ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 2003. Серия 1. Том 10, № 2, 3–16

УДК 519.72

ВЫЧИСЛЕНИЕ ЦЕНТРИРОВАННОЙ ФУНКЦИИ ПО ЕЕ ЗНАЧЕНИЯМ НА СРЕДНИХ СЛОЯХ БУЛЕВА КУБА

С. В. Августинович, А. Ю. Васильева

Введено понятие центрированной функции, обобщающее совершенные коды с расстоянием 3. Рассмотрены некоторые свойства таких функций. Установлено, что значения центрированной функции на всех вершинах n-мерного булева куба однозначно определяются по значениям на среднем слое. Получена формула для вычисления центрированной функции по ее значениям на среднем слое.

Введение

В настоящей статье объектом изучения являются функции специального вида, заданные в вершинах n-мерного куба, а именно центрированные функции. Они являются обобщением совершенных кодов с расстоянием 3, точнее, их характеристических функций, которые и образуют мощный класс нетривиальных примеров центрированных функций. Постановка рассматриваемой задачи весьма традиционна и встречается во многих разделах математики: если мы знаем лишь некоторую частичную информацию об объекте из заданного класса, то можно ли восстановить по ней более полную информацию об этом объекте? В данном случае в качестве класса объектов рассматриваются центрированные функции, в качестве частичной информации — множество значений функции на одном из двух средних слоев булева куба нечетной размерности (такое ограничение на размерность вытекает из свойств рассматриваемых функций, см. следствие 1).

В [1] было показано, что совершенный код с расстоянием 3 однозначно определяется множеством вершин этого кода, принадлежащих среднему слою куба, т. е. вершин веса $(n+1)/2$. В настоящей статье рассматривается более общий случай — так называемые центрированные функции, каждая из которых обладает тем свойством, что сумма ее значений в вершинах шара радиуса 1 в булевом кубе не зависит от

выбора шара. Для таких функций, среди которых находятся и характеристические функции совершенных кодов с расстоянием 3, доказывается аналогичный результат и находится точная формула значения центрированной функции в любой вершине, если известны ее значения в вершинах среднего слоя.

При доказательстве этого факта наиболее существенны два обстоятельства. Во-первых, это свойство обратимости преобразования Фурье (как следует из леммы 2, вводимая в разделе 2 функция φ фактически задает коэффициенты Фурье). Для центрированной функции коэффициенты Фурье имеют простой геометрический смысл (формула (9)). Во-вторых, это описание возникающих комбинаторных объектов в терминах схемы отношений Джонсона и существенное использование ее свойств.

Основной результат — формула, по которой вычисляются значения центрированной функции по ее значениям в среднем слое, — содержится в четвертом разделе. Доказательство основано на представлении функции через ее коэффициенты Фурье. Там же имеется лемма 5, которая играет ключевую роль в доказательстве основного результата. В ней производится указанный переход к схеме отношений Джонсона. В первом разделе даются необходимые определения и обозначения, приводятся используемые факты из теории схем отношений. Во втором разделе определяется центрированная функция и устанавливаются некоторые ее свойства. В третьем разделе доказываются две леммы, которые используются при доказательстве теоремы 3. Результаты данной статьи были анонсированы авторами в [2].

1. Предварительные сведения

Введем используемые в дальнейшем обозначения и понятия. Множество всех двоичных наборов длины n называется *n-мерным булевым кубом* (или *n-кубом*) и обозначается через E^n. Обозначим $\mathbf{0} = (0, \dots, 0)$ и $\mathbf{1} = (1, \dots, 1)$. Пусть все вершины n-куба некоторым образом занумерованы. *Расстоянием Хемминга* $\rho(\mathbf{x}, \mathbf{y})$ между вершинами $\mathbf{x}$ и $\mathbf{y}$ из E^n называется число координат, в которых эти вершины различаются. *Весом Хемминга* $w(\mathbf{x})$ вершины $\mathbf{x}$ называется расстояние между вершинами $\mathbf{x}$ и $\mathbf{0}$. *Расстояние Джонсона* $g(\mathbf{x}, \mathbf{y})$ между вершинами $\mathbf{x}$ и $\mathbf{y}$ одинакового веса определяется как половина расстояния Хемминга: $g(\mathbf{x}, \mathbf{y}) = \rho(\mathbf{x}, \mathbf{y})/2$. Говорят, что вершина $\mathbf{y} = (y_1, y_2, \dots, y_n)$ *предшествует* вершине $\mathbf{x} = (x_1, x_2, \dots, x_n)$, если $x_i \leqslant y_i$ при любом i, $0 \leqslant i \leqslant n$. Для произвольных вершин $\mathbf{x}$ и $\mathbf{y}$ из n-куба через $\mathbf{x} \oplus \mathbf{y}$ обозначается их сумма по модулю 2.

