Сибирский математический журнал
Май—июнь, 2008. Том 49, № 3

УДК 519.719.1

ТЕОРЕМЫ ВОССТАНОВЛЕНИЯ ДЛЯ ЦЕНТРИРОВАННЫХ ФУНКЦИЙ И СОВЕРШЕННЫХ КОДОВ

С. В. Августинович, А. Ю. Васильева

Аннотация. Объект изучения — центрированные функции и совершенные коды в пространстве всех двоичных наборов длины n. Доказано, что все значения центрированной функции в шаре радиуса $k \leq (n+1)/2$ однозначно определены ее радиальными суммами относительно вершин соответствующей сферы. Приведены теоремы полного и частичного восстановления центрированной функции по части ее значений. Получено новое свойство групп симметрий центрированных функций.

Ключевые слова: центрированные функции, совершенные коды, дискретное преобразование Фурье.

При изучении математических объектов часто возникает вопрос точного указания объекта из заданного класса по его свойствам или частям, т. е. вопрос восстановления объекта. В настоящей статье этот вопрос рассматривается для класса центрированных функций, заданных на пространстве всех двоичных наборов фиксированной длины, т. е. таких функций, что сумма значений каждой из них во всех шарах радиуса 1 постоянна. В частности, в этот класс включаются и столь важные дискретные объекты, как совершенные двоичные коды с расстоянием 3 (т. е. исправляющие одну ошибку).

Известно [1–3], что центрированная функция полностью определяется своими значениями в вершинах веса $(n+1)/2$. Более того, все значения центрированной функции в шаре радиуса $k \leq (n+1)/2$ (где n — размерность пространства) однозначно определяются ее значениями в вершинах соответствующей сферы [4]. В настоящей статье доказана теорема об однозначной определенности всех значений центрированной функции в шаре радиуса $k \leq (n+1)/2$ (где n — размерность пространства) ее радиальными суммами относительно вершин соответствующей сферы, т. е. суммами значений в минимальных гранях, каждая из которых содержит одну вершину сферы и ее центр (теорема 3). Кроме того, приведены теорема об однозначной определенности всех значений центрированной функции в шаре ее значениями на соответствующей сфере (теорема 2) и теорема об однозначной определенности центрированной функции ее значениями на сфере радиуса $k \leq (n+1)/2$ (теорема 1). Как следствие, получено новое свойство групп симметрий центрированных функций (теорема 4), а значит, и совершенных кодов.

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (код проекта 07–01–00248–а), а также Новосибирского гос. университета.

1. Предварительные сведения

Будем обозначать через E^n и называть *булевым кубом* множество всех двоичных наборов длины n. В этом пространстве будем рассматривать метрику Хэмминга, в которой расстояние $\rho(\mathbf{x},\mathbf{y})$ между двумя вершинами $\mathbf{x}$ и $\mathbf{y}$ равно числу позиций, в которых они различаются. Под *скалярным произведением* $\langle \mathbf{x},\mathbf{y}\rangle$ вершин $\mathbf{x}$ и $\mathbf{y}$ будем понимать число позиций, в которых обе вершины имеют единицы. *Весом Хэмминга* $wt(\mathbf{x})$ вершины $\mathbf{x}$ называем число ненулевых позиций $\mathbf{x}$; через W_k будем обозначать множество всех вершин веса k, которое будем называть *k-м слоем* булева куба. В случае, когда n — размерность куба — является нечетным числом, слои $W_{(n-1)/2}$ и $W_{(n+1)/2}$ называем *средними*. В булевом кубе обычным образом определяем частичный порядок: $\mathbf{x} = (x_1,\dots,x_n) \preceq \mathbf{y} = (y_1,\dots,y_n)$, если $x_i \le y_i$ для всех $i = 1,2,\dots,n$.

Хорошо известно (см., например, [5]), что произвольная функция $f : E^n \to \mathbb{R}$ может быть представлена с помощью своих коэффициентов Фурье

$$f(\mathbf{x}) = \frac{1}{2^n}\sum_{\mathbf{a}\in E^n}(-1)^{\langle \mathbf{a},\mathbf{x}\rangle}\hat{f}(\mathbf{a}), \tag{1}$$

где

$$\hat{f}(\mathbf{a}) = \sum_{\mathbf{x}\in E^n}(-1)^{\langle \mathbf{a},\mathbf{x}\rangle}f(\mathbf{x}), \quad \mathbf{a}\in E^n.$$

Из этого следует, что система функций

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

образует базис пространства всех действительнозначных функций, заданных на булевом кубе.

