IIIT Hyderabad **Scribed By: MEHTHAB SHAIK(20161205)**
Intro to Coding Theory (ECE539) **Lecture #4**
Instructor: Dr. Prasad Krishnan **17-1-20**

Hamming Bound. *Properties(inequalities/bounds) proofs.*

1 First Part

$$d_H(x1, x2) \leq d_H(x1, y) + d_H(x2, y) \leq 2t$$

•Contradiction to given statement
•Decoding should be correct

Only if :

$$Gn : Correct \quad decoding$$

To show :

$$d(\mathcal{C}) \geq 2t + 1$$

Info conveyed $log_2|\mathcal{C}|$ bits

$$c \in \mathcal{C}\,(n \quad time \quad slots)$$

$$log_{|\mathcal{X}|}|\mathcal{C}| \quad : \mathcal{X} - symbols$$

Rate R = $\frac{log_{|x_1|}|\mathcal{C}|}{n}$ (X - symbols per time slot)

To compare 2 different codes info conveyed is not sufficient. n should also be taken into picture .

$$R \leq 1$$

Rate does not tell about error correcting capabilities.

Better compression → Reduces Quality

2 Rate Adaptation

- Given, $d(\mathcal{C})$ = we can correct upto $\lfloor \frac{d-1}{2} \rfloor$ errors surely.
- Trade - off the error correcting capability and rate.
- Suppose n is fixed what is the trade-off b/w d & $|\mathcal{C}|$?

Theorem : Hamming Bound

Let $|\mathcal{X}| = q$; let $\mathcal{C} \subseteq x_n$ be a code with $d\mathcal{C}$

then

$$|\mathcal{C}| \quad \leq \quad \frac{q^n}{\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}$$

(shpere packing bound for hamming metric)

Proof :

$$|\mathcal{C}| \left(\Sigma_{i=0}^{t} \binom{n}{i} (q-1)^i \right) \quad \leq \quad q^n$$

$\Rightarrow$

$$|\mathcal{C}| \quad \leq \quad \frac{q^n}{\Sigma_{i=1}^{t} \binom{n}{i} (q-1)^i}$$

$$B * \left(C, \lfloor \frac{d-1}{2} \rfloor \right) := \quad \{ v \in \mathcal{X}^n : d_H(v, c) \leq \lfloor \frac{d-1}{2} \rfloor \quad \}$$

$$B * \left(C, \lfloor \frac{d-1}{2} \rfloor \right) \cap B * \left(C', \lfloor \frac{d-1}{2} \rfloor \right) = \phi \quad \forall \quad C, C' \in \mathcal{C} \, (distinct)$$

$$\Sigma_{C \in \mathcal{C}} \quad |B * \left(C, \lfloor \frac{d-1}{2} \rfloor \right)| \leq q^n$$

$$\Rightarrow \quad \Sigma_{C \in \mathcal{C}} \left(\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right) \leq q^n$$

$$\Rightarrow \quad |\mathcal{C}| \left(\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right) \leq q^n$$

$$\Rightarrow \quad |\mathcal{C}| \leq \frac{q^n}{\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}$$

Hamming Bound $\rightarrow$ upper bound on $|\mathcal{C}|$ such that C has $d_{min} = d \quad \& length = n$

• Perfect codes meet hamming bound with equality

• Repetition code

$$d(\mathcal{C}) = q \quad \frac{q^n}{\Sigma_{i=0}^{\left(\frac{q}{2}-1\right)} \binom{n}{i} (q-1)^i}$$

3 Lecture 4

- $\mathcal{C} \subseteq \mathcal{X}^n \quad |\mathcal{X}| = q$
- $d(\mathcal{C}) \rightarrow minimum \quad distance \quad of \quad the \quad code$
- $d(\mathcal{C}) = d \Leftrightarrow \quad \lfloor \frac{d-1}{2} \rfloor \quad errors \quad are \quad surely \quad corrected$
- $R(\mathcal{C}) = \frac{\log_q |\mathcal{C}|}{n}$

$(Normalized \quad amount \quad of \quad information \quad sent \quad through \quad the \quad channel \quad) \Rightarrow \quad more \quad rate$