Обозначим через W_i множество всех вершин веса i. В дальнейшем окажется, что можно ограничиться рассмотрением булевых кубов

нечетной размерности. В этом случае булев куб размерности n имеет два средних слоя: $W_{(n-1)/2}$ и $W_{(n+1)/2}$. Слой $W_{(n+1)/2}$ будет играть особую роль, поэтому для него введем отдельное обозначение — $A = W_{(n+1)/2}$ — и будем называть *верхним средним слоем* n-куба (или просто *средним слоем*).

Множество всех вершин из E^n, совпадающих в фиксированных $n-m$ координатах, называется *m-мерной гранью* n-куба. Через $\Gamma_{\mathbf{x}}$ будем обозначать грань, состоящую из всех вершин, предшествующих вершине $\mathbf{x} = (x_1, \dots, x_n)$.

Совершенным двоичным кодом с расстоянием 3 называется такое множество C вершин из E^n, что шары радиуса 1 с центрами из C не пересекаются и в совокупности покрывают n-куб.

Обозначим через $P_k(x; N)$ и $E_k(x; h, n)$ соответственно многочлен Кравчука и многочлен Эберлейна (см., например, [3]):

$$P_k(x;N) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{N-x}{k-j}, \tag{1}$$

$$E_k(x;h,n) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{h-x}{k-j} \binom{n-h-x}{k-j}. \tag{2}$$

Известны также другие формы записи этих многочленов, например:

$$P_k(x;N) = \sum_{j=0}^{k} (-1)^j 2^{k-j} \binom{N-x}{k-j} \binom{N-k+j}{j}, \tag{3}$$

$$E_k(i;h,n) = \sum_{j=0}^{k} (-1)^{k-j} \binom{h-j}{k-j} \binom{h-i}{j} \binom{n-h-i+j}{j}. \tag{4}$$

Весовым спектром произвольной функции $f : E^n \longrightarrow \mathbf{R}$ относительно вершины $\mathbf{x}$ называется последовательность длины $n+1$, i-й член которой $(0 \leqslant i \leqslant n)$ равен сумме значений функции f в вершинах сферы радиуса i с центром в вершине $\mathbf{x}$, т. е. $\sum\limits_{\mathbf{y} \in W_i} f(\mathbf{x} \oplus \mathbf{y})$.

Приведем используемые сведения из теории схем отношений. (Развернутое изложение можно найти, например, в [3].) *Схемой отношений Джонсона* называется множество W_h всех двоичных векторов длины n и веса h с заданными на нем отношениями R_i, $0 \leqslant i \leqslant h$:

$$(\mathbf{x}, \mathbf{y}) \in R_i \Longleftrightarrow g(\mathbf{x}, \mathbf{y}) = i.$$

Отношения R_i можно описывать матрицами инцидентности D_i, т. е. (0,1)-матрицами размера $|W_h| \times |W_h|$ с элементами

$$(D_i)_{\mathbf{x},y} = \begin{cases} 1, & \text{если } g(\mathbf{x},\mathbf{y}) = i, \\ 0 & \text{в остальных случаях,} \end{cases}$$

строки и столбцы которых соответствуют вершинам множества W_h. Векторное пространство, состоящее из всех линейных комбинаций матриц инцидентности (образующих линейно независимую систему), является алгеброй, которая называется *алгеброй Боуза — Меснера* данной схемы. Эта алгебра ассоциативна и коммутативна. Поэтому она имеет однозначно определяемый базис из примитивных идемпотентов J_i, удовлетворяющих следующим условиям:

$$\sum_{i=0}^{h} J_i = E; \quad J_i^2 = J_i; \quad J_i J_j = 0, \quad i \neq j. \tag{5}$$

Два базиса алгебры Боуза — Меснера (базис из матриц инцидентности и базис из примитивных идемпотентов) могут быть выражены друг через друга. В случае схемы Джонсона эти соотношения имеют следующий вид:

$$D_k = \sum_{i=0}^{h} E_k(i;h,n) J_i, \tag{6}$$

$$J_i = \frac{1}{|W_h|} \sum_{j=0}^{h} q_i(j) D_j, \tag{7}$$

$$q_i(j) = \frac{\mu_i}{v_j} E_j(i;h,n), \quad \mu_i = \frac{n-2i+1}{n-i+1}\binom{n}{i}, \quad v_j = \binom{h}{j}\binom{n-h}{j}.$$

В дальнейшем будем использовать схему Джонсона с параметром $h = (n-1)/2$.

2. Некоторые свойства центрированных функций

Функцию, заданную на вершинах n-куба и принимающую действительные значения, назовем K*-центрированной*, если сумма ее значений в вершинах любого шара радиуса 1 равна K.

Интерес к изучению центрированных функций определяется тем, что они являются естественным обобщением совершенных кодов с расстоянием 3. Действительно, характеристические функции таких кодов — это в точности все 1-центрированные функции в кубе соответствующей размерности, принимающие значения 0 и 1.

K-центрированная функция называется *тривиальной*, если она тождественно равна константе $K/(n+1)$.

Нетрудно убедиться в справедливости следующего утверждения.