Совершенным двоичным кодом длины n с расстоянием 3 называется такое подмножество вершин булева куба, что шары радиуса 1 с центрами в кодовых вершинах не пересекаются и покрывают весь куб. Функция $f : E^n \to \mathbb{R}$ называется *ϑ-центрированной*, если в каждом шаре радиуса 1 сумма ее значений равна ϑ. Легко заметить, что характеристическая функция χ_C совершенного кода C является 1-центрированной, а функция $\chi_C - 1/(n+1)$ — 0-центрированной. Вообще, произвольная функция f ϑ-центрированна тогда и только тогда, когда функция $f - \vartheta/(n+1)$ является 0-центрированной. Про функцию $f(\mathbf{x}) = \vartheta/(n+1)$ будем говорить, что она является *тривиальной ϑ-центрированной функцией*. Отметим (см. [2]), что нетривиальные ϑ-центрированные функции $f : E^n \to \mathbb{R}$ существуют тогда и только тогда, когда размерность n булева куба нечетна.

Положим по определению

$$v_i = \sum_{\mathbf{x}\in W_i} f(\mathbf{x})$$

и назовем вектор $v = (v_0, v_1,\dots,v_n)$ *весовым спектром* функции f. Аналогично случаю совершенных кодов нетрудно показать, что весовой спектр произвольной ϑ-центрированной функции однозначно определяется своей начальной компонентой $v_0 = f(\mathbf{0})$.

Отметим также [2], что множество всех 0-центрированных функций совпадает с одним из собственных подпространств матрицы смежности булева куба. Точнее, это подпространство, базисом которого является множество функций

$$\{f^{\mathbf{a}} : E^n \to \mathbb{R} \mid f^{\mathbf{a}}(\mathbf{x}) = (-1)^{\langle \mathbf{a},\mathbf{x}\rangle},\ \mathbf{a}\in W_{(n+1)/2}\}.$$

Везде в дальнейшем, не оговаривая особо, мы рассматриваем только 0-центрированные функции на гиперкубе.

2. Теоремы восстановления

Для произвольного $\mathbf{a} \in W_k$ определим *радиальную сумму* $S_{\mathbf{a}}$ функции f относительно вершины $\mathbf{a}$ следующим образом:

$$S_{\mathbf{a}} = \sum_{\mathbf{x} \preceq \mathbf{a}} f(\mathbf{x}). \tag{2}$$

Ранее мы видели, что коэффициенты Фурье $\hat{f}(\mathbf{a})$ произвольной 0-центрированной функции f могут быть ненулевыми только в том случае, когда $wt(\mathbf{a}) = (n+1)/2$ и для любой вершины $\mathbf{a} \in W_{(n+1)/2}$ соответствующий ей коэффициент Фурье равен (с точностью до константы) радиальной сумме относительно вершины, антиподальной к данной:

$$\hat{f}(\mathbf{a}) = 2^{(n+1)/2} S_{\mathbf{1} \oplus \mathbf{a}}.$$

Учитывая это соотношение, получим частный вид формулы преобразования Фурье (1) в случае 0-центрированных функций.

Предложение 1. *Пусть n нечетно, f — произвольная 0-центрированная функция и $i \le n$. Тогда для произвольной вершины $\mathbf{x} \in W_i$ выполняется*

$$f(\mathbf{x}) = \frac{(-1)^i}{2^{(n-1)/2}} \sum_{\mathbf{b} \in W_{(n-1)/2}} (-1)^{\langle \mathbf{b}, \mathbf{x} \rangle} S_{\mathbf{b}}. \tag{3}$$

В [6] доказано, что произвольный совершенный код однозначно определяется своим пересечением со средним слоем булева куба, т. е. всеми своими вершинами веса $(n-1)/2$. Теорема 1 обобщает этот факт и утверждает, что произвольная 0-центрированная функция однозначно определяется своими значениями во всех вершинах среднего слоя. Более того, найдена формула, в соответствии с которой все значения такой функции можно вычислить по значениям в вершинах среднего слоя. Эта формула представлена в терминах значений многочленов Кравчука $K_j(x, N)$ и Эберлейна $E_j(x; h, N)$ (см., например, [5]).

