{7}$$

Доказательство. Выбирая $f(x) = \binom{n-x}{k}$ для $k = 0, 1, \ldots, t$ в теореме 3, получаем

$$\sum_{i=0}^{n} \binom{n-i}{k} p_i = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{n-i}{k} (q-1)^i = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{k} \binom{n-k}{i} (q-1)^i =$$
$$= \frac{M}{q^n} \binom{n}{k} \sum_{i=0}^{n} \binom{n-k}{i} (q-1)^i = \frac{M}{q^n} \binom{n}{k} q^{n-k}. \quad \blacktriangle$$

Следующая теорема – первое из следствий теоремы 3, которые мы будем использовать для решения нашей задачи.

Теорема 5. *Пусть C является* $\mathrm{OA}(M, n, q, t)$, *и пусть $\boldsymbol{v} \in \mathbb{F}_q^n$. Если $\boldsymbol{p}(\boldsymbol{v}) = (p_0, p_1, \ldots, p_n)$ – распределение расстояний ортогональной таблицы C относительно $\boldsymbol{v}$, то при $k = 0, 1, \ldots, t$*

$$\sum_{i=0}^{n} p_i i^k = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} i^k (q-1)^i, \tag{8}$$

$$\sum_{i=0}^{n} p_i (n-i)^k = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i (n-i)^k. \tag{9}$$

Доказательство. Выбирая $f(x) = x^k$ для $k = 0, 1, \ldots, t$ в теореме 3, получаем (8). Аналогично, полагая $f(x) = (n-x)^k$, получаем (9). $\blacktriangle$

Равенства (8), (9) показывают, что $(p_0, p_1, \ldots, p_n)$ является решением двух эквивалентных линейных систем с неотрицательными целыми коэффициентами. Наша задача – найти все их неотрицательные целые решения, т.е. среди всех целочисленных решений выделить неотрицательные.

Хорошо известно, что пространством решений линейной системы $\boldsymbol{A}\boldsymbol{x}^\tau = \boldsymbol{b}$ является смежный класс $\boldsymbol{x}_0 + \boldsymbol{U}$, где $\boldsymbol{x}_0$ – частное решение, а $\boldsymbol{U}$ – нулевое пространство оператора $\boldsymbol{A}$. В нашем случае $\operatorname{rank} \boldsymbol{A} = t+1$, т.е. $\dim \boldsymbol{U} = n+1-(t+1) = n-t$. Следовательно, $\boldsymbol{U}$ порождается строками $((n-t)\times(n+1))$-матрицы $\boldsymbol{A}^\perp$ ранга $n-t$, удовлетворяющей соотношению $\boldsymbol{A}(\boldsymbol{A}^\perp)^\tau = \boldsymbol{O}$.

В теореме 6 дана явная форма матрицы $\boldsymbol{A}^\perp$. Ее доказательство основано на следующей лемме.

Лемма 3. *Для любого $\ell = 0, 1, 2, \ldots, r$ и любого неотрицательного целого s имеет место соотношение*

$$\sum_{j=0}^{r} \binom{r}{j} (j+s)^\ell x^{j+s} = (1+x)^{r-\ell} g_\ell(x), \quad \deg g_\ell(x) = \ell + s, \tag{10}$$

причем старший коэффициент многочлена $g_\ell(x)$ равен $(r+s)^\ell$.

Доказательство леммы вынесено в Приложение.

Теорема 6. *Пусть $\boldsymbol{A} = (a_{ki}) = (i^k)$, $k = 0, 1, \ldots, t$, $i = 1, 2, \ldots, n$. При $t < m \leqslant n$ вектор*

$$\left(1, -\binom{m}{1}, \binom{m}{2}, \ldots, (-1)^j \binom{m}{j}, \ldots, (-1)^m, 0, \ldots, 0\right)$$

и все его $n-m-1$ правых циклических сдвигов линейно независимы и принадлежат нулевому пространству матрицы $\boldsymbol{A}$. В частности, при $m = t+1$ они образуют базис нулевого пространства.

Доказательство. Полагая $x = -1$ и $r = m$ в (10), для $\ell = 0, 1, \ldots, m-1$ получаем

$$\sum_{j=0}^{m} (-1)^{j+s} \binom{m}{j} (j+s)^{\ell} = 0,$$

что и доказывает теорему. ▲

Частное решение $\boldsymbol{x}_0$ легко можно найти, полагая $n-t$ переменных равными нулю и решая полученную систему из $t+1$ уравнений с $t+1$ неизвестными.

