Lecture 19: Hamming Sphere and Ball, Vector Space

Summary:
We explore Hamming spheres and balls, establishing formulas for their sizes and examining their role in error correction. We prove bounds on code size based on error-correcting capabilities and introduce vector spaces, defining their fundamental properties and operations. We demonstrate how these concepts provide a framework for understanding linear codes.

Topics Covered: Hamming ball, Hamming sphere, vector space

Proposition:

C is a code with Hamming distance $d(C)$

1. C detects up to s errors $\iff d(C) \geq s+1$
2. C corrects up to t errors $\iff d(C) \geq 2t+1$

Hamming sphere:

$$x \in \mathbb{F}_q^m, r \in \mathbb{N}$$

The Hamming sphere with center x and radius r is denoted

$$S(x,r) = \{y \in \mathbb{F}_q^m \ : \ d(x,y) = r\}$$

Hamming ball:

$$B(x,r) = \{y \in \mathbb{F}_q^m \ : \ d(x,y) \leq r\}$$

Note that

$$|\mathbb{F}_q^m| = q^m$$

Example 1:

$$x = (1,1) \in \mathbb{F}_2^2, \ r = 1$$

$$S(x,r) = \{(0,1),(1,0)\}$$

$$B(x,r) = \{(1,1),(0,1),(1,0)\}$$

Suppose we have $r = 2$. Then, we get

$$S(x,r) = \{(0,0)\}$$

$$B(x,r) = \mathbb{F}_2^2$$

Example 2:

$$x = (a,b,c,d) \in \mathbb{F}_q^4, \ r = 2$$

Lemma:

$$|S(x,r)| = \binom{m}{r}(q-1)^r$$

$$|B(x,r)| = \sum_{i=0}^{r} \binom{m}{r}(q-1)^i$$

Note that

$$B(x,r) = \bigsqcup_{i=0}^{r} S(x,i)$$

Binomial theorem:

binomial theorem

- tags
  - math
  - CS
- related
  - binomial coefficients

Theorem 23.1 — Binomial Theorem.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

$$(x+y)^n = \underbrace{(x+y)(x+y)\dots(x+y)}_{n \text{ times}}.$$

Fact D.2. (Binomial theorem) Let n be a positive integer. Then for any x, y,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{D.10}$$

Theorem:

Let $C \subseteq \mathbb{F}_q^m$ be a code of size $M = |C|$.

Suppose that C corrects up to t errors.

Then,

$$M \sum_{i=0}^{t} \binom{m}{i} (q-1)^i \leq q^m$$

$$M \leq \frac{q^m}{\sum_{i=0}^{t} \binom{m}{i} (q-1)^i}$$

Proof:

Since C corrects up to t errors, we know that $d(C) \geq 2t+1$.

$$\implies y_1, y_2 \in C,\ y_1 \neq y_2,\ d(y_1, y_2) \geq 2t+1 \implies$$

$$B(y,t) \cap B(y_2,t) = \emptyset$$

$$a \in B(y_1,t) \cap B(y_2,t)$$

$$d(y_1,y_2) \subseteq d(y-1,a) + d(a,y_2) \leq 2t$$

Note that

$$|\mathbb{F}_q^m| = q^m$$

points

For each of the M elements of C, we have a ball of radius t around it with

$$\sum_{i=1}^{t} \binom{m}{i} (q-1)^i \leq q^m$$

Example:

$C \subseteq \mathbb{F}_2^{10}$ code that corrects up to 2 errors. Show that $|C| \leq 18$.

Solution:

$$|C| \left(\sum_{i=0}^{2} \binom{10}{i} \right) \leq 2^{10}$$

$$\binom{10}{0} + \binom{10}{1} + \binom{10}{2}$$

$$|C| \leq \frac{1024}{56} = 18.3$$

Definition:

A vector space is a set $\mathcal{V}$ over a field $\mathbb{F}$ with a binary operation $+$ on $\mathcal{V}$ and a scalar multiplication operation $\cdot : \ \mathbb{F} \times \mathcal{V} \to \mathcal{V}$ such that

1. $\forall u, v \in \mathcal{V}. \ u + v \in \mathcal{V}$
2. $\forall u, v, w \in \mathcal{V}. \ (u + v) + w = u + (v + w)$
3. $\exists \vec{0} \in \mathcal{V}. \ \forall v \in \mathcal{V}. \ \vec{0} + v = v$
4. $\forall v \in \mathcal{V}. \ \exists (-v) \in \mathcal{V}. \ v + (-v) = \vec{0}$
5. $\forall u, v \in \mathcal{V}. \ . u + v = v + u$
6. $\forall a \in \mathbb{F}. \forall v \in \mathcal{V}. \ \ av \in \mathcal{V}$
7. $\forall a, b \in \mathbb{F}. \ \forall v \in \mathcal{V}. \ a(bv) = (ab)v$
8. $\forall a, b \in \mathbb{F}. \ \forall v \in \mathcal{V}. \ (a + b) \cdot v = av + bv$
9. $\forall a \in \mathbb{F}. \ \forall u, v \in \mathcal{V}. \ a(u + v) = au + av$
10. $\forall v \in \mathcal{V}. \ 1 \cdot v = v$