Лемма 1. *Функция $f : E^n \to \mathbf{R}$ является K-центрированной тогда и только тогда, когда она является суммой тривиальной K-центрированной функции и некоторой 0-центрированной функции.*

В силу этого утверждения основное внимание в данной статье уделяется изучению 0-центрированных функций.

В [4] для совершенных кодов с расстоянием 3 была доказана теорема, которая в более общем виде во введенных терминах формулируется следующим образом.

Теорема 1. *Весовой спектр 0-центрированной функции f в n-кубе относительно произвольной вершины $\mathbf{x} \in E^n$ однозначно определяется ее значением в вершине $\mathbf{x}$, а его производящая функция имеет следующий вид:*

$$f(\mathbf{x})(1+t)^{(n-1)/2}(1-t)^{(n+1)/2}. \tag{8}$$

Доказательство этого факта почти дословно совпадает с рассуждениями из [4].

Следствие 1. *Если $f : E^n \to \mathbf{R}$ — нетривиальная 0-центрированная функция, то число n нечетно.*

Доказательство. По определению производящая функция весового спектра произвольной 0-центрированной функции относительно любой вершины $\mathbf{x}$ из n-куба является многочленом степени не более n. Из (8) следует, что при четном n это верно только в том случае, когда $f(\mathbf{x}) = 0$ для любой вершины $\mathbf{x} \in E^n$. Следствие 1 доказано.

В силу этого утверждения в дальнейшем без ограничения общности будем рассматривать только центрированные функции, заданные на кубах нечетных размерностей.

Пользуясь теоремой 1 и обобщая рассуждения из [5] для совершенных кодов с расстоянием 3 на центрированные функции, можно доказать следующее утверждение.

Теорема 2. *Функция $f : E^n \to \mathbf{R}$ является 0-центрированной тогда и только тогда, когда она принадлежит линейному пространству, базисом которого является система функций*

$$\{f^{\mathbf{a}} : E^n \to \mathbf{R} \mid f^{\mathbf{a}}(\mathbf{x}) = (-1)^{\langle \mathbf{a},\mathbf{x}\rangle}, \mathbf{x} \in A\}.$$

Рассмотрим такую функцию φ, определенную на среднем слое n-куба, что для любой вершины $\mathbf{a} \in A$ значение $\varphi(\mathbf{a})$ равно сумме значений функции f в $(n-1)/2$-мерной грани $\Gamma_{\mathbf{1}\oplus\mathbf{a}}$, т. е.

$$\varphi(\mathbf{a}) = \sum_{\mathbf{x}\in\Gamma_{\mathbf{1}\oplus\mathbf{a}}} f(\mathbf{x}). \tag{9}$$

Лемма 2. *Пусть f — произвольная 0-центрированная функция. Тогда для любой вершины $\mathbf{x} \in E^n$ выполняется равенство*

$$f(\mathbf{x}) = \frac{1}{2^{(n-1)/2}} \sum_{\mathbf{a} \in A} (-1)^{\langle \mathbf{a}, \mathbf{x} \rangle} \varphi(\mathbf{a}). \tag{10}$$

Доказательства двух последних утверждений почти дословно совпадают с рассуждениями для частного случая, относящегося к совершенным кодам [5]. Заметим, что, доопределяя функцию φ на всех вершинах $\mathbf{a} \in E^n \setminus A$ нулем, получим преобразование Фурье функции f с точностью до постоянного множителя.

3. Вспомогательные утверждения

В этом разделе доказываются две леммы, которые будут использованы при доказательстве основной теоремы 3 и ключевой леммы 5.

Для произвольной вершины $\mathbf{a} \in A$ пусть

$$t_j(\mathbf{a}, \mathbf{x}) = \sum_{\mathbf{b} \in A,\ g(\mathbf{a}, \mathbf{b}) = j} (-1)^{\langle \mathbf{b}, \mathbf{x} \rangle}.$$

Лемма 3. *Если $\mathbf{a} \in A$, $\mathbf{x} \in E^n$ и $j \leqslant (n-1)/2$, то*

$$t_j(\mathbf{a}, \mathbf{x}) = (-1)^{\langle \mathbf{a}, \mathbf{x} \rangle} P_j(\langle \mathbf{a}, \mathbf{x} \rangle; (n+1)/2)\ P_j(w(\mathbf{x}) - \langle \mathbf{a}, \mathbf{x} \rangle; (n-1)/2). \tag{11}$$

Доказательство. Заметим, что любую вершину среднего слоя, находящуюся на расстоянии Джонсона j от данной вершины $\mathbf{a} = (a_1, \ldots, a_n)$, можно получить, заменив j нулей в последовательности координат $(a_1, \ldots, a_n)$ на единицы и столько же единиц — на нули. Поэтому

$$\begin{aligned} t_j(\mathbf{a}, \mathbf{x}) &= \sum_{\mathbf{b} \in A,\ \rho(\mathbf{a}, \mathbf{b}) = 2j} (-1)^{\langle \mathbf{b}, \mathbf{x} \rangle} = \sum_{\mathbf{u} \in \Gamma_{\mathbf{a}} \cap W_j} \ \sum_{\mathbf{u}' \in \Gamma_{\mathbf{1} \oplus \mathbf{a}} \cap W_j} (-1)^{\langle \mathbf{a} \oplus \mathbf{u} \oplus \mathbf{u}', \mathbf{x} \rangle} \\ &= \sum_{\mathbf{u} \in \Gamma_{\mathbf{a}} \cap W_j} \ \sum_{\mathbf{u}' \in \Gamma_{\mathbf{1} \oplus \mathbf{a}} \cap W_j} (-1)^{\langle \mathbf{a}, \mathbf{x} \rangle - \langle \mathbf{u}, \mathbf{x} \rangle + \langle \mathbf{u}', \mathbf{x} \rangle} \\ &= (-1)^{\langle \mathbf{a}, \mathbf{x} \rangle} \Bigg(\sum_{\mathbf{u} \in \Gamma_{\mathbf{a}} \cap W_j} (-1)^{\langle \mathbf{u}, \mathbf{x} \rangle} \Bigg) \Bigg(\sum_{\mathbf{u}' \in \Gamma_{\mathbf{1} \oplus \mathbf{a}} \cap W_j} (-1)^{\langle \mathbf{u}', \mathbf{x} \rangle} \Bigg) \\ &= (-1)^{\langle \mathbf{a}, \mathbf{x} \rangle} r_j(\mathbf{a}, \mathbf{x}) r_j(\mathbf{1} \oplus \mathbf{a}, \mathbf{x}), \end{aligned}$$

где

$$r_j(\mathbf{y}, \mathbf{x}) = \sum_{\mathbf{v} \in \Gamma_{\mathbf{y}} \cap W_j} (-1)^{\langle \mathbf{v}, \mathbf{x} \rangle}.$$

Осталось вычислить величину $r_j(\mathbf{y},\mathbf{x})$ для произвольных вершин $\mathbf{x}$ и $\mathbf{y}$ из n-куба. Пусть $\mathbf{z} \in E^n$ — вершина максимального веса из пересечения граней $\Gamma_{\mathbf{x}}$ и $\Gamma_{\mathbf{y}}$. Это значит, что $w(\mathbf{z}) = \langle \mathbf{y},\mathbf{x}\rangle$ и для любой вершины $\mathbf{v}$ из грани $\Gamma_{\mathbf{y}}$ выполняется равенство $\langle \mathbf{v},\mathbf{x}\rangle = \langle \mathbf{v},\mathbf{z}\rangle$. Поэтому

$$r_j(\mathbf{y},\mathbf{x}) = \sum_{\mathbf{v}\in\Gamma_{\mathbf{y}}\cap W_j} (-1)^{\langle \mathbf{v},\mathbf{z}\rangle}.$$

Из свойств многочленов Кравчука [3] следует, что выражение в правой части равно $P_j(w(\mathbf{z}); w(\mathbf{y}))$. Подставив значение веса вершины $\mathbf{z}$, получим

$$r_j(\mathbf{y},\mathbf{x}) = P_j(\langle \mathbf{y},\mathbf{x}\rangle; w(\mathbf{y})).$$

Поэтому

$$t_j(\mathbf{a},\mathbf{x}) = (-1)^{\langle \mathbf{a},\mathbf{x}\rangle} \cdot P_j(\langle \mathbf{a},\mathbf{x}\rangle; w(\mathbf{a})) \cdot P_j(w(\mathbf{x}) - \langle \mathbf{a},\mathbf{x}\rangle; n - w(\mathbf{a})).$$

Из этого равенства следует (11). Лемма 3 доказана.

Теперь рассмотрим величины $d_i(n)$, где

$$d_i(n) = \sum_{k=0}^{(n-1)/2} (-1)^k E_k(i), \tag{12}$$

$n \geqslant 0$ нечетно, $0 \leqslant i \leqslant (n-1)/2$ и $E_k(i) = E_k(i;(n-1)/2, n)$ — значения многочленов Эберлейна. Смысл этих величин станет ясен при доказательстве леммы 5.

Лемма 4. *Пусть $n \geqslant 0$ нечетно и $0 \leqslant i \leqslant (n-1)/2$. Тогда величина $d_i(n)$ не равна нулю и*

$$d_i(n) = 2^i P_{(n-1)/2-i}((n+1)/2 - i; n-2i). \tag{13}$$

Доказательство. Пусть $h = (n-1)/2$. Сначала упростим формулу для вычисления значения $d_i(n)$, воспользовавшись формулой (4) для многочленов Эберлейна и соотношением $2h+1 = n$:

$$\begin{aligned} d_i(n) &= \sum_{k=0}^{h}(-1)^k \sum_{j=0}^{k}(-1)^{k-j}\binom{h-j}{k-j}\binom{h-i}{j}\binom{h+1-i+j}{j} \\ &= \sum_{j=0}^{h}\sum_{k=j}^{h}(-1)^{2k-j}\binom{h-j}{k-j}\binom{h-i}{j}\binom{h+1-i+j}{j} \\ &= \sum_{j=0}^{h}(-1)^j\binom{h-i}{j}\binom{h+1-i+j}{j}\sum_{k=j}^{h}\binom{h-j}{k-j} \\ &= \sum_{j=0}^{h}(-1)^j 2^{h-j}\binom{h-i}{j}\binom{h+1-i+j}{j}. \end{aligned} \tag{14}$$

Теперь найдем $d_0(n)$. Из (14) следует, что

$$d_0(n) = \sum_{j=0}^{h} (-1)^j 2^{h-j} \binom{h}{j} \binom{h+1+j}{j}.$$

Сравнивая это выражение с формулой (3) для многочленов Кравчука, видим, что величина $d_0(n)$ равна значению одного из них, а именно

$$d_0(n) = P_{(n-1)/2}((n+1)/2; n).$$

Наконец, покажем, что $d_i(n) = 2d_{i-1}(n-2)$. Из формулы (14) получаем, что

$$\begin{aligned} d_i(n) = \sum_{j=0}^{h-1} (-1)^j 2^{h-j} \binom{h-i}{j} \binom{h+1-i+j}{j} \\ + (-1)^h 2^{h-h} \binom{h-i}{h} \binom{n-i}{h} = 2d_{i-1}(n-2) + 0. \end{aligned}$$

Следовательно,

$$\begin{aligned} d_i(n) = 2d_{i-1}(n-2) = \ldots = 2^j d_{i-j}(n-2j) = \ldots \\ = 2^i d_0(n-2i) = 2^i P_{(n-1)/2-i}((n+1)/2 - i; n-2i). \end{aligned}$$

Из свойств многочленов Кравчука следует, что

$$P_{2t}((n+1)/2, n) = -P_{2t+1}((n+1)/2, n) = (-1)^t \binom{(n-1)/2}{t}.$$

(Для этого надо вспомнить, что производящая функция последовательности $P_k(x; N)$, $0 \leqslant k \leqslant N$, имеет вид $(1-t)^x(1+t)^{N-x}$, и преобразовать ее.) Следовательно, $d_i(n) \neq 0$. Лемма 4 доказана.

4. Основной результат

Введем в рассмотрение матрицы D и $\widetilde{D}$ следующим образом. Через D обозначим квадратную матрицу порядка $|A|$, строки и столбцы которой соответствуют вершинам среднего слоя, с элементами

$$D_{\mathbf{a},\mathbf{b}} = (-1)^{\langle \mathbf{a},\mathbf{b} \rangle}, \quad \mathbf{a}, \mathbf{b} \in A.$$

Определим прямоугольную матрицу $\widetilde{D}$ размера $2^n \times |A|$, подматрицей которой является матрица D. Строки матрицы $\widetilde{D}$ соответствуют всем вершинам n-куба, а столбцы — вершинам среднего слоя, элементы определены аналогично, т. е.

$$\widetilde{D}_{\mathbf{x},\mathbf{a}} = (-1)^{\langle \mathbf{a},\mathbf{x} \rangle}, \quad \mathbf{x} \in E^n, \ \mathbf{a} \in A.$$

Следующая лемма 5 является ключевой при доказательстве основной теоремы 3.

Лемма 5. *Пусть число n нечетно. Тогда квадратная матрица D невырождена, причем для любых вершин $\mathbf{a}, \mathbf{b} \in A$ элемент обратной матрицы, находящийся в строке, соответствующей вершине $\mathbf{a}$, и столбце, соответствующем вершине $\mathbf{b}$, однозначно определяется расстоянием Джонсона между этими вершинами*:

$$(D^{-1})_{\mathbf{a},\mathbf{b}} = \frac{1}{|A|} \sum_{i=0}^{(n-1)/2} \frac{q_i(g(\mathbf{a},\mathbf{b}))}{d_i}, \tag{15}$$

где числа $d_i = d_i(n)$ определены по формуле (12).

Доказательство. Если выписать в явном виде матрицу D^{-1}, то тем самым будет доказана невырожденность матрицы D.

Сначала заметим, что из определения матрицы D следует, что

$$D = \sum_{j=1}^{(n+1)/2} (-1)^j S_j,$$

где S_j — квадратная матрица порядка $|A|$, строки и столбцы которой соответствуют вершинам множества A, с элементами

$$(S_j)_{\mathbf{a},\mathbf{b}} = \begin{cases} 1, & \text{если } \langle \mathbf{a}, \mathbf{b} \rangle = j, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Легко видеть, что для любых вершин $\mathbf{a}, \mathbf{b} \in A$ выполняется соотношение $g(\mathbf{a}, \mathbf{b}) + \langle \mathbf{a}, \mathbf{b} \rangle = (n+1)/2$. Другое очевидное наблюдение состоит в том, что $g(\mathbf{a}, \mathbf{b}) = g(\mathbf{1} \oplus \mathbf{a}, \mathbf{1} \oplus \mathbf{b})$. Поэтому для любого j, $1 \leqslant j \leqslant (n+1)/2$, имеем

$$g(\mathbf{1} \oplus \mathbf{a}, \mathbf{1} \oplus \mathbf{b}) = (n+1)/2 - \langle \mathbf{a}, \mathbf{b} \rangle.$$

Поскольку для любых вершин $\mathbf{a}, \mathbf{b} \in A$ вершины $\mathbf{1} \oplus \mathbf{a}$ и $\mathbf{1} \oplus \mathbf{b}$ имеют вес $(n-1)/2$, из последней формулы следует, что

$$S_j = D_{(n+1)/2-j}, \quad 1 \leqslant j \leqslant (n+1)/2,$$

где D_i, $0 \leqslant i \leqslant (n-1)/2$, — матрицы инцидентности схемы Джонсона с параметром $h = (n-1)/2$.

Итак, имеем

$$D = \sum_{j=1}^{(n+1)/2} (-1)^j S_j = \sum_{j=1}^{(n+1)/2} (-1)^j D_{(n+1)/2-j} = \sum_{k=0}^{(n-1)/2} (-1)^k D_k.$$

Таким образом, матрица D является элементом алгебры Боуза — Меснера схемы отношений Джонсона с параметром $h = (n-1)/2$. Выразим

ее через идемпотенты J_i, $0 \leqslant i \leqslant (n-1)/2$, этой алгебры. Для этого воспользуемся соотношением (6):

$$D = \sum_{k=0}^{(n-1)/2} (-1)^k \sum_{i=0}^{(n-1)/2} E_k(i) J_i$$

$$= \sum_{i=0}^{(n-1)/2} \Bigg(\sum_{k=0}^{(n-1)/2} (-1)^k E_k(i) \Bigg) J_i = \sum_{i=0}^{(n-1)/2} d_i J_i,$$

где $E_k(i) = E_k(i;(n-1)/2, n)$ и числа $d_i = d_i(n)$ определены по формуле (12). Поскольку идемпотенты обладают свойствами (5) и по лемме 4 величины d_i, $0 \leqslant i \leqslant (n-1)/2$, не равны нулю, имеем

$$D^{-1} = \sum_{i=0}^{(n-1)/2} \frac{1}{d_i} J_i.$$

(В справедливости этого равенства можно убедиться, проверив, что произведение матриц D и D^{-1} является единичной матрицей.) Следовательно, матрица D невырождена.

Теперь с помощью соотношения (7) матрицу D^{-1} выразим через исходный базис, состоящий из матриц D_i, $0 \leqslant i \leqslant (n-1)/2$:

$$D^{-1} = \frac{1}{|A|} \sum_{i=0}^{(n-1)/2} \frac{1}{d_i} \sum_{j=0}^{(n-1)/2} q_i(j) D_j = \frac{1}{|A|} \sum_{j=0}^{(n-1)/2} D_j \Bigg(\sum_{i=0}^{(n-1)/2} \frac{q_i(j)}{d_i} \Bigg).$$

Использовав определение матриц инцидентности, получаем

$$(D^{-1})_{\mathbf{a},\mathbf{b}} = \frac{1}{|A|} \sum_{j=0}^{(n-1)/2} (D_j)_{\mathbf{a},\mathbf{b}} \Bigg(\sum_{i=0}^{(n-1)/2} \frac{q_i(j)}{d_i} \Bigg) = \frac{1}{|A|} \sum_{i=0}^{(n-1)/2} \frac{q_i(g(\mathbf{a},\mathbf{b}))}{d_i}.$$

Лемма 5 доказана.

Вернемся к рассмотрению центрированных функций. Оказывается, значение 0-центрированной функции f в произвольной вершине $\mathbf{x}$ из n-куба выражается линейно через ее значения во всех вершинах $\mathbf{a}$ среднего слоя, причем коэффициенты этой линейной комбинации однозначно определяются весом вершины $\mathbf{x}$ и расстоянием между вершинами $\mathbf{x}$ и $\mathbf{a}$ (или их скалярным произведением). В этом состоит смысл следующей основной теоремы.