Теорема 1. *Пусть n нечетно и f — произвольная 0-центрированная функция. Тогда функция f однозначно определяется своими значениями в вершинах веса $(n+1)/2$. Более того, для любого h, $0 \le h \le n$, и произвольного $\mathbf{x} \in W_h$ выполнено*

$$f(\mathbf{x}) = \sum_{l=0}^{(n+1)/2} \Big(\sum_{\substack{\mathbf{a} \in W_{(n+1)/2}, \\ \langle \mathbf{a}, \mathbf{x} \rangle = l}} f(\mathbf{a}) \Big) \alpha(l, h), \tag{4}$$

где

$$\begin{aligned} \alpha(l,h) = \frac{(-1)^l}{|W_{(n+1)/2}|} \sum_{i=0}^{(n-1)/2} \sum_{j=0}^{(n-1)/2} \frac{n-2i+1}{n-i+1} \frac{\binom{n}{i}}{\binom{(n-1)/2}{j}\binom{(n+1)/2}{j}} \\ \times E_j(i; (n-1)/2, n) \frac{K_j(l; (n+1)/2) K_j(h-l; (n-1)/2)}{2^i K_{(n-1)/2-i}((n+1)/2 - i; n-2i)}. \end{aligned} \tag{5}$$

Какова будет картина, если нам известны все значения центрированной функции в вершинах некоторого слоя, не совпадающего со средним? Оказывается, возможно обобщение предыдущей теоремы, однако теперь мы сможем восстановить не всю функцию, а лишь часть ее значений.

Теорема 2 [4]. *Пусть n нечетно, $k \le (n+1)/2$ и f — произвольная* 0*-центрированная функция. Тогда все значения функции f в вершинах веса не более k однозначно определяются значениями f во всех вершинах веса k.*

Так же, как в случае полного восстановления 0-центрированной функции, можно указать формулу для прямого вычисления значений в вершинах веса менее k по ее значениям в вершинах веса k. Эта формула представлена в [7].

В настоящей статье будет доказана следующая

Теорема 3. *Пусть n нечетно, $k \le (n-1)/2$ и f — произвольная* 0*-центрированная функция. Тогда по значениям k-радиальных сумм функции f относительно всех вершин веса k однозначно определяются значения f во всех вершинах веса не более k. Более того, для любого $\mathbf{x} \in W_i$ выполнено*

$$f(\mathbf{x}) = (-1)^i \sum_{l=0}^{i} \Big(\sum_{\substack{\mathbf{b} \in W_k, \\ \langle \mathbf{b}, \mathbf{x} \rangle = l}} S_{\mathbf{b}} \Big) \left(\sum_{j=0}^{i} \frac{(-1)^j \binom{l}{j}}{2^{k-j} \binom{(n-1)/2-j}{k-j}} \right). \tag{6}$$

Эта теорема обобщает известную формулу (3) преобразования Фурье для частного случая 0-центрированных функций. Действительно, при $k = (n-1)/2$ формула (6) приобретает вид (3). Теорема 3 будет доказана в п. 4.

Заметим, что теорему 3 можно распространить на так называемые собственные функции преобразования Лапласа. Функцию f, заданную на пространстве E^n, будем называть *собственной функцией преобразования Лапласа* с собственным числом λ, если для всех $\mathbf{x} \in E^n$ выполнено условие

$$\sum_{\mathbf{y} \in S_1(\mathbf{x})} f(\mathbf{y}) = \lambda f(\mathbf{x}),$$

где $S_1(\mathbf{x})$ — сфера радиуса 1 с центром в вершине $\mathbf{x}$. Очевидно, что произвольная 0-центрированная функция является собственной функцией преобразования Лапласа с собственным числом $\lambda = -1$. Для функций такого вида верен аналог основной теоремы, при этом изменения в формуле затрагивают только биномиальный коэффициент, стоящий в знаменателе дроби под второй суммой. Доказательство дословно повторяет доказательство теоремы 3.

3. Группы симметрий

Рассмотрим произвольную функцию $f : E^n \to \mathbb{R}$ и целое $k \in \{0, 1, \ldots, n\}$. Будем говорить, что множество перестановок

$$\mathrm{Sim}_k(f) = \{\pi \in S_n \mid f(\mathbf{x}) = f(\pi(\mathbf{x})),\ \mathbf{x} \in W_k\}$$

является *группой симметрий функции f в k-м слое булева куба.* Легко проверить, что $\mathrm{Sim}_k(f)$ действительно является группой. Аналогичным образом определим *группу симметрий произвольного кода C в k-м слое булева куба*: это множество перестановок

$$\mathrm{Sim}_k(C) = \{\pi \in S_n \mid \mathbf{x} \in C \Leftrightarrow \pi(\mathbf{x}) \in C,\ \mathbf{x} \in W_k\}.$$

Следующее утверждение вытекает из теоремы 1.

Теорема 4. *Пусть n нечетно и f — произвольная* 0*-центрированная функция. Тогда*

$$\mathrm{Sim}_0(f) \ge \mathrm{Sim}_1(f) \ge \cdots \ge \mathrm{Sim}_{(n-1)/2}(f).$$

Частным случаем является следующее аналогичное утверждение о совершенных кодах.

Следствие 1. *Пусть n нечетно и C — произвольный совершенный код длины n. Тогда*

$$\mathrm{Sim}_0(C) \geq \mathrm{Sim}_1(C) \geq \cdots \geq \mathrm{Sim}_{(n-1)/2}(C).$$

Таким образом, оказывается, что для произвольных $i \leq j \leq (n-1)/2$ группа симметрий 0-центрированной функции (совершенного кода) в j-м слое вложена в группу симметрий этой функции (этого кода) в i-м слое.

4. Доказательство основной теоремы

В случае частично упорядоченного множества вершин булева куба известная формула обращения Мёбиуса (см., например, [8]) принимает следующий вид.

Лемма 1. *Пусть $f : E^n \to \mathbb{R}$ — произвольная функция. Тогда для произвольного $\mathbf{x} \in W_i$ выполняется*

$$f(\mathbf{x}) = (-1)^i \sum_{\mathbf{a} \preceq \mathbf{x}} (-1)^{\langle \mathbf{a},\mathbf{x}\rangle} S_{\mathbf{a}}. \tag{7}$$

Предыдущая лемма верна для всех действительнозначных функций. Далее будем рассматривать только центрированные функции и найдем соотношения между различными радиальными суммами такой функции.

Лемма 2. *Пусть n нечетно, $k \leq (n-1)/2$ и $f : E^n \to \mathbb{R}$ — произвольная 0-центрированная функция. Тогда для любого $\mathbf{a} \in W_i$, $0 \leq i \leq k$, выполняется*

$$S_{\mathbf{a}} = \frac{1}{2^{k-i}\binom{(n-1)/2-i}{k-i}} \sum_{\substack{\mathbf{b} \succeq \mathbf{a},\\ \mathbf{b} \in W_k}} S_{\mathbf{b}}. \tag{8}$$

Доказательство. Проведем доказательство обратной индукцией по i, $i = k, k-1, \ldots, 1, 0$.

База индукции. Пусть $i = k$. Тогда формула (8) принимает вид равенства $S_{\mathbf{a}} = S_{\mathbf{a}}$.

Предположим, что формула (8) верна для любой вершины веса $i+1$, и докажем ее для произвольной вершины $\mathbf{a}$ веса i. По определению 0-центрированной функции имеем

$$\sum_{\mathbf{x} \preceq \mathbf{a}} \sum_{\mathbf{y} \in B_1(\mathbf{x})} f(\mathbf{y}) = 0,$$

где через $B_1(\mathbf{x})$ обозначен шар радиуса 1 с центром в вершине $\mathbf{x}$.

С другой стороны, по определению радиальной суммы

$$\sum_{\mathbf{x} \preceq \mathbf{a}} \sum_{\mathbf{y} \in B_1(\mathbf{x})} f(\mathbf{y}) = (i+1)S_{\mathbf{a}} + \sum_{\substack{\mathbf{a}' \in W_{i+1},\\ \mathbf{a}' \succeq \mathbf{a}}} (S_{\mathbf{a}'} - S_{\mathbf{a}}) = \sum_{\substack{\mathbf{a}' \in W_{i+1},\\ \mathbf{a}' \succeq \mathbf{a}}} S_{\mathbf{a}'} - (n-2i-1)S_{\mathbf{a}}.$$

Поэтому

$$S_{\mathbf{a}} = \frac{1}{n-2i-1} \sum_{\substack{\mathbf{a}' \in W_{i+1},\\ \mathbf{a}' \succeq \mathbf{a}}} S_{\mathbf{a}'}.$$

Используя предположение индукции, из последней формулы получим

$$S_{\mathbf{a}} = \frac{1}{2((n-1)/2-i)} \sum_{\substack{\mathbf{a}'\in W_{i+1},\\ \mathbf{a}'\succeq\mathbf{a}}} \frac{1}{2^{k-i-1}\binom{(n-1)/2-i-1}{k-i-1}} \sum_{\substack{\mathbf{b}\in W_k,\\ \mathbf{b}\succeq\mathbf{a}'}} S_{\mathbf{b}}$$

$$= \frac{1}{2((n-1)/2-i)2^{k-i-1}\binom{(n-1)/2-i-1}{k-i-1}} \sum_{\substack{\mathbf{b}\in W_k,\\ \mathbf{b}\succeq\mathbf{a}}} (k-i)S_{\mathbf{b}}.$$

Это выражение нетрудно привести к виду (8), что завершает доказательство леммы.

