УДК 621.391.15

МАТЕМАТИКА

Ж. Г. Маргарян, Г. Л. Мовсисян

Об одном методе построения линейных кодов

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 15/IV 1983)

Рассмотрим n -мерное пространство B_n над полем $GF(2)$ ⁽¹⁾. Элементы этого пространства будем называть n -точками и обозначим через

$$\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n), \quad \tilde{\beta} = (\beta_1, \beta_2, \dots, \beta_n)$$

и т. д., где α_i, β_i равны 0 или 1. Геометрически n -точки представляют собой вершины n -мерного куба в евклидовом пространстве E_n .

Расстояние по Хэммингу между n -точками $\tilde{\alpha}$ и $\tilde{\beta}$ определим по формуле

$$d(\tilde{\alpha}, \tilde{\beta}) = \sum_{i=1}^n |\alpha_i - \beta_i|.$$

Весом Хэмминга n -точки $\tilde{\alpha}$ назовем число его ненулевых компонент. Обозначим через B_n^k множество n -точек веса k .

Кодом длины n над полем $GF(2)$ называется любое непустое подмножество V множества B_n . Элементы из V называются кодовыми словами. Обозначим через $R(V)$ множество значений, принимаемых расстоянием между различными кодовыми словами, т. е. $d \in R(V)$ тогда и только тогда, когда существуют такие различные кодовые слова $\tilde{\alpha}, \tilde{\beta}$, что $d(\tilde{\alpha}, \tilde{\beta}) = d$. Предположим, что $R = \{d_1, d_2, \dots, d_q\}$ некоторое непустое подмножество множества $A = \{1, 2, \dots, n\}$. Обозначим через $F(n; R)$ семейство кодов V таких, что $R(V) \subseteq R$. Пусть*

$$M(n; R) = \max_{V \in F(n; R)} |V|.$$

Относительно метрического функционала $M(n; R)$ известна ⁽²⁾ следующая верхняя оценка, имеющая место для всех R одинаковой мощности, а именно

$$M(n; R) \leq 1 + C_n^1 + C_n^2 + \dots + C_n^{|R|}.$$

Используя информацию о строении множества R , в ряде случаев нам удалось улучшить приведенную оценку.

Теорема 1. Если любой элемент множества R является числом вида $4r+2$, то имеет место неравенство

* В статье приняты следующие обозначения: $[\xi]$ — целая часть числа ξ , $|V|$ — мощность множества V .

$$M(n; R) \leq |R| (n+1) + 1.$$

Следствие. Если код V такой, что $|V| > 2 \left\lfloor \frac{n+2}{4} \right\rfloor (n+1) + 3$, то множество $R(V)$ содержит элемент, кратный 4.

Подпространство пространства B_n называется линейным кодом. Любое множество базисных n -точек линейного кода можно рассматривать как строки матрицы, называемой порождающей матрицей кода. Число d называется минимальным расстоянием кода V , если

$$d = \min_{\bar{\alpha} \neq \bar{\beta}} \{d(\bar{\alpha}, \bar{\beta})\},$$

где $\bar{\alpha}, \bar{\beta} \in V$.

Минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов. Линейный код размерности k , длины n и с минимальным расстоянием d называется $[n, k, d]$ -кодом.

Следующие два результата относятся к таким кодам, для которых расстояние между различными кодовыми словами равно d_1 или d_2 . Любое натуральное число N можно представить в виде $N = P \cdot 2^a$, где P — нечетное число. Предположим, что

$$d_i = P_{d_i} \cdot 2^{a_i}, \quad i = 1, 2.$$

Теорема 2. Если существует линейный V код такой, что $R(V) = \{d_1, d_2\}$, то имеет место неравенство $k \leq \log \frac{2d_1 d_2}{P_{d_1} P_{d_2}}$.

Замечание. Для некоторых d_1, d_2 существует семейство линейных кодов, для которых граница, задаваемая в теореме 2, достигается.

Обозначим через G_k матрицу, столбцами которой являются все n -точки с весом k . Предположим, что n -точка $\bar{\alpha}$ имеет вес a . Через $f_k(n; a)$ обозначим вес вектора $\bar{\alpha} G_k$. Все операции в произведении $\bar{\alpha} G_k$ выполняются над полем $GF(2)$.

Лемма 1. Если $d(\bar{\alpha}, \bar{\beta}) = a$, то $d(\bar{\alpha} G_k, \bar{\beta} G_k) = f_k(n; a)$.

