IIIT Hyderabad | **Scribed By: Chigullapally Rasagna(20171003)**
Introduction to Coding Theory | **Lecture #3**
Instructor: Dr. Prasad Krishnan | **28-1-20**

Outline. *Unique decoding in worst case error model and Hamming bound(HB).*

1 Worst Case Error Model

In this model we assume that out of n symbols, atmost t can be altered by the channel to some other symbols (atmost t errors occur)

$$d_H(\underline{x}, \underline{y}) \leqslant t \leqslant n$$

$\underline{y}$ is the received vector.

Lemma 1. *A code C can correct any t-errors under minimum Hamming distance decoder iff*

$$d(C) \geqslant 2t + 1$$

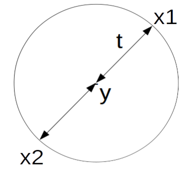
Proof. **If part** :
Given : $d(C) \geqslant 2t + 1$
To show : Decoding is correct (Unique Decoding)
For Unique decoding, no 2 codewords should exist which are at distance $\leqslant t$ from $\underline{y}$(received vector)
Suppose correct coding is not guaranteed then $\exists\ \underline{y} \in X^n$ s.t $\underline{x_1}, \underline{x_2} \in C$ exist such that

$$d_H(\underline{x_1}, \underline{y}) \leqslant t$$

$$d_H(\underline{x_2}, \underline{y}) \leqslant t$$

$$\Rightarrow d_H(\underline{x_1}, \underline{x_2}) \leqslant d_H(\underline{x_1}, \underline{y}) + d_H(\underline{x_2}, \underline{y}) \leqslant 2t$$

This contradicts the given statement, so, decoding should be correct.
Only if part :
Given : Correct Decoding
To show : $d(C) \geqslant 2t + 1$
(By Contradiction) Let us assume that $d(C) < 2t + 1$



From the figure we can observe that 2 codewords exist which are at distance $\leqslant t$ from $\underline{y}$(Unique decoding is not possible).
This contradicts the given statement, so, $d(C) \geqslant 2t+1$.
Hence proved. □

- Information conveyed is $log_{|X|}|C|$ X-symbols.
- Rate $\mathbf{R} = \dfrac{log_{|X|}|C|}{n}$ $(R \leqslant 1)$
- If d(C) = d, then we can correct upto $\lfloor \dfrac{d-1}{2} \rfloor$ errors surely.

Example 1.1. *Repetition code:*

$$C = \{(0,0,...,0),(1,1,...,1)\}$$

$$R = \frac{1}{n}, d(C) = n, t = \lfloor \frac{n-1}{2} \rfloor$$

2 Hamming Bound

Theorem 1. *(Sphere Packing Bound) Let $C \subseteq X^n$ $(|X| = q)$ be a code with $d(C) = d$ then*

$$|C| \leqslant \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}$$

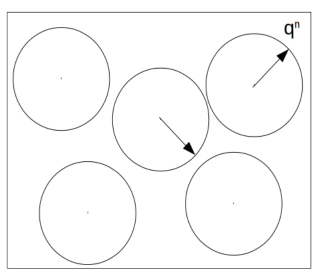


Figure 1: Non-intersecting Hamming balls with radius $r = \lfloor \frac{d-1}{2} \rfloor$

Proof. Hamming ball -

$$B(\underline{c}, \lfloor \frac{d-1}{2} \rfloor) \triangleq \{\underline{v} \in X^n : d_H(\underline{v}, \underline{c}) \leqslant \lfloor \frac{d-1}{2} \rfloor\}$$

$$B(\underline{c}, \lfloor \frac{d-1}{2} \rfloor) \cap B(\underline{c^1}, \lfloor \frac{d-1}{2} \rfloor) = \emptyset \qquad \forall \underline{c}, \underline{c^1} \in C$$

$$\Rightarrow \sum_{\underline{c} \in C} |B(\underline{c}, \lfloor \frac{d-1}{2} \rfloor)| \leqslant q^n$$

$$\Rightarrow \sum_{\underline{c} \in C} \left(\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right) \leqslant q^n$$

$$\Rightarrow |C| \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leqslant q^n$$

$$\Rightarrow |C| \leqslant \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}$$

$$Hence\ Proved.$$

□

- Codes which meet Hamming Bound with equality are called **Perfect Codes**.