В качестве иллюстрации приведем следующий пример 1. Однако в описываемом ниже алгоритме мы применяем несколько отличный подход, не использующий метод Гаусса. Это показано в примере 2.

Пример 1. Рассмотрим OA($M = 18$, $n = 7$, $q = 3$, $t = 2$). Матрица $\boldsymbol{A}$ и столбец свободных членов $\boldsymbol{b}$ из уравнения (9) имеют вид

$$\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 49 & 36 & 25 & 16 & 9 & 4 & 1 & 0 \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} 18 \\ 42 \\ 126 \end{pmatrix}.$$

Матрица, порождающая нулевое пространство, согласно теореме 6 имеет вид

$$\boldsymbol{A}^{\perp} = \begin{pmatrix} 1 & -3 & 3 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 3 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 3 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -3 & 3 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 & 3 & -1 \end{pmatrix}.$$

С помощью метода Гаусса можно привести $\boldsymbol{A}^{\perp}$ к систематическому (приведенному ступенчатому) виду $\boldsymbol{A}^{\perp} \sim (\boldsymbol{I}_{n-t} \boldsymbol{B})$, где $\boldsymbol{B}$ – матрица размера $(n-t) \times (t+1)$ с целыми элементами. Для матрицы из примера 1 получаем

$$\boldsymbol{A}^{\perp} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -21 & 35 & -15 \\ 0 & 1 & 0 & 0 & 0 & -15 & 24 & -10 \\ 0 & 0 & 1 & 0 & 0 & -10 & 15 & -6 \\ 0 & 0 & 0 & 1 & 0 & -6 & 8 & -3 \\ 0 & 0 & 0 & 0 & 1 & -3 & 3 & -1 \end{pmatrix}.$$

Систематический вид показывает, что для нахождения всех неотрицательных целых решений системы следует вначале вычислить все линейные комбинации строк этой систематической матрицы с целыми коэффициентами из интервала $[0, M]$.

Ненулевые координаты вектора $\boldsymbol{x}_0$ нужно выбирать в тех позициях, где находится матрица $\boldsymbol{B}$ (в нашем примере это последние $t+1$ координат). Тогда после прибавления $\boldsymbol{x}_0$ к вычисленным линейным комбинациям нужно выбрать те из полученных векторов, последние $t+1$ координат которых неотрицательны. В рассматриваемом примере частным решением системы является $(0, 0, 0, 0, 0, 42, -42, 18)$.

Верхние границы для $\boldsymbol{p} = (\boldsymbol{p_0}, \boldsymbol{p_1}, \ldots, \boldsymbol{p_n})$. Число $(M+1)^{n-t}$ слишком велико даже при малых значениях параметров M, n, q, t. К счастью, лишь немногие p_i могут принимать значения, близкие к M. Для большинства значений i интервал значений p_i гораздо короче. Действительно, снова применяя теорему 3, заключаем, что если $f(i) \geqslant 0$ для всех $i = 0, 1, \ldots, n$, то

$$p_i \leqslant f_0 M / f(i).$$

Изменяя многочлен $f(x)$, можно получить множество верхних границ на p_i и затем взять минимум из них. Каждый из многочленов x^k и $(n-x)^k$, используемых при выводе формул (8), (9), дает одну из таких возможностей. При четном k можно использовать, например, многочлены

$$f(x) = (2x-n)^k, \quad f(x) = (3x-n)^k, \quad f(x) = (3n-4x)^k, \quad f(x) = (3x-2n)^k.$$

С помощью описанного метода для ортогональной таблицы из примера 1 получаем следующий вектор верхних границ:

$$\boldsymbol{u} = (1, 1, 3, 6, 14, 16, 8, 4).$$

Для свободных неизвестных не обязательно выбирать именно первые $n-t$ позиций, годятся любые $n-t$. В примере 2 в качестве свободных неизвестных выбираются неизвестные с номерами 1, 2, 3, 4 и 8. Затем следует породить $1 \cdot 1 \cdot 3 \cdot 6 \cdot 4 = 72$ возможных кандидата для $\boldsymbol{p} = (p_0, p_1, \ldots, p_n)$. Это дает значительный выигрыш в количестве вычислений по сравнению с числом 19^5. Разумеется, нужно привести матрицу $\boldsymbol{A}^\perp$ к правильному виду. Требуемая для этого процедура описана ниже.

