ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2010. Том 17, № 5. С. 15–21

УДК 519.725

О ВОССТАНОВЛЕНИИ ДВОИЧНЫХ КОДОВ ПО РАЗМЕРНОСТЯМ ИХ ПОДКОДОВ *)

Е. В. Горкунов, С. В. Августинович

Аннотация. Доказано, что для восстановления произвольного двоичного кода с точностью до эквивалентности достаточно знать размерности всех его подкодов чётной мощности. Показано, что теорема носит неулучшаемый характер.

Ключевые слова: код, сильная изометрия кодов, эквивалентность кодов.

Введение

Пусть два произвольных двоичных кода C_1 и C_2 имеют одинаковые мощность и длину n. Отображение $I\colon C_1 \to C_2$ называется *сильной изометрией*, если для каждого $B \subseteq C_1$ выполняется равенство

$$\mathrm{Dim}(B) = \mathrm{Dim}(I(B)), \tag{1}$$

где $\mathrm{Dim}(B)$ — размерность минимальной грани двоичного куба E^n, содержащей код B. Отображение I назовём *полусильной изометрией*, если равенство (1) имеет место для всех подкодов $B \subseteq C_1$ чётной мощности. Заметим, что $\mathrm{Dim}\{x, y\} = d(x, y)$, где $d(x, y)$ — расстояние Хэмминга между $x, y \in E^n$, измеряемое числом координат, в которых эти векторы различаются. Таким образом, выполнение (1) для всех подкодов мощности 2 означает, что и сильные, и полусильные изометрии являются изометриями в обычном смысле.

Обычно проблема жёсткости кодов формулируется как проблема продолжения изометрии пары кодов до эквивалентности [5, 9]. В настоящей статье исследуется несколько иная постановка. Код называется *метрически жёстким*, если он однозначно (вариант — с точностью до эквивалентности) восстанавливается по некоторому набору своих метрических

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 10–01–00616), а также Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429).

инвариантов. В качестве инвариантов могут выступать следующие: набор попарных расстояний [3] между кодовыми вершинами; граф минимальных расстояний [5, 9]; граф вершин, находящихся на фиксированном растоянии p друг от друга [6]; попарные расстояния между тройками вершин, которые выражаются в виде троек соответствующих натуральных чисел [1]. Наиболее сильным инвариантом оказался [4] набор размерностей подкодов кода. Исследование, изложенное ниже, показывает, что этот инвариант избыточен. Именно, для однозначного восстановления двоичного кода достаточно знать размерности только подкодов чётной мощности. Примеры, приведённые в конце статьи, показывают, что этот набор размерностей минимален.

1. Полусильные изометрии двоичных кодов

Рассмотрим пару двоичных кодов одинаковых мощности и длины. В [4] доказано, что всякая сильная изометрия между такими кодами продолжается до изометрии всего пространства. В частности, это означает, что сильно изометричные коды эквивалентны. Целью настоящей статьи является усиление результатов, полученных в [4].

Теорема 1. *Произвольная полусильная изометрия двоичных кодов продолжается до изометрии булева куба.*

Очевидным образом из этой теоремы вытекает

Следствие 1. *Полусильно изометричные двоичные коды эквивалентны.*

Для доказательства теоремы 1 понадобится один факт о восстановлении функции по известным суммам её значений. Этот факт удобно сформулировать на языке графов. Предположим, что $G = (V, E)$ — произвольный связный граф, на вершинах которого задана *весовая функция* $\omega\colon V \to \mathbb{N}$, а по ней построена *рёберная весовая функция* $\varphi_\omega\colon E \to \mathbb{N}$ по правилу $\varphi_\omega(e) = \omega(u) + \omega(v)$, где $e = (u, v) \in E$.

Лемма 1. *Если связный граф содержит нечётный цикл, то его весовая функция однозначно вычисляется по рёберной весовой функции.*

Доказательство. Действительно, пусть φ — рёберная весовая функция простого нечётного цикла $(v_0, v_1, \ldots, v_{k-1})$. В этом случае справедлива формула

$$\omega(v_j) = \frac{1}{2} \sum_{s=j}^{k-1+j} (-1)^{s+j} \varphi(v_s, v_{s+1}), \quad j = 0, 1, \ldots, k-1, \tag{2}$$

в которой индексы s и $s+1$ необходимо брать по модулю k. Таким образом, если в графе G найдётся нечётный цикл, то значения весовой функции в вершинах этого цикла легко находятся по формуле (2). Поскольку граф связен, для всякой его вершины, в частности, вес которой неизвестен, существует простая цепь, соединяющая эту вершину с одной из вершин рассмотренного нечётного цикла. Вдоль этой цепи значения весовой функции ω легко определяются по её известному значению на цикле и значениям функции φ на рёбрах цепи. Лемма 1 доказана.