Теперь перейдем непосредственно к доказательству теоремы 3. По формуле Мёбиуса (лемма 1)

$$f(\mathbf{x}) = (-1)^i \sum_{j=0}^{i} (-1)^j \sum_{\substack{\mathbf{a}\in W_j,\\ \mathbf{a}\preceq\mathbf{x}}} S_{\mathbf{a}}.$$

Подставляя выражение (8) для $S_{\mathbf{a}}$ в эту формулу, имеем

$$f(\mathbf{x}) = (-1)^i \sum_{j=0}^{i} \frac{(-1)^j}{2^{k-i}\begin{pmatrix}(n-1)/2-j\\ k-j\end{pmatrix}} \sum_{\substack{\mathbf{a}\in W_j,\\ \mathbf{a}\preceq\mathbf{x}}} \sum_{\substack{\mathbf{b}\in W_k,\\ \mathbf{b}\succeq\mathbf{a}}} S_{\mathbf{b}}.$$

Непосредственным вычислением получаем

$$\sum_{\substack{\mathbf{a}\in W_j,\\ \mathbf{a}\preceq\mathbf{x}}} \sum_{\substack{\mathbf{b}\in W_k,\\ \mathbf{b}\succeq\mathbf{a}}} S_{\mathbf{b}} = \sum_{\mathbf{b}\in W_k} \begin{pmatrix}\langle\mathbf{x},\mathbf{b}\rangle\\ j\end{pmatrix} S_{\mathbf{b}}.$$

Отсюда

$$f(\mathbf{x}) = (-1)^i \sum_{j=0}^{i} \frac{(-1)^j}{2^{k-i}\binom{(n-1)/2-j}{k-j}} \sum_{l=0}^{i} \begin{pmatrix}l\\ j\end{pmatrix} \sum_{\substack{\mathbf{b}\in W_k,\\ \langle\mathbf{x},\mathbf{b}\rangle=l}} S_{\mathbf{b}}.$$

Теперь осталось изменить порядок суммирования, чтобы получить требуемую формулу (6).

Авторы благодарят Д. С. Кротова за ценные замечания.

ЛИТЕРАТУРА

1. *Августинович С. В., Васильева А. Ю.* О восстановлении центрированной функции // Материалы междунар. конф. «Дискретный анализ и исследование операций», Новосибирск, Россия, 26 июня — 1 июля 2000. Новосибирск: Изд-во Ин-та математики СО РАН, 2000. С. 64.
2. *Августинович С. В., Васильева А. Ю.* Вычисление центрированной функции по ее значениям на средних слоях булева куба // Дискретный анализ и исследование операций. Сер. 1. 2003. Т. 10, № 2. С. 3–16.
3. *Heden O.* On the reconstruction of perfect codes // Discrete Math. 2002. V. 256, N 1. P. 479–485.
4. *Avgustinovich S. V., Vasil'eva A. Yu.* Testing sets for 1-perfect codes // Lecture Notes in Comput. Sci. 2006. V. 4123, November. P. 938–940.
5. *Delsarte P.* An algebraic approach to the association schemes of coding theory // Philips Res. Rep. Suppl. 1973. N 10.
6. *Августинович С. В.* Об одном свойстве совершенных двоичных кодов // Дискретный анализ и исследование операций. 1995. Т. 2, № 1. С. 4–6.

7. *Vasil'eva A. Yu.* Partial reconstruction of perfect binary codes // Proc. of Intern. Workshop on Coding and Cryptography, March 24–28, 2003, Versailles, France. P. 445–452.
8. *Холл М.* Комбинаторика. М.: Мир, 1970.

Статья поступила 28 декабря 2006 г.

Августинович Сергей Владимирович, Васильева Анастасия Юрьевна
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
avgust@math.nsc.ru, vasilan@math.nsc.ru