Для больших значений параметров получаемый выигрыш еще более значителен и делает задачу вычисления распределений расстояний поддающейся решению. Однако, к сожалению, нет такого многочлена, который улучшает границы во всех координатах. Каждый многочлен дает лучшие границы для некоторых координат и худшие для остальных. Использование приведенных выше многочленов можно рассматривать как первое приближение для вектора верхних границ $\boldsymbol{u}$. Столбцы $s+1, \ldots, s+t+1$ матрицы $\boldsymbol{A}^\perp$ также можно использовать для улучшения $\boldsymbol{u}$ (см. ниже замечание после алгоритма вычисления нулевого пространства).

Далее мы опишем более эффективный алгоритм для вычисления $\boldsymbol{p}$, не использующий метод Гаусса. Этот алгоритм основан на следующих утверждениях.

Теорема 7. *Пусть C является* $\mathrm{OA}(M, n, q, t)$, *и пусть* $\boldsymbol{v} \in \mathbb{F}_q^n$. *Если* $\boldsymbol{p}(\boldsymbol{v}) = (p_0, p_1, \ldots, p_n)$ – *распределение расстояний ортогональной таблицы C относительно* $\boldsymbol{v}$, *то для* $k = 0, 1, \ldots, t$ *и целого s справедливы равенства*

$$\sum_{i=0}^{n} p_i \binom{i-s}{k} = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i \binom{i-s}{k}. \tag{11}$$

Доказательство. Подставляя $f(x) = \binom{x-s}{k}$ в теорему 3 для $k = 0, 1, \ldots, t$ и целого s, получаем требуемое утверждение. ▲

Лемма 4. *Пусть* $\boldsymbol{R}_t = (r_{ij}) = \left(\binom{j}{i}\right)$, *где* $i, j = 0, 1, 2, \ldots, t$. *Тогда обратная матрица имеет вид*

$$\boldsymbol{R}_t^{-1} = \left((-1)^{i+j} \binom{j}{i}\right).$$

Доказательство леммы см. в Приложении.

Алгоритм

P1. Определить наилучший возможный вектор $\boldsymbol{u}$ верхних границ на векторы $\boldsymbol{p}$ возможных распределений.

P2. Выбрать $t+1$ последовательных позиций, где $\boldsymbol{u}$ содержит максимальные значения, и присвоить номер s позиции перед ними. Вычислить частное решение системы (11) с нулями во всех позициях, кроме $t+1$ выбранных.

P3. Применить алгоритм построения нулевого пространства, приведенный ниже.

P4. Прибавляя частное решение к каждому вектору нулевого пространства, найти целочисленные решения системы (11).

P5. Выбрать решения, имеющие неотрицательные значения в позициях $s+1, \ldots, s+t+1$. (Все остальные позиции, очевидно, неотрицательны.)

Решения с нулевой первой координатой – это распределения расстояний относительно внешней точки ортогональной таблицы, а решения с ненулевой первой координатой соответствуют распределениям относительно внутренних точек. Если первая координата больше единицы, то это означает, что точка встречается более одного раза, т.е. ортогональная таблица является мультимножеством.

Алгоритм построения нулевого пространства

NS1. Построить матрицу

$$\boldsymbol{A} = (a_{ij}) = \left(\binom{j-s}{i} \right),$$

где ненулевыми позициями частного решения $\boldsymbol{x}_0$ являются $s+1, \ldots, s+t+1$. В столбцах $s{+}1, \ldots, s{+}t{+}1$ она содержит матрицу $\boldsymbol{R}_t$, определенную в лемме 4.

NS2. Умножая слева на матрицу $\boldsymbol{R}_t^{-1}$ (см. лемму 4), привести матрицу $\boldsymbol{A}$ к ступенчатому виду $\boldsymbol{B}$, содержащему единичную $((t+1)\times(t+1))$-матрицу $\boldsymbol{I}_{t+1}$ в столбцах $s+1, \ldots, s+t+1$, т.е. получить матрицу

$$\boldsymbol{B} = \boldsymbol{R}_t^{-1}\boldsymbol{A} = (\boldsymbol{U}_1 \boldsymbol{I}_{t+1} \boldsymbol{U}_2),$$

где $\boldsymbol{U}_1$ и $\boldsymbol{U}_2$ – матрицы размера $(t+1)\times s$ и $(t+1)\times(n-t-s)$ соответственно.

NS3. Построить порождающую нулевое пространство матрицу

$$\boldsymbol{A}^{\perp} = \begin{pmatrix} \boldsymbol{I}_s & -\boldsymbol{U}_1^{\tau} & \boldsymbol{O}_1 \\ \boldsymbol{O}_2 & -\boldsymbol{U}_2^{\tau} & \boldsymbol{I}_{n-t-s} \end{pmatrix},$$

где $\boldsymbol{O}_1$ и $\boldsymbol{O}_2$ – нулевые матрицы соответствующих размеров.

NS4. Вычислить все линейные комбинации строк матрицы $\boldsymbol{A}^{\perp}$ с неотрицательными коэффициентами, ограниченные вектором $\boldsymbol{u}$.

Замечание. Минимизация вектора верхних границ $\boldsymbol{u}$ имеет очень важное значение. Уменьшение даже на единицу одной позиции вектора $\boldsymbol{u}$ приводит к значительному сокращению числа проверок. Полезным шагом в этом направлении является вычисление матрицы, порождающей нулевое пространство (т.е. п. **NS3**), для $s = n-t$ или $n-t-1$ и сравнение ее элементов с соответствующим частным решением. Это может привести к улучшению вектора верхних границ $\boldsymbol{u}$.

Пример 2. Рассмотрим OA($M = 18$, $n = 7$, $q = 3$, $t = 2$). Значение $s = 4$ соответствует частному решению $\boldsymbol{x}_0 = (0,0,0,0,18,-12,12,0)$. Имеем

$$\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 \\ 10 & 6 & 3 & 1 & 0 & 0 & 1 & 3 \end{pmatrix}, \quad \boldsymbol{R}_2^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\boldsymbol{B} = \begin{pmatrix} 15 & 10 & 6 & 3 & 1 & 0 & 0 & 1 \\ -24 & -15 & -8 & -3 & 0 & 1 & 0 & -3 \\ 10 & 6 & 3 & 1 & 0 & 0 & 1 & 3 \end{pmatrix},$$

$$\boldsymbol{A}^{\perp} \sim \boldsymbol{B}^{\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & -15 & 24 & -10 & 0 \\ 0 & 1 & 0 & 0 & -10 & 15 & -6 & 0 \\ 0 & 0 & 1 & 0 & -6 & 8 & -3 & 0 \\ 0 & 0 & 0 & 1 & -3 & 3 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 3 & -3 & 1 \end{pmatrix}.$$

Затем вычисляем 72 линейные комбинации строк с неотрицательными коэффициентами, ограниченные вектором $\boldsymbol{u}$, и после прибавления к ним частного решения $(0,0,0,0,18,-12,12,0)$ удаляем векторы с отрицательными пятой, шестой и седьмой координатами. Оставшиеся 43 вектора являются кандидатами на распределения расстояний относительно точки. Только два из них, $(1,0,0,1,0,15,1,0)$ и $(1,0,0,0,3,12,2,0)$, соответствуют внутренней точке. Остальные 41 соответствуют внешней точке.

§ 4. Заключение

В статье предложен эффективный алгоритм вычисления распределения расстояний ортогональной таблицы относительно произвольной точки. Знание возможных распределений имеет важное значение для решения задач существования и классификации, а также дает полезную информацию о радиусе покрытия ортогональной таблицы, рассматриваемой как q-ичный код.

Для полноты изложения вкратце опишем, как можно применить знание возможных распределений расстояний относительно вектора из $\mathcal{A}^n$ для изучения ортогональных таблиц и как получить информацию об их структуре.

Пусть теперь C – $\mathrm{OA}(M,n,q,t)$, а $\check{C}$ – ортогональная таблица, полученная из C удалением первого столбца. Через C_i, $i=0,1,\ldots,q-1$, обозначим множество, полученное выбором всех столбцов C с i-м элементом алфавита $\mathcal{A}$ в первом столбце и последующим удалением первого столбца (множество C_0 соответствует элементу 0 в первом столбце.) Согласно теореме 2

$$\check{C} \text{ является } \mathrm{OA}(M,n-1,q,t), \quad \text{а} \quad C_i \text{ является } \mathrm{OA}(M/q,n-1,q,t-1),$$

причем будем также предполагать, что C содержит нулевой вектор. Теперь применим описанный алгоритм вычисления всех возможных распределений расстояний для C, C_i и $\check{C}$, а также при необходимости для любых других таблиц, получающихся из C.

