УДК 519.1

МАТЕМАТИКА

Г. Л. Мовсисян

О радиусе покрытия подмножеств точек
 единичного n -мерного куба

(Представлено чл.корр. АН Армянской ССР Р. Р. Варшамовым 15/II 1982)

Рассмотрим пространство E_n двоичных последовательностей длины n с заданной на нем метрикой Хэмминга $\rho(x, y) = \sum_{i=1}^n |x^i - y^i|$, где $x = (x^1 \ x^2 \ \dots \ x^n)$, $y = (y^1 \ y^2 \ \dots \ y^n)$.

Пусть $E_n^k = \{(x^1 \ x^2 \ \dots \ x^n) \in E_n / \sum_{i=1}^n x_i = k\}$.

Множество $S_n^t(x) = \{y \in E_n / \rho(x, y) \leq t\}$ будем называть шаром радиуса t с центром x . Последовательности из E_n будем называть точками.

Одним из важнейших параметров кода $A \subseteq E_n (A \subseteq E_n^k)$ является радиус покрытия, который определяется следующим образом (см. (1)):

$$r(A) = \max_{x \in E_n} \min_{y \in A} \rho(x, y) \quad (\bar{r}(A) = \max_{x \in E_n^k} \min_{y \in A} \rho(x, y)).$$

В содержательном смысле $r(A) (\bar{r}(A))$ — наименьшее число, такое, что шары радиуса $r(A) (\bar{r}(A))$ покрывают все множество $E_n (E_n^k)$, т. е. для любой точки $x \in E_n (E_n^k)$ существует точка $y \in A$ такая, что $\rho(x, y) \leq r(A) (\bar{r}(A))$. Иногда этот параметр называют истинным внешним расстоянием кода.

Заметим, что если через $D_x (\bar{D}_x)$ обозначить область Дирихле (2) точки x в множестве $E_n (E_n^k)$, то

$$r(A) = \max_{x \in A} \max_{y \in D_x} \rho(x, y) \quad (\bar{r}(A) = \max_{x \in A} \max_{y \in \bar{D}_x} \rho(x, y)).$$

Введем величину

$$r(s) = \min_{|A|=s} r(A) \quad (\bar{r}(s) = \min_{|A|=s} \bar{r}(A)).$$

Определение. Код $A \subseteq E_n (A \subseteq E_n^k)$ назовем оптимальным относительно радиуса покрытия, если

$$r(A) = r(s) \quad (\bar{r}(A) = \bar{r}(s)).$$

В настоящей работе исследуются оптимальные коды относительно радиуса покрытия. Для $r(s), \bar{r}(s)$ получены асимптотические оцен-

ки, а также точная их асимптотика при определенных значениях параметров s и n .

Обозначим через $m(t)$ величину, удовлетворяющую условиям:

1) существует код $A = \{x_1, x_2, \dots, x_{m(t)}\}$ такой, что шары радиуса t с центрами в кодовых точках покрывают E_n ,

2) для величины $m(t) - 1$ условие 1) не выполняется.

Пусть M матрица из нулей и единиц размеров $p \times g$, в каждом столбце которой содержится ровно l единиц.

Обозначим через $\mu(M)$ минимальное число строк матрицы M , таких, что в подматрице M' , образованной этими строками, нет нулевых столбцов.

Пусть далее $x_1, x_2, \dots, x_{2^n}$ — все точки E_n . Образую матрицу $M'_n = \{a_{ij}\}$ размеров $2^n \times 2^n$ следующим образом:

$$a_{ij} = \begin{cases} 1, & \text{если } x_i \in S'_n(x_j), \\ 0 & \text{в противном случае.} \end{cases}$$

Очевидно, что в каждой из строк и столбцов матрицы содержится $S'_n = \sum_{i=0}^l C'_n$ единиц.

Лемма 1. Если шары радиуса t с центрами в кодовых точках кода $A = \{x_1, x_2, \dots, x_{m(t)}\}$ покрывают все множество E_n , то

$$\mu(M'_n) = m(t).$$

Доказательство немедленно следует из определений $m(t)$ и $\mu(M)$.

Теорема 1. Для любого натурального s имеет место неравенство

$$s < \frac{2^n}{S_n^{r(s)-1}} \ln(S_n^{r(s)-1} + 1).$$

Доказательство. Из определения величины $r(s)$ следует, что E_n не покрывается шарами радиуса $r(s) - 1$ при любом расположении s центров этих шаров в E_n .

Ясно, что

$$s < m(r(s) - 1). \quad (1)$$

В (3) была получена верхняя оценка для $\mu(M)$:

$$\mu(M) < \frac{p}{l} \ln \frac{g \cdot l}{p} + \frac{p}{l} + 1.$$

Отсюда следует, что

$$\mu(M'_n) < \frac{2^n}{S'_n} \ln(S'_n + 1) + 1.$$

Из (1), используя лемму, получаем

$$s < m(r(s) - 1) < \frac{2^n}{S_n^{r(s)-1}} \ln(S_n^{r(s)-1} + 1) + 1.$$

Так как $s, m(t)$ — целые, то

$$s < \frac{2^n}{S_n^{r(s)-1}} \ln(S_n^{r(s)-1} + 1),$$

что и требовалось.

Лемма 2. При $r(s) = o(n)$ справедливо неравенство
 $r(s) (\log n - \log r(s)) \geq n - \log s \quad (n \rightarrow \infty).$

Лемма 3. При $r(s) = o(n)$ имеет место неравенство
 $(r(s) - 1)(\log n - \log(r(s) - 1)) \leq n - \log s \quad (n \rightarrow \infty).$

Доказательство. Согласно теореме 1

$$s < \frac{2^n}{S_n^{r(s)-1}} (\ln(S_n^{r(s)-1} + 1)),$$

т. е.

$$n - \log s > \log S_n^{r(s)-1} - \log \ln(S_n^{r(s)-1} + 1). \quad (2)$$

Поскольку $\log \ln(S_n^{r(s)-1} + 1) = o(\log S_n^{r(s)-1})$, то из (2) следует, что

$$n - \log s \geq \log S_n^{r(s)-1}.$$

Отсюда получаем

$$n - \log s \geq (r(s) - 1) \log n - \left(\frac{(r(s) - 1)^2}{2n} + O(\log(r(s) - 1)) \right) \log e - (r(s) - 1) \times \\ \times \log(r(s) - 1) + (r(s) - 1) \log e - O(\log(r(s) - 1)) - (r(s) - 1)(\log n - \log(r(s) - 1)),$$

что и требовалось доказать.

Лемма 4. Если $\log s \geq n - n^c$, $c < 1$, то $r(s) = o(n)$ ($n \rightarrow \infty$).

Лемма 5. Если $\log s \geq n - n^c$, $c < 1$, то решение уравнения

$$r(s)(\log n - \log r(s)) = n - \log s$$

имеет вид $r(s) \sim \frac{n - \log s}{\log(n \cdot \log n) - \log(n - \log s)}$.

Из предыдущих четырех лемм вытекает следующая

Теорема 2. Если $\log s \geq n - n^c$, $c < 1$, то

$$\frac{n - \log s}{\log\left(\frac{n \cdot \log n}{n - \log s}\right)} \leq r(s) \leq \frac{n - \log s}{\log\left(\frac{n \cdot \log n}{n - \log s}\right)} + 1.$$

Лемма 6. Если $r(s) < r(s-1)$, то $s = m(r(s))$.

Теорема 3. Если

1) $\log s \geq n - n^c$, $c < 1$;

2) $r(s) < r(s-1)$,

то

$$r(s) \sim \frac{n - \log s}{\log\left(\frac{n \cdot \log n}{n - \log s}\right)}.$$

Аналогичными рассуждениями можно доказать относительно величины $\bar{r}(s)$ следующие утверждения.

Теорема 4. Если

- 1) $k = o(n)$ ($n \rightarrow \infty$);
- 2) $\log s \geq (k - k^c) \log n$, $c < 1$ ($n \rightarrow \infty$),

то

$$\frac{k \log \frac{n}{k} - \log s}{\log \left(\frac{k(n-k) \log k(n-k)}{\left(k \log \frac{n}{k} - \log s \right)^2} \right)} \leq \frac{\bar{r}(s)}{2} \leq \frac{k \log \frac{n}{k} - \log s}{\log \left(\frac{k(n-k) \log k(n-k)}{\left(k \log \frac{n}{k} - \log s \right)^2} \right)} + 1.$$

Теорема 5. Если

- 1) $k = o(n)$ ($n \rightarrow \infty$);
- 2) $\log s \geq (k - k^c) \log n$, $c < 1$ ($n \rightarrow \infty$);
- 3) $\bar{r}(s) < \bar{r}(s-1)$,

то

$$\frac{\bar{r}(s)}{2} \sim \frac{k \log \frac{n}{k} - \log s}{\log \left(\frac{k(n-k) \log k(n-k)}{\left(k \log \frac{n}{k} - \log s \right)^2} \right)} \quad (n \rightarrow \infty).$$

Автор благодарит В. К. Леонтьева за большое внимание к работе.

Ереванский государственный университет

Ղ. Լ. ՄՈՎՍԻՍՅԱՆ

n -չափանի միավոր խորանարդի կետերի ենթաբազմությունների ծածկույթի շառավղի մասին

Դիցուք E_n -ը n -չափանի միավոր խորանարդն է, հետևյալ մետրիկայով $\rho(x, y) = \sum_{i=1}^n |x^i - y^i|$, որտեղ $x = (x^1 x^2 \dots x^n)$; $y = (y^1 y^2 \dots y^n)$.

$$E_n^k = \left\{ (x^1 x^2 \dots x^n) \in E_n / \sum_{i=1}^n x^i = k \right\}.$$

$A \subseteq E_n$ ($A \subseteq E_n^k$) կողի ծածկույթի շառավղի կոչվում է հետևյալ մեծությունը

$$r(A) = \max_{x \in E_n} \min_{y \in A} \rho(x, y) \quad (\bar{r}(A) = \max_{x \in E_n^k} \min_{y \in A} \rho(x, y))$$

$A \subseteq E_n (A \subseteq E_n^k)$ կողը կոչվում է օպտիմալ ծածկույթի շառավղի նկատմամբ,
եթե՝

$$r(A) = r(s) = \min_{|B|=s} r(B) \quad (\bar{r}(A) = \bar{r}(s) = \min_{|B|=s} r(B)).$$

Աշխատանքում ստացված են $r(s)$, $\bar{r}(s)$ մեծությունների համար ասիմպտոտիկ գնահատականներ, ինչպես նաև S և n պարամետրերի որոշակի արժեքների համար ստացված է նրանց ճիշտ ասիմպտոտիկան:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

¹ Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн, Теория кодов, исправляющих ошибки, Связь, М., 1979. ² Г. Л. Мовсисян, в сб.: Прикладная математика и математическое обеспечение ЭВМ, МГУ, 1980. ³ В. К. Леонтьев, Мат. заметки, т. 15, № 3 (1974).