Лемма 2. $f_k(n; a) = \sum_{i=1}^{\lfloor \frac{a+1}{2} \rfloor} C_a^{2i-1} C_{n-a}^{k-2i+1}$.

Теорема 3. Имеет место неравенство $M(n; \{d, n-d\}) \leq 1 + \frac{n(n-1)}{2}$. Если имеет место равенство, то существует матрица

Адамара порядка $1 + \frac{n(n-1)}{2}$.

Утверждение 1. $f_{n-k}(n; a) = \frac{1 + (-1)^{a+1}}{2} C_n^k + (-1)^a f_k(n; a)$.

Утверждение 2. $f_n(n; a) = \frac{1 + (-1)^{a+1}}{2}$.

Лемма 3. Имеет место равенство

$$\sum_{h=1}^{\lfloor \frac{n+1}{2} \rfloor} f_{2h-1}(n; a) = \begin{cases} 2^{n-2}, & \text{при } a \neq n, \\ 2^{n-1}, & \text{при } a = n. \end{cases}$$

Теорема 4. Для произвольного натурального числа m существуют двоичные линейные коды со следующими параметрами:

(I) при $m \equiv 1 \pmod{2}$

$$\begin{cases} n = 2^{m-1} - m - 1 \\ d = 2^{m-2} - m + 1 \\ k = m \end{cases}$$

(II) при $m \equiv 0 \pmod{2}$

$$\begin{cases} n = 2^{m-1} - 2m \\ d = 2^{m-2} - 2m + 4 \\ k = m \end{cases}$$

Порождающая матрица линейного кода I (II) представляет собой $(m \times (2^{m-1} - m - 1))$ ($(m \times (2^{m-1} - 2m))$)—матрицу, столбцами которой являются все ненулевые двоичные m -точки с весом $2k-1$, где $k = 2, 3, \dots, s-1$ ($k = 2, 3, \dots, s$).

Теорема 5. Для любого натурального числа m существует линейный код со следующими параметрами:

$$(III) \begin{cases} n = 2^{m-1} - m \\ d = 2^{m-2} - m + 1 \\ k = m. \end{cases}$$

Столбцами порождающей матрицы линейного кода III являются все ненулевые двоичные m -точки с весом $2k-1$, где $k = 2, 3, \dots, \lfloor \frac{m+1}{2} \rfloor$.

Лемма 5. Имеют место следующие равенства:

1.

$$\sum_{k=1}^{\lfloor \frac{n+3}{4} \rfloor} f_{4k-3}(n; a) = \begin{cases} 2^{n-3} + 2^{\frac{n-1}{2}} \left\{ \cos \frac{\pi}{4} (n-2) + \cos \frac{\pi}{4} (2a-n-2) \right\}, & \text{при } a \neq n, \\ 2^{n-2} + 2^{\frac{n-2}{2}} \cos \frac{\pi}{4} (n-2), & \text{при } a = n. \end{cases}$$

2.

$$\sum_{k=1}^{\lfloor \frac{n+1}{4} \rfloor} f_{4k-1}(n; a) = \begin{cases} 2^{n-3} - 2^{\frac{n-4}{2}} \left\{ \cos \frac{\pi}{4} (n-2) + \cos \frac{\pi}{4} (2a-n-2) \right\}, & \text{при } a \neq n, \\ 2^{n-2} - 2^{\frac{n-2}{2}} \cos \frac{\pi}{4} (n-2), & \text{при } a = n. \end{cases}$$

Из этой леммы при $n \equiv 1 \pmod{4}$ получаем:

$$\sum_{k=1}^{\lfloor \frac{n+3}{4} \rfloor} f_{4k-3}(n; a) = \begin{cases} 2^{n-3}, & \text{при } a \equiv 0 \text{ или } 3 \pmod{4}, \\ 2^{n-3} + 2^{\frac{n-3}{2}} (-1)^{\frac{n-1}{4}}, & \text{при } a \equiv 1 \text{ или } 2 \pmod{4}, \\ 2^{n-2} + 2^{\frac{n-3}{2}} (-1)^{\frac{n-1}{4}}, & \text{при } a = n. \end{cases} \quad (1)$$

$$\sum_{k=2}^{\lfloor \frac{n+1}{4} \rfloor} f_{4k-1}(n; a) = \begin{cases} 2^{n-3}, & \text{при } a \equiv 0 \text{ или } 3 \pmod{4}, \\ 2^{n-3} - 2^{\frac{n-3}{2}} (-1)^{\frac{n-1}{4}}, & \text{при } a \equiv 1 \text{ или } 2 \pmod{4}, \\ 2^{n-2} - 2^{\frac{n-3}{2}} (-1)^{\frac{n-1}{4}}, & \text{при } a = n. \end{cases} \quad (2)$$

