29/1/2021 