Рассмотрим двоичный код C. Сопоставим его кодовой $(k \times n)$-матрице M функцию $\omega\colon E^k \to \mathbb{N}$ такую, что для $\alpha \in E^k$ значение $\omega(\alpha)$ равно числу вхождений столбца α^{T} в матрицу M. Функцию ω назовём *характеристической функцией кода* C (матрицы M). Заметим, что таким образом коду C соответствует множество характеристических функций, однако справедлива

Лемма 2. *Всякий двоичный код задаётся своей характеристической функцией с точностью до перестановки координат.*

Доказательством этой леммы может служить очевидное замечание, что при перестановке столбцов матрицы M её характеристическая функция остаётся неизменной.

Далее, пусть между кодами C_1 и C_2 из E^n имеется полусильная изометрия I, т. е. $I(C_1) = C_2$. Поскольку группа автоморфизмов булева куба транзитивна, для доказательства теоремы 1 достаточно рассмотреть коды, содержащие нулевой вектор 0, причём без ограничения общности положим $I(0) = 0$. Обозначим через M_1 и M_2 кодовые матрицы кодов C_1 и C_2 соответственно, а через ω_1 и ω_2 — их характеристические функции. Для простоты будем предполагать, что первые строки этих матриц нулевые и отображение I сопоставляет каждой строке матрицы M_1 соответствующую строку матрицы M_2. Поскольку по предположению $I(0) = 0$, продолжением полусильной изометрии I до изометрии булева куба E^n может служить только некоторая перестановка $\pi \in S_n$, действующая на позициях координат кодовых слов. Отсюда с учётом леммы 2 получаем, что полусильная изометрия I продолжается до изометрии булева куба E^n тогда и только тогда, когда $\omega_1 \equiv \omega_2$.

Таким образом, доказательство теоремы 1 сводится к вопросу об однозначном восстановлении характеристической функции ω произвольного приведённого кода $C \in E^n$ по набору известных размерностей подкодов чётной мощности, содержащихся в C. При этом поскольку код приведённый, $\omega(\alpha) \equiv 0$ в грани $\alpha_0 = 1$ куба E^k. Также стоит отметить,

что результаты, полученные в [4], позволяют однозначно восстановить эту функцию, если известны размерности всех подкодов кода C.

Теорема 2 [4]. *Произвольный приведённый двоичный код по набору размерностей всех своих подкодов восстанавливается с точностью до перестановки координат.*

Для исследования восстановимости ω по размерностям чётных подкодов введём некоторые обозначения. Пусть код $C \subseteq E^n$ имеет мощность k. Строки матрицы M, а также координаты векторов из E^k будем нумеровать числами от 0 до $k-1$. Положим $K = \{0, \ldots, k-1\}$. Для произвольного $S \subseteq K$ примем следующие обозначения:

$M(S)$ — матрица, полученная из матрицы M обнулением строк с номерами из $K \setminus S$;

$\alpha(S)$ — вектор, полученный из $\alpha \in E^k$ обнулением координат с номерами из $K \setminus S$;

$C(S)$ — код, образованный строками матрицы M с номерами из S;

$\chi(S)$ — характеристический вектор множества S.

Размерность матрицы $M(S)$ определим как размерность кода $C(S)$ и обозначим через $\mathrm{D}(S)$. Отметим, что $M(K) = M$ и $\mathrm{D}(K) = \mathrm{Dim}(C)$. Легко видеть, что имеет место формула

$$\mathrm{D}(S) = \sum_{\substack{\alpha \in E^k, \\ \alpha(S) \notin \{0, \chi(S)\}}} \omega(\alpha). \tag{3}$$

Действительно, в размерность $\mathrm{D}(S)$ ненулевой вклад вносят лишь те столбцы матрицы M, в которых среди компонент с номерами из S встречаются и 0, и 1. Сделаем также следующее наблюдение. Если векторы $\alpha, \beta \in E^k$ антиподальны на множестве координат с номерами из $S \subseteq K$, то эти векторы вносят одинаковый вклад в размерность каждого из подкодов кода $C(S)$.

Для доказательства следующей леммы понадобятся функции

$$\omega_0(\alpha) = \omega(\alpha) + \omega(\bar{\alpha} + e_0), \tag{4}$$

$$\omega_i(\alpha) = \omega(\alpha) + \omega(\alpha + e_i), \quad i \in K \setminus \{0\}. \tag{5}$$

Равенство (4) определяет соотношение между функцией ω и характеристической функцией матрицы, полученной из M инвертированием всех элементов тех столбцов, в которых в первой строке имеется 1, и последующим занулением строки с индексом 0. Иначе говоря, ω_0 — это характеристическая функция приведённого кода $C(K \setminus \{0\})$. Функция ω_i

совпадает с характеристической функцией матрицы, полученной из M занулением i-й строки.

Лемма 3. *Пусть C — приведённый двоичный код. Если известны размерности всех подкодов чётной мощности кода C, то характеристическая функция ω восстанавливается однозначно.*

Доказательство проведём индукцией по мощности k кода C. База индукции очевидна и состоит в том, что если $|C| = 2$ и длина кода равна n, то легко находим $\omega(01) = \mathrm{Dim}(C)$, $\omega(00) = n - \mathrm{Dim}(C)$ и $\omega(10) = \omega(11) = 0$. Пусть утверждение леммы справедливо для всех кодов мощности меньше k, докажем его справедливость для $|C| = k$.

Возможны два случая. Если k чётно, то размерность кода C известна. По предположению индукции для любого $S \subset K$ характеристическая функция подкода $C(S) \subset C$ восстанавливается однозначно. Таким образом становятся известны размерности всех подкодов кода C. Тогда из теоремы 2 следует, что характеристическая функция ω однозначно восстановима.

Пусть k нечётно и имеется кодовая матрица M кода C. По предположению индукции для любого $i \in K$ характеристическая функция подкода $C(K \setminus \{i\})$ известна и, как замечено выше, совпадает с функцией ω_i, определённой в (4) или (5).

Поскольку код C приведённый, $\omega(\alpha) \equiv 0$ в грани $\alpha_0 = 1$ куба E^k. Остаётся восстановить функцию ω в грани $\alpha_0 = 0$, индуцированный граф которой обозначим через G. Согласно формулам (4) и (5) для характеристической функции ω определены суммы её значений для каждой пары антиподальных и каждой пары смежных вершин в G. Дополним граф G рёбрами, соединяющими антиподальные вершины. Тем самым получим граф G', не являющийся двудольным, рёберная весовая функция которого задана. По лемме 1 функция ω, которая является весовой функцией для G', вычисляется однозначно по построенной рёберной весовой функции. Лемма 3 доказана.

Доказательством леммы 3 завершается доказательство теоремы 1. Интересно отметить следующие следствия из леммы 3.

Следствие 2. *Если для двоичного кода заданы размерности всех его подкодов чётной мощности, то размерности всех остальных его подкодов вычисляются однозначно.*

Следствие 3. *Произвольная полусильная изометрия между двоичными кодами является сильной изометрией.*

Согласно теореме 1 двоичный код можно восстановить с точностью

до эквивалентности, если известны размерности всех его подкодов чётной мощности. Возникает естественный вопрос: каков наименьший набор размерностей подкодов, позволяющий восстановить код? Следующие примеры с кодами, отличающимися размерностями лишь одного подкода чётной мощности, показывают неулучшаемый характер теоремы 1.

Пример 1. Построим кодовые матрицы M_1 и M_2 кодов C_1 и C_2 чётной мощности k следующим образом. В качестве столбцов матрицы M_1 возьмём все векторы $\alpha \in E^k$, лежащие в грани $\alpha_0 = 0$ и имеющие нечётный вес. Напротив, столбцами матрицы M_2 пусть будут все векторы той же грани, имеющие чётный вес. При таком определении размерности всех подкодов C_1 и C_2 совпадают, кроме размерностей самих кодов, которые отличаются на 1.

Пример 2. Рассмотрим код $C = \{0^n, x, y, 1^n\}$, где x и y имеют одинаковый вес. Сдвигая векторы x и y на различное расстояние друг от друга и не изменяя при этом их вес, получим множество кодов, которые различаются лишь размерностью $\mathrm{Dim}\{x, y\} = d(x, y)$. Размерности остальных подкодов чётной мощности (включая сами коды) в этом случае одинаковы.

ЛИТЕРАТУРА

1. **Абдурахманов Ж. К.** О геометрической структуре кодов, исправляющих ошибки: Дис. ... канд. физ.-мат. наук: 01.01.09. — Ташкент, 1991. — 66 с.
2. **Августинович С. В.** К строению графов минимальных расстояний совершенных бинарных $(n, 3)$-кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 1998. — Т. 3, № 5. — С. 3–5.
3. **Августинович С. В.** Об изометричности плотно упакованных бинарных кодов // Дискрет. анализ. — Новосибирск: Ин-т математики, 1994. — С. 3–5. — (Тр. РАН. Сиб. отд-ние. Ин-т математики; Т. 27).
4. **Августинович С. В.** О сильной изометрии бинарных кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 3. — С. 3–5.
5. **Августинович С. В., Соловьёва Ф. И.** К метрической жесткости двоичных кодов // Пробл. передачи информ. — 2003. — Т. 39, № 2. — С. 23–28.
6. **Красин В. Ю.** О слабых изометриях булева куба // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 4. — С. 26–32.
7. **Могильных И. Ю.** О слабых изометриях кодов Препараты // Пробл. передачи информ. — 2009. — Т. 45, № 2. — С. 78–83.
8. **Mogilnykh I. Yu., Östergård P. R. J., Pottonen O., Solov'eva F. I.** Reconstructing extended perfect binary one-error-correcting codes from their minimum distance graphs // IEEE Trans. Inform. Theory — 2009. — V. 55. — P. 2622–2625.

9. Solov'eva F. I., Avgustinovich S. V., Honold T., Heise W. On the extendability of code isometries // J. Geom. — 1998. — V. 61. — P. 3–16.

Горкунов Евгений Владимирович,
e-mail: evgumin@gmail.com
Августинович Сергей Владимирович,
e-mail: avgust@math.nsc.ru

Статья поступила
20 мая 2010 г.