А при $n \equiv 3 \pmod{4}$ получаем

$$\sum_{k=1}^{\lfloor \frac{n+3}{4} \rfloor} f_{4k-3}(n; a) = \begin{cases} 2^{n-3}, & \text{при } a \equiv 0 \text{ или } 1 \pmod{4}, \\ 2^{n-3} + 2^{\frac{n-3}{2}} (-1)^{\frac{n-3}{4}}, & \text{при } a \equiv 2 \text{ или } 3 \pmod{4}, \\ 2^{n-2} + 2^{\frac{n-3}{2}} (-1)^{\frac{n-3}{4}}, & \text{при } a = n. \end{cases} \quad (3)$$

$$\sum_{k=1}^{\lfloor \frac{n+1}{4} \rfloor} f_{4k-1}(n; a) = \begin{cases} 2^{n-3}, & \text{при } a \equiv 0 \text{ или } 1 \pmod{4}, \\ 2^{n-3} - 2^{\frac{n-3}{2}} (-1)^{\frac{n-3}{4}}, & \text{при } a \equiv 2 \text{ или } 3 \pmod{4}, \\ 2^{n-2} - 2^{\frac{n-3}{2}} (-1)^{\frac{n-3}{4}}, & \text{при } a = n. \end{cases} \quad (4)$$

Теорема 6. Для произвольного нечетного числа m существуют двоичные линейные коды со следующими параметрами:

$$(IV) \quad \begin{cases} n = 2^{m-2} + 2^{\frac{m-3}{2}} \\ d = 2^{m-3} \\ k = m \end{cases} \quad (V) \quad \begin{cases} n = 2^{m-2} - 2^{\frac{m-3}{2}} \\ d = 2^{m-3} - 2^{\frac{m-3}{2}} \\ k = m \end{cases}$$

Из соотношений (1)–(4) следует: когда $m \equiv 5$ или $7 \pmod{8}$, то порождающая матрица линейного кода IV (V) представляет собой $(m \times (2^{m-2} + 2^{\frac{m-3}{2}}))$ ($(m \times (2^{m-2} - 2^{\frac{m-3}{2}}))$) – матрицу, столбцами которой являются все ненулевые двоичные m -точки с весом $w \equiv 3 \pmod{4}$ ($w \equiv 1 \pmod{4}$). А если $m \equiv 1$ или $3 \pmod{8}$, то столбцами порождающей матрицы линейного кода IV (V) являются все ненулевые m -точки с весом $w \equiv 1 \pmod{4}$ ($w \equiv 3 \pmod{4}$).

Обозначим через $d_{\max}(n; k)$ максимум минимального расстояния по всем линейным кодам длины n , размерности k (³). При $m \geq 7$ полученные семейства линейных кодов являются новыми и улучшают известные нижние границы для $d_{\max}(n; k)$ (см. (³)).

Ереванский государственный университет

Փ. Գ. ՄԱՐԴԱՐՅԱՆ, Ղ. Լ. ՄՈՎՍԻՍՅԱՆ

Գծային կոդերի կառուցման մի մեթոդի մասին

Միավոր խորանարդի ցանկացած ենթաբազմություն կոչվում է կոդ, իսկ նրա էլեմենտները կոդային բառեր: Երկու իրարից տարբեր կոդային բառերի հեմինգյան հեռավորության արժեքների բազմությունը կոչվում է կոդի հեռավորությունների բազմություն: Նշանակենք $(M; R)$ -ով այն կոդի հզորությունը, որն ունի ամենամեծ հզորություն և որի հեռավորությունների բազմությունը հանդիսանում է R -ի ենթաբազմություն: Բազմության վրա որոշակի սահմանափակումների դեպքում աշխատանքում հաջողվել է լավացնել $M(n; R)$ մետրիկական ֆունկցիոնալի հայտնի (²) վերին գնահատականը: Այնուհետև աշխատանքում նկարագրված է գծային կոդերի կառուցման մի մեթոդ և այդ մեթոդով ստացված է գծային կոդերի 5 բնտանիք:

ЛИТЕРАТУРА — Գ Ր Ա Վ Ա Ն Ո Ւ Թ Յ Ո Ւ Ն

¹ Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн, Теория кодов, исправляющих ошибки, Связь, М., 1979. ² P. Delsarte, Information and Control, v. 23 (1973). ³ H. J. Helgert, R. D. Stinaff, IEEE Trans. Inform. Theory, v. 19 (1973).