

А. А. Григорьянц

Об одном случае достижимости границы расстояния для фрактальных кодов

(Представлено академиком А. А. Талаляном 7/V 2003)

В [1] предложена новая конструкция линейных двоичных кодов, исправляющих ошибки. Новый код получается из двух семейств кодов с помощью суммы соответствующих тензорных произведений. Получена также формула для размерности нового кода и верхняя граница для расстояния. Эти результаты будут кратко сформулированы ниже. Установление общих условий достижимости границы расстояния, по всей видимости, является трудной задачей. В настоящей статье рассмотрен случай, когда одно из семейств кодов является вложенным. В этом случае граница расстояния достигается. Указаны также некоторые примеры экстремальных фрактальных кодов на коротких составных длинах, полученные из вложенных семейств.

В данной статье под (n, k, d) -кодами понимаются линейные двоичные коды на длине n , размерности k , с минимальным расстоянием d , т.е. k -мерные подпространства арифметического линейного пространства F_2^n над полем $F_2 = \{0, 1\}$. Используется также терминология, принятая в алгебраической теории кодирования (мы следуем [2], см. также русский перевод [3]) и стандартные понятия линейной и тензорной алгебры. Пусть $C = \{C_i\}_{i=1}^s$ и $D = \{D_i\}_{i=1}^{s'}$ – два семейства линейных двоичных кодов на длине n и n' соответственно. В [1] были введены фрактальные коды, получающиеся с помощью семейств C , D по формуле

$$C \otimes D = C_1 \otimes D_1 + \dots + C_s \otimes D_{s'}, \quad (1)$$

т.е. являющиеся суммой тензорных произведений соответствующих кодов из семейств C и D . Формула (1) задает код на длине pn' .

Пусть $S = \{1; \dots; s\}$ – множество первых s натуральных чисел и $\alpha = \{i_1; \dots; i_r\} \subset S$ произвольное подмножество в S . Обозначим $|\alpha| = r$. Для произвольного семейства кодов $\{C_i\}_{i=1}^s$ введем в рассмотрение следующие коды:

$$\begin{aligned} C^\alpha &= \sum_{i \in \alpha} C_i \\ C_\alpha &= \bigcap_{i \in \alpha} C_i \end{aligned} \quad (2)$$

Таким образом, C^α и C_α – суть сумма и пересечение линейных подпространств, соответствующих мультииндексу α . Мы также пишем C_{12} для $C_1 \cap C_2$ и т. п. Параметры этих кодов мы будем обозначать $(n^\alpha, k^\alpha, d^\alpha)$ и $(n_\alpha, k_\alpha, d_\alpha)$ соответственно. Обозначим также $(n'^\alpha, k'^\alpha, d'^\alpha)$ и $(n'_\alpha, k'_\alpha, d'_\alpha)$ параметры соответствующих кодов для семейства D .

Семейство векторов $e = \{e_i\} \subset \cup C$ назовем базисом семейства подпространств C , если $C_\alpha \cap e$ – порождает C_α и, кроме того, является минимальным (в смысле частичного порядка, порождаемого отношением включения) семейством, обладающим указанным свойством. Легко видеть, что любое семейство подпространств обладает базисом, но базис семейства не всегда будет линейно независимым. Более детальное исследование свойств базисов семейств выходит за рамки настоящей статьи.

Семейство подпространств, для которого существует линейно независимый базис, назовем ациклическим.

Обозначим через α_a максимальный по мощности мультииндекс, для которого $a \in C_{\alpha_a}$. Очевидно, что этот мультииндекс определен однозначно. Для произвольного семейства векторов $a = \{a_i\}$ обозначим $\Psi(a) = \{\alpha_{a_i} \mid a_i \in a\}$. Пусть теперь Ψ – произвольное подмножество мультииндексов. Выбирая по одному элементу из каждого мультииндекса в Ψ мы получим некоторый мультииндекс. Множество всех таких мультииндексов обозначим Ψ^* .