Пусть $\boldsymbol{c}=(c_1,c_2,\ldots,c_n)\in C$, т.е. $\boldsymbol{c}_0=(c_2,\ldots,c_n)\in C_0$ или C_i. Пусть $\boldsymbol{p}(\boldsymbol{c})=$ $=(p_0,p_1,\ldots,p_n)$ – распределение расстояний C относительно точки $\boldsymbol{c}$, а $\boldsymbol{p}^0(\boldsymbol{c}_0)=$ $=(p_0^0,p_1^0,\ldots,p_{n-1}^0)$ – распределение расстояний C_0 (или C_i) относительно $\boldsymbol{c}_0$ соответственно. Если $\boldsymbol{c}=\boldsymbol{0}$, то $\boldsymbol{p}(\boldsymbol{c})$ и $\boldsymbol{p}(\boldsymbol{c}_0)$ являются распределениями весов для C и C_0.

Нетрудно непосредственно доказать, что

- вектор $(p_0,p_1,\ldots,p_{n-1})$ должен *мажорировать* $(p_0^0,p_1^0,\ldots,p_{n-1}^0)$, т.е. $p_i\geqslant p_i^0$ для всех i, когда $p_0^0\geqslant 1$;
- вектор $(p_1,p_2,\ldots,p_n)$ должен мажорировать $(p_0^0,p_1^0,\ldots,p_{n-1}^0)$, когда $p_0^0=0$;
- разность $\overline{\boldsymbol{p}}(\boldsymbol{c})=(p_1-p_1^0,\ldots,p_{n-1}-p_{n-1}^0,p_n)$ должна быть распределением расстояний для $C_1\cup\ldots\cup C_{q-1}$ относительно внешней точки $\boldsymbol{c}_0$;
- вектор $\check{\boldsymbol{p}}=\overline{\boldsymbol{p}}(\boldsymbol{c})+\boldsymbol{p}^0$ должен быть распределением расстояний $\check{C}$ относительно $\boldsymbol{c}_0$.

Для рассмотренной в примерах ортогональной таблицы $C=\mathrm{OA}(18,7,3,2)$ имеем $C_i=\mathrm{OA}(6,6,3,1)$ и $\check{C}=\mathrm{OA}(18,6,3,2)$. Для точки $\boldsymbol{c}\in C$ мы получили два возможных распределения $\boldsymbol{p}(\boldsymbol{c})=(1,0,0,1,0,15,1,0)$ и $\boldsymbol{p}(\boldsymbol{c})=(1,0,0,0,3,12,2,0)$. Первое распределение мажорирует три возможных распределения, а второе – только одно, что дает четыре из десяти возможных распределений для $\check{C}$ относительно внутренней точки и лишь три из 29 распределений для C_i относительно внешней точки. Поскольку можно выбирать $\boldsymbol{c}=\boldsymbol{0}$, по крайней мере одно из этих распределений и его подраспределений должно быть распределением весов. Таким образом, мы получили много информации о структуре C, которую можно использовать для построения и классификации таких ортогональных таблиц. Все неизоморфные $\mathrm{OA}(18,n,3,2)$ для $3\leqslant n\leqslant 7$ классифицированы в [15], куда мы и отсылаем заинтересованного читателя за дальнейшими подробностями.

Разработанный алгоритм был применен к различным открытым случаям ортогональных таблиц с $q = 3$ уровнями. Стандартный подход к ним приводит к практически не осуществимым вычислениям (видимо, именно по этой причине эти случаи оставались открытыми). Было доказано несуществование некоторых из них и определена возможная структура других. Определение распределения расстояний является важнейшим шагом, но не единственным. Чтобы полностью разобрать какой-либо случай, нужны дополнительные соображения, выходящие за пределы настоящей статьи.

ПРИЛОЖЕНИЕ

Доказательство леммы 3. Применим математическую индукцию. По формуле бинома Ньютона получаем

$$\sum_{j=0}^{r} \binom{r}{j} x^{j+s} = x^s(1+x)^r.$$

Дифференцируя и умножая на x, получаем

$$\sum_{j=0}^{r} \binom{r}{j} (j+s)x^{j+s} = (1+x)^{r-1}x^s[(r+s)x+s] = (1+x)^{r-1}g_1(x),$$

где $\deg g_1(x) = s+1$, а его старший коэффициент равен $r+s$.