• Hamming Bound :C is a n-length code with d(C)=d over a q-ary alphabet

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

$\bullet |e_{max}| = A(n,d,q)$

$\bullet A \quad n-length \quad code \quad with \quad d(\mathcal{C}) = d \quad over \quad aq-ary \quad alphabet \quad is (n,d)_q code.$

$A \quad (n,d)_q \quad code \quad \mathcal{C} \quad is \quad perfect \quad if \quad it \quad satisfies \quad H-bound \quad with \quad equality \quad .$

$Eg:- \quad (n, d=n)_2 \quad code \quad (Repetition \quad code) \quad n = odd$

$$e_{rep} = \{(0,0,...,0),(1,1,...,1)\}$$

$$|\mathcal{C}| \quad = \quad 2 \qquad \frac{q^n}{\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i} \quad = \frac{2^n}{\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} (q-1)^i} = 2$$

$$\Rightarrow \quad |\mathcal{C}| = \frac{q^n}{\Sigma_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i} \quad \Rightarrow \quad perfect \quad code$$

$Eg:- \quad (n, d=n)_q \quad code$

$$\mathcal{C} \quad = \quad \{(i_0, i_1, ...i_x)\, i \in \mathcal{X}\}$$

- $\underline{Singleton \quad bound}: -$ $Let \quad \mathcal{C} \quad be \quad a \quad (n,d)_q \quad code. \quad Then$

$$|\mathcal{C}| \leq q^{n-d+1}$$

$Proof: -$

$$1 \leq d \leq n$$

$(d-1) \quad columns \quad are \quad ignored.$

$rows \quad of \quad this \quad punctured \quad table \quad remain \quad unique.$

rows of this table differ in atleast d position .

$This \quad process \quad of \quad removing \quad columns \quad is \quad calld \quad puncturing.$

$\Rightarrow \quad totally \quad |\mathcal{C}| \quad still \quad remian.$

$\Rightarrow \quad \leq q^{n-d+1}$

(max no. of unique vectors of length n-d+1)

•For $d = n$ rep. code meets singleton bound with equality

•Maximum distance seperable codes(MDS) :-

$(n,d)_q$code which meets singleton bound with equality

•$\underline{LowerBound}: -(Gilbert - Varshamov)\,(G-V) \quad bound$

$Let \quad A\,(n,q,d) \quad$ be the maximum coordinality of any $\quad (n,d)_q \quad .Then,$

$$A\,(n,d,q) = \frac{q_n}{\Sigma_{i=0}^{d-1}\binom{n}{i}(q-1)^i}$$

$(shpere \quad covering \quad bound)$

Sphere can overlap but the centre of one sphere can not lie inside another sphere.

Proof:-Let $\quad e_{max} \quad be \quad (n,d)_q \quad code \quad with \quad |\mathcal{C}|_{max} = A\,(n,d,q)$

$|B * (c, d-1)\,| = \Sigma_{i=0}^{d-1}\binom{n}{i}(q-1)^i$ Then,

$$\bigcup_{c \in \mathcal{C}} B * (c, d-1) = \mathcal{X}^n$$

If there is a vector in $\mathcal{X}^n$ which does not belong to the union .

$\Rightarrow$ we add that vector to code.(as minimum distance is not changed)

$\Rightarrow$ Our code is not a maximum cardinality code

$\Rightarrow$ contradiction

$\Rightarrow$ Such a vector does not exist,

$\Rightarrow \Sigma_{c\in\mathcal{C}}|B*(c,d-1)\,| \geq q^n$

$\Rightarrow \quad A\,(n,d,q) \geq \frac{q_n}{\Sigma^{d-1}i=0\binom{n}{i}(q-1)^i}$

- For q=2,

$$\frac{2^n}{\Sigma_{i=0}^{d-1}\binom{n}{i}} \qquad \leq A\,(n,d,q=2) \quad \leq \quad \frac{2^n}{\Sigma_{i=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{n}{i}}$$

This is called 'sandwich property'

- *Behaviour of the bounds as n grows larger:-*

$$n|d=\partial n \quad \partial d=\frac{d}{n} \quad (relative \quad distance) \quad is \quad kept \quad const \in (0,1)$$

what happens to te inequality above ?

$$2^{nH(\lambda)} \leq A\,(n,q=2,d) \leq \quad 2^{nH\left(\frac{\lambda}{2}\right)}$$

References

[1] None