Теорема 3. *Пусть число n нечетно. Значение 0-центрированной функции $f : E^n \to \mathbf{R}$ в произвольной вершине $\mathbf{x}$ из n-куба однозначно определяется значениями функции f на среднем слое этого куба, причем*

$$f(\mathbf{x}) = \sum_{l=0}^{(n+1)/2} \Bigg(\sum_{\mathbf{a} \in A, \langle \mathbf{a},\mathbf{x} \rangle = l} f(\mathbf{a}) \Bigg) \alpha(l, w(\mathbf{x})), \tag{16}$$

где

$$\alpha(l,w)=\frac{(-1)^l}{|A|}\sum_{i=0}^{(n-1)/2}\sum_{j=0}^{(n-1)/2} q_i(j) \times\frac{P_j(l;(n+1)/2)P_j(w-l;(n-1)/2)}{2^i P_{(n-1)/2-i}((n+1)/2-i;n-2i)}. \tag{17}$$

Доказательство. Сначала введем дополнительные обозначения. Через F обозначим вектор значений функции f во всех вершинах среднего слоя A, через $\widetilde{F}$ — вектор значений функции f во всех вершинах n-куба, а через Φ — вектор значений функции φ, определенной по формуле (9), в ее области определения A. Тогда по лемме 2 имеем

$$2^{-(n-1)/2}\widetilde{D}\Phi=\widetilde{F}. \tag{18}$$

В частности,

$$2^{-(n-1)/2}D\Phi=F. \tag{19}$$

В силу леммы 5 матрица D невырождена. Поэтому из (18) и (19) получаем

$$\widetilde{F}=HF,\qquad \text{где } H=\widetilde{D}D^{-1}. \tag{20}$$

Следовательно, вектор $\widetilde{F}$ однозначно определяется вектором F. Укажем теперь формулу для вычисления компонент вектора $\widetilde{F}$ через компоненты вектора F.

Воспользовавшись леммой 5, для произвольных вершин $\mathbf{x}\in E^n$ и $\mathbf{a}\in A$ вычислим элемент матрицы H, находящийся в строке, соответствующей вершине $\mathbf{x}$, и столбце, соответствующем вершине $\mathbf{a}$:

$$\begin{aligned}
H_{\mathbf{x},\mathbf{a}} &= \sum_{\mathbf{b}\in A}\widetilde{D}_{\mathbf{x},\mathbf{b}}(D^{-1})_{\mathbf{b},\mathbf{a}}=\frac{1}{|A|}\sum_{\mathbf{b}\in A}(-1)^{\langle\mathbf{b},\mathbf{x}\rangle}\sum_{i=0}^{(n-1)/2}\frac{q_i(g(\mathbf{a},\mathbf{b}))}{d_i}\\
&=\frac{1}{|A|}\sum_{i=0}^{(n-1)/2}\sum_{\mathbf{b}\in A}(-1)^{\langle\mathbf{x},\mathbf{b}\rangle}\frac{q_i(g(\mathbf{a},\mathbf{b}))}{d_i}\\
&=\frac{1}{|A|}\sum_{i=0}^{(n-1)/2}\sum_{j=0}^{(n-1)/2}\frac{q_i(j)}{d_i}\sum_{\mathbf{b}\in A,\,g(\mathbf{a},\mathbf{b})=j}(-1)^{\langle\mathbf{x},\mathbf{b}\rangle}\\
&=\frac{1}{|A|}\sum_{i=0}^{(n-1)/2}\sum_{j=0}^{(n-1)/2}\frac{q_i(j)t_j(\mathbf{a},\mathbf{x})}{d_i}.
\end{aligned}$$

Используя формулы (11) и (13), последнее выражение преобразуем к виду

$$\frac{(-1)^{\langle \mathbf{a},\mathbf{x}\rangle}}{|A|}\sum_{i=0}^{(n-1)/2}\sum_{j=0}^{(n-1)/2} q_i(j)\frac{P_j(\langle \mathbf{a},\mathbf{x}\rangle;(n+1)/2)P_j(w(\mathbf{x})-\langle \mathbf{a},\mathbf{x}\rangle;(n-1)/2)}{2^i P_{(n-1)/2-i}((n+1)/2-i;n-2i)}.$$

Следовательно, элемент $H_{\mathbf{x},\mathbf{a}}$ матрицы H однозначно определяется весом вершины $\mathbf{x}$ и скалярным произведением вершин $\mathbf{a}$ и $\mathbf{x}$. Наконец, применяя (20), запишем компоненты вектора $\widetilde{F}$:

$$\begin{aligned} f(\mathbf{x}) &= \sum_{\mathbf{a}\in A} H_{\mathbf{x},\mathbf{a}} f(\mathbf{a}) = \sum_{l=0}^{(n+1)/2}\sum_{\mathbf{a}\in A,\langle \mathbf{a},\mathbf{x}\rangle=l} H_{\mathbf{x},\mathbf{a}} f(\mathbf{a}) \\ &= \frac{1}{|A|}\sum_{l=0}^{(n+1)/2}(-1)^l\Bigg(\sum_{\mathbf{a}\in A,\ \langle \mathbf{a},\mathbf{x}\rangle=l} f(\mathbf{a})\Bigg) \\ &\times \sum_{i=0}^{(n-1)/2}\sum_{j=0}^{(n-1)/2} q_i(j)\frac{P_j(l;(n+1)/2)\ P_j(w(\mathbf{x})-l;(n-1)/2)}{2^i P_{(n-1)/2-i}((n+1)/2-i;n-2i)}. \end{aligned}$$

Теорема 3 доказана.