Это дает базу индукции. Предположим, что справедливо соотношение (10). Докажем его для $\ell+1$. Дифференцируя и умножая на x, получаем

$$\sum_{j=0}^{r} \binom{r}{j} (j+s)^{\ell+1}x^{j+s} = x\left[(r-\ell)(1+x)^{r-\ell-1}g_\ell(x) + (1+x)^{r-\ell}g'_\ell(x)\right] =$$
$$= (1+x)^{r-\ell-1}x\left[(r-\ell)g_\ell(x) + (1+x)g'_\ell(x)\right] = (1+x)^{r-\ell-1}g_{\ell+1}(x).$$

Нетрудно убедиться, что старшим коэффициентом многочлена $g_{\ell+1}(x)$ является $(r-\ell)(r+s)^\ell + (\ell+s)(r+s)^\ell = (r+s)^{\ell+1}$ и что $\deg g_{\ell+1} = \ell+s+1$. ▲

Доказательство леммы 4. Доказательство основано на следующем комбинаторном тождестве, приведенном в [16, § 1.2]: для любых натуральных чисел m и k справедливо соотношение

$$\sum_{j=k}^{m} (-1)^j \binom{m}{j}\binom{j}{k} = (-1)^k\delta_{mk}.$$

Используя его, получаем

$$\sum_{j=0}^{n} r_{kj}((-1)^{j+m}r_{jm}) = (-1)^m \sum_{j=0}^{n} (-1)^j \binom{j}{k}\binom{m}{j} = (-1)^m(-1)^k\delta_{mk} = \delta_{mk}. \quad ▲$$

СПИСОК ЛИТЕРАТУРЫ

1. *Hedayat A., Sloane N.J.A., Stufken J.* Orthogonal Arrays: Theory and Applications. New York: Springer-Verlag, 1999.
2. A Library of Orthogonal Arrays (online tables; maintained by Sloane N.J.A.), `http://neilsloane.com/oadir/index.html`.
3. A Library of Distance Distributions of Ternary Orthogonal Arrays (online tables), `https://store.fmi.uni-sofia.bg/fmi/algebra/stoyanova/toa.html`.

4. *Бойваленков П., Кулина Х.* Исследование двоичных ортогональных таблиц через их распределение расстояний // Пробл. передачи информ. 2013. Т. 49. № 4. С. 28–40.
5. *Boyvalenkov P., Marinova T., Stoyanova M.* Nonexistence of a Few Binary Orthogonal Arrays // Discrete Appl. Math. 2017. V. 217. Part 2. P. 144–150.
6. *Boumova S., Marinova T., Stoyanova M.* On Ternary Orthogonal Arrays // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XVI). Svetlogorsk, Russia. Sept. 2–8, 2018. P. 102–105. Available at `https://www.dropbox.com/s/h7u89lh8vyirww9/Proceedings\%20final.pdf?dl=0`.
7. *Levenshtein V.I.* Krawtchouk Polynomials and Universal Bounds for Codes and Designs in Hamming Spaces // IEEE Trans. Inform. Theory. 1995. V. 41. № 5. P. 1303–1321.
8. *Krawtchouk M.* Sur une généralisation des polynômes d'Hermite // C. R. Acad. Sci. Paris. 1929. V. 189. № 17. P. 620–622.
9. *Szegő G.* Orthogonal Polynomials. New York: Amer. Math. Soc., 1939.
10. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
11. *Delsarte P.* Bounds for Unrestricted Codes, by Linear Programming // Philips Res. Rep. 1972. V. 27. P. 272–289.
12. *Delsarte P.* Four Fundamental Parameters of a Code and Their Combinatorial Significance // Infor. Control. 1973. V. 23. № 5. P. 407–438.
13. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10.
14. *Bose R.C., Bush K.A.* Orthogonal Arrays of Strength Two and Three // Ann. Math. Statist. 1952. V. 23. № 4. P. 508–524.
15. *Evangelaras H., Koukouvinos C., Lappas E.* 18-Run Nonisomorphic Three Level Orthogonal Arrays // Metrika. 2007. V. 66. № 1. P. 31–37.
16. *Riordan J.* Combinatorial Identities. New York: Wiley, 1968.

Манев Николай Лазаров
Институт математики и информатики АН Болгарии,
София, Болгария
`nlmanev@math.bas.bg`

Поступила в редакцию
26.03.2019
После доработки
05.12.2019
Принята к публикации
22.12.2019