В [1] показано, что в случае ациклических семейств C и D размерность кода (1) вычисляется по формуле

$$k = \sum_{\alpha} (-1)^{|\alpha|+1} k_{\alpha} k'_{\alpha} \quad (3)$$

Верхняя граница расстояния кода (1) имеет вид:

$$\delta \leq \min_{\alpha, \beta} (d_{\alpha} d'^{\alpha}, d^{\beta} d'_{\beta}) \quad (4)$$

где минимум берется по всем тем α и β , для которых подпространства C_{α} , D_{β} ненулевые.

Нижняя граница расстояния кода (1) имеет вид:

$$\delta \geq \max \left(\max_{\psi_0 \subset \Psi(e)} \left[\max_{\alpha \in \psi_0} (d_{\alpha} d'^{\alpha}) \max_{\beta \in \psi_0^*} d^{\beta} \right], \min_{\psi_0 \subset \Psi(g)} \left[\max_{\alpha \in \psi_0} d^{\alpha} \max_{\beta \in \psi_0^*} (d'_{\beta} d^{\beta}) \right] \right). \quad (5)$$

где Ψ_0 произвольное непустое подмножество $\Psi(e)$ (или $\Psi(g)$).

Семейство C назовем вложенным, если $C_i \subset C_{i+1}$ для всех тех i , для которых оба кода определены. Вложенное семейство, очевидно, ациклично.

Основным результатом настоящей статьи является следующая

Теорема 1. *Если одно из семейств C , D вложено, а другое ациклично, то граница (4) достигается. Более того, верхняя граница (4) и нижняя граница (5) в этой ситуации совпадают.*

Для доказательства теоремы нам понадобится следующая

Лемма 1. *Если семейство C ациклично, то для произвольного вектора $x \in C \otimes D$ существует единственное представление:*

$$x = e_1 \otimes b_1 + \dots + e_r \otimes b_r, \quad (6)$$

где $e = \{e_i\}$ – базис в C и $b_i \in D^{\alpha_{e_i}}$.

Доказательство (см. также лемму 1 в [1]). Т. к. $x \in C \otimes D$, то x представляется в виде $x = x_1 + \dots + x_s$, где $x_i \in C_i \otimes D_i$, а каждый x_i согласно лемме 1 в [1] представляется в виде :

$$x_i = \sum_j e_i^j \otimes b_i^j,$$

где $e_i^j \in e \cap C_i$, а $b_i^j \in D_i$ для всех i, j . Группируя подобные члены (т.е. вынося за скобки одинаковые векторы e_i^j), получим представление вида (6), где, очевидно, $b_i \in D^{\alpha_{e_i}}$. Единственность следует из того, что для любого вектора $y = \sum_i a_i \otimes b_i$ из линейной независимости векторов a_i , следует, что равенство нулю y равносильно равенству нулю всех b_i .

Пусть теперь, скажем, семейство C ациклично, а семейство D вложено. Для произвольного вектора $x \in C \otimes D$ проверим выполнение обратного неравенства в (4). Во-первых, отметим, что из леммы 1 следует существование для вектора x представления вида:

$$x = e_1 \otimes b_1 + \dots + e_r \otimes b_r,$$

где e_i – базис в C , а $b_i \in D_{p_i}$, где p_i – максимальный индекс, для которого $e_i \in C_{p_i}$. Введем в рассмотрение мультииндекс $\pi = \{p_i\}$. Пусть также $p = \min \pi$. Тогда вес вектора $b = \cup_i b_i$ не меньше, чем d^p (расстояние кода D_p). Напомним, что вектор $e_i \otimes b_i$ можно представить как матрицу, у которой строки, соответствующие ненулевым позициям вектора b_i , совпадают с вектором e_i , а остальные строки нулевые. Соответственно вектор x представляется как сумма матриц такого вида и, следовательно, строки вектора x , соответствующие ненулевым позициям вектора b , являются линейными комбинациями векторов e_i и имеют вес не меньший, чем d^π .

Таким образом, вес вектора x не меньше, чем $d^\pi d'_\pi$.

Покажем теперь совпадение нижней границы (5) и верхней границы (4).