Утверждение теоремы 3 легко обобщить на K-центрированные функции, когда $K\neq 0$. В этом случае из леммы 1 и теоремы 3 получаем

Следствие 2. *Пусть число n нечетно. Значение K-центрированной функции $f: E^n\to \mathbf{R}$ в произвольной вершине $\mathbf{x}$ из n-куба однозначно определяется значениями функции f на среднем слое этого куба, причем*

$$f(\mathbf{x}) = \frac{K}{n+1} + \sum_{l=0}^{(n+1)/2}\Bigg(\sum_{\mathbf{a}\in A,\langle \mathbf{a},\mathbf{x}\rangle=l}\Big(f(\mathbf{a})-\frac{K}{n+1}\Big)\Bigg)\alpha(l,w(\mathbf{x})), \qquad (21)$$

где значения $\alpha(l,w)$ определяются из формулы (17).

В частности, если f является 1-центрированной функцией со значениями из множества $\{0,1\}$, то f является характеристической функцией совершенного кода [5], и формула (21) позволяет восстановить все значения этой функции по ее значениям на среднем слое. Применив следствие 2 к таким функциям, в терминах подмножеств n-куба получаем

Следствие 3. *Пусть $B\subset A$. Если существует такой совершенный код C_B с расстоянием 3, что $C_B\cap A = B$, то этот код единствен,*

причем произвольная вершина $\mathbf{x}$ *из* n*-куба принадлежит коду* C_B *тогда и только тогда, когда выполняется равенство*

$$(n+1)\sum_{l=0}^{(n+1)/2}\alpha(l,w(\mathbf{x}))|\{\mathbf{a}\in B\mid\langle\mathbf{a},\mathbf{x}\rangle=l\}| \\ = n+\sum_{l=0}^{(n+1)/2}\alpha(l,w(\mathbf{x}))\binom{w(\mathbf{x})}{l}\binom{(n+1)/2-w(\mathbf{x})}{n-l},$$

где значения $\alpha(l,w)$ *определяются из формулы* (17).

Пусть $\phi : A \to \mathbf{R}$ — произвольная функция, и пусть $f^\phi : E^n \to \mathbf{R}$ — функция, получающаяся подстановкой в правую часть формулы (21) значений $\phi(\mathbf{a}), \mathbf{a} \in A$. При доказательстве теоремы 3 на самом деле получено следующее более сильное утверждение, справедливость которого становится очевидной при подробном рассмотрении приведенного выше доказательства.

Следствие 4. *Функция* f^ϕ *является* K*-центрированной, и в вершинах среднего слоя* n*-куба ее значения совпадают со значениями функции* ϕ.

Иначе говоря, если задать функцию на среднем слое произвольным образом и продолжить ее на весь n-куб по формуле (21), то получим K-центрированную функцию. В частности, можно задать значения этой функции таким образом, что в некоторой вершине $\mathbf{a} \in A$ она будет принимать значение 1, а в остальных вершинах среднего слоя — значение 0, и продолжить ее до 0-центрированной функции. Различные 0-центрированные функции такого вида (различающиеся выбором вершины среднего слоя, в которой значение функции полагается равным 1) являются линейно независимыми, их число совпадает с размерностью пространства всех 0-центрированных функций, Значит, они образуют базис этого пространства. Из формулы (16) получаем, что эти функции имеют следующий вид:

$$f_{\mathbf{a}}(\mathbf{x}) = \alpha(\langle\mathbf{a},\mathbf{x}\rangle, w(\mathbf{x})), \quad \mathbf{a}\in A,\ \mathbf{x}\in E^n,$$

где значения α определяются из формулы (17).

Следствие 5. *Множество функций* $\{f_{\mathbf{a}}(\mathbf{x}) \mid \mathbf{a} \in A\}$ *является базисом пространства всех* 0*-центрированных функций.*

ЛИТЕРАТУРА

1. **Августинович С. В.** Об одном свойстве совершенных двоичных кодов // Дискрет. анализ и исслед. операций. 1995. Т. 2. № 1. С. 4–6.
2. **Августинович С. В., Васильева А. Ю.** О восстановлении центрированной функции // Междунар. конф. «Дискретный анализ и исследование операций». Материалы конференции (Новосибирск, 26 июня – 1 июля 2000). Новосибирск: Изд-во Ин-та математики, 2000. С. 65.
3. **Дельсарт Ф.** Алгебраический подход к схемам отношений теории кодирования. М.: Мир, 1976.
4. **Ллойд С. П.** Бинарное блочное кодирование // Кибернетический сборник. Вып. 1. М.: Изд-во иностр. лит., 1960. С. 206–226.
5. **Vasil'eva A. Yu.** A representation of perfect binary codes // Algebraic and combinatorial coding theory. Seventh Intern. Workshop (Bansko, 18–24 June, 2000). Proc. Bulgaria: Inst. of Math. and Inform., 2000. P. 311–315.

Адрес авторов:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия.
E-mail: avgust@math.nsc.ru
vasilan@math.nsc.ru

Статья поступила
27 февраля 2002 г.