ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 2000. Серия 1. Том 7, № 3, 3–5

УДК 519.72

О СИЛЬНОЙ ИЗОМЕТРИИ БИНАРНЫХ КОДОВ*)

С. В. Августинович

Доказано, что любые два сильно изометричных бинарных кода являются эквивалентными.

В данной статье изучается сильная изометрия бинарных кодов, т. е. произвольных подмножеств, состоящих из различных бинарных слов одинаковой длины. Она является продолжением исследований из [1–3, 5]. В самом общем виде проблему изометрии кодов можно сформулировать следующим образом. Пусть E — произвольное метрическое пространство с богатой (как минимум транзитивной) группой автоморфизмов. Два подпространства (подмножества) пространства E называются *эквивалентными*, если каждое из них может быть переведено в другое посредством некоторого автоморфизма пространства E. Два подпространства называются *изометричными*, если между ними существует взаимно однозначное соответствие, сохраняющее расстояния. Ясно, что эквивалентные подпространства изометричны, но обратное верно не всегда. Например, коды Адамара одной длины изометричны по определению, но могут быть неэквивалентными. Таким образом, мы приходим к вопросу: в каких случаях отказ от рассмотрения метрических подпространств с точностью до эквивалентности и переход к рассмотрению их с точностью до изометрии может дать дополнительные возможности. Результаты работ [2, 3, 5] показывают, что в случае плотно упакованных кодов с малыми расстояниями таких возможностей не возникает. Подобным же образом можно интерпретировать и результат данной статьи.

Пусть C_1 и C_2 — два произвольных равномощных бинарных кода длины n. Отображение $I : C_1 \to C_2$ называется *сильной изометрией*, если для каждого $C^* \subseteq C_1$ выполняется равенство $\dim(C^*) = \dim(I(C^*))$.

*) Исследование выполнено при финансовой поддержке Межвузовской научной программы «Университеты России — фундаментальные исследования» (проект 1792), Российского фонда фундаментальных исследований (проект 99–01–00539) и Федеральной целевой программы «Интеграция» (объединенный проект АО–110).

Здесь $\dim(C)$ обозначает размерность минимальной грани в кубе E^n, содержащей код C.

Целью настоящей статьи является доказательство следующего утверждения, которое в [1] было выдвинуто в качестве гипотезы.

Теорема 1. *Если два бинарных кода C_1 и C_2 сильно изометричны, то они эквивалентны.*

Доказательство. Представим условие теоремы в матричном виде. Кодам C_1 и C_2 поставим в соответствие бинарные (т. е. из нулей и единиц) матрицы M_1 и M_2 размера $N \times n$ каждая, где $N = |C_1| = |C_2|$, а n — кодовая длина. Строками матриц являются кодовые векторы, причем, не теряя общности, можно считать, что первые строки матриц M_1 и M_2 нулевые, а сильная изометрия I с i-й строкой матрицы M_1 сопоставляет i-ю строку матрицы M_2, $i = 1, 2, \dots, N$.

Пусть $S \subseteq \{1, 2, \dots, N\}$ и $j \in \{1, 2\}$. Обозначим через M_j^S матрицу, составленную из строк матрицы M_j с номерами из S. Размерностью $\dim(M_j^S)$ матрицы M_j^S назовем число ее столбцов, в каждом из которых содержатся 0 и 1. Легко убедиться в том, что определенная таким образом размерность подматрицы совпадает с размерностью соответствующего подкода. Обозначим через R_j^S число столбцов матрицы M_j, в которых единицы находятся на местах с номерами из S, а на остальных местах находятся нули.

Итак, по условию $\dim(M_1^S) = \dim(M_2^S)$ для всех $S \subseteq \{1, 2, \dots, N\}$. Требуется показать, что существует перестановка столбцов матрицы M_1, переводящая ее в M_2. Это равносильно тому, что мультимножества столбцов (столбцы могут повторяться) матриц M_1 и M_2 совпадают или, другими словами, $R_1^S = R_2^S$ для всех S.

Предложение 1. *Пусть M — произвольная бинарная матрица размера $N \times n$, содержащая на первом месте нулевую строку. Тогда для всех $S \subseteq \{1, 2, \dots, N\}$, $1 \notin S$, выполняется соотношение*

$$\dim(M^{\overline{S}}) + \sum_{s \subseteq S} R^s = n.$$

Доказательство. Заметим, что единицы каждого столбца матрицы M задают некоторое множество X номеров строк, причем если $X \cap \overline{S} = \varnothing$, то данный столбец вносит единичный вклад в сумму и нулевой вклад в $\dim(M^{\overline{S}})$. Если же $X \cap \overline{S} \neq \varnothing$, то, напротив, данный столбец вносит нулевой вклад в сумму и единичный в $\dim(M^{\overline{S}})$, поскольку среди строк матрицы M есть нулевая. Тем самым левая часть доказываемого равенства равна количеству столбцов матрицы M. По условию это количество равно n.

Следствие. *Зная набор значений* $\dim(M^S)$ *для всех* $S \subseteq \{1, 2, \dots, N\}$, *можно вычислить все значения* R^S.

Доказательство легко проводится по возрастанию мощности S с использованием предложения 1 на каждом индукционном шаге.

Вернемся к доказательству теоремы. Остается заметить, что следствие устанавливает равенство $R_1^S = R_2^S$ для всех $S \subseteq \{1, 2, \dots, N\}$, что и требовалось доказать.

ЛИТЕРАТУРА

1. **Абдурахманов Ж. К.** О геометрической структуре кодов, исправляющих ошибки: Дис. ... канд. физ.-мат. наук. 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. 5, № 4. С. 3–5.
3. **Августинович С. В.** Об изометричности плотно упакованных бинарных кодов // Дискретный анализ. Новосибирск: Изд-во Ин-та математики, 1994. С. 3–5. (Тр. / РАН. Сиб. отд-ние. Ин-т математики; Т. 27).
4. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. **Solov'eva F. I., Avgustinovich S. V., Honold T., Heise W.** On the extendability of code isometries // J. Geometry. 1998. V. 61, N 1/2. P. 3–16.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила
16 февраля 2000 г.