В данном случае, $\Psi(g) = \{\{123\dots s\}, \{23\dots s\}, \dots, \{s\}\}$. Пусть $\max_{\alpha \in \Psi_0} d^\alpha$ достигается на некотором $\alpha_0 \in \Psi_0$ и, скажем, $\alpha_0 = \{i_0; \dots; s\}$. Заметим, что в этом случае можно считать $\min_{\alpha \in \Psi_0} |\alpha| = |\alpha_0|$ и, следовательно, $i_0 \in \alpha$ для любого $\alpha \in \Psi_0$. Из сказанного можно заключить, что $\beta_0 = \{i_0\} \in \Psi_0^*$, а, значит, $\max_{\beta \in \Psi_0^*} d'^\beta \geq d'_{i_0} = d'_{\alpha_0}$, откуда окончательно получаем

$$(\max_{\alpha \in \Psi_0} d^\alpha) (\max_{\beta \in \Psi_0^*} d'^\beta) \geq d^{\alpha_0} d'_{\alpha_0}$$

что завершает доказательство теоремы.

Следствие 1. Если C и D – два вложенных семейства кодов, то для размерности и расстояния кода:

$$E = C_1 \otimes D_s + C_2 \otimes D_{s-1} + \dots + C_s \otimes D_1 \quad (7)$$

верны формулы

$$k = k_1 k'_s + (k_2 - k_1) k'_{s-1} + \dots + (k_s - k_{s-1}) k'_1$$

$$\delta = \min_i (d_i d_{s-i+1})$$

Пример 1. (32, 16, 8)-код.

Рассмотрим два вложенных семейства кодов: $C_1 \subset C_2 \subset C_3$ и $D_1 \subset D_2 \subset D_3$ со следующими параметрами:

код	(n, k, d)	код	(n, k, d)
C_1	(4,1,4)	D_1	(8,1,8)
C_2	(4,3,2)	D_2	(8,4,4)
C_3	(4,4,1)	D_3	(8,7,2)

Все коды определены однозначно, кроме кода D_2 , который может быть выбран произвольно. Согласно следствию 1, код, определенный формулой (7) является (32, 16, 8)-кодом. Этот код эквивалентен коду Рида-Маллера $\mathcal{R}(\nabla, \epsilon)$ и является экстремальным.

Пример 2. (28, 22, 4)-код.

Рассмотрим два вложенных семейства кодов (см. пример 4 в [1]): $C_1 \subset C_2 \subset C_3$ и $D_1 \subset D_2 \subset D_3$ со следующими параметрами

код	(n, k, d)	код	(n, k, d)
C_1	(7,3,4)	D_1	(4,1,4)
C_2	(7,6,2)	D_2	(4,3,2)
C_3	(7,7,1)	D_3	(4,4,1)

Согласно следствию 1, код, определенный формулой (7), является (28, 22, 4)-кодом. Этот код также является экстремальным.

Российско-Армянский (Славянский) государственный университет

Литература

1. Григорьянц А. А. Известия НАН Армении. Математика. 2003. М1.
2. MacWilliams F.J., Sloane N.J. – The Theory of Error-correcting Codes. Bell Laboratories Murray Hill NJ 07974 U.S.A. 1977.
3. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. – Теория кодов, исправляющих ошибки. М. Связь. 1979.

Ա. Ա. Գրիգորյանց

Ֆրակտալ կոդերի հեռավորությաներին եզրի հասանելիության մասին

Ֆրակտալ կոդերը հեղինակը ներկայացնում է նախորդ աշխատության մեջ, որտեղ նաև նշվել են այդ կոդերի հեռավորության վերին և ստորին եզրերը և դրվել է վերին եզրին հասնելու, ինչպես նաև վերին և ստորին եզրերի համընկնելու ընդհանուր պայմանները գտնելու խնդիրը: Սույն հոդվածում ցույց է տրվել, որ հեռավորության վերին եզրը հավասար է (իսկ ստորին համընկնում է վերինի հետ) ներդրված կոդերի ընտանիքի համար, և բերված են որոշ օրինակներ փոքր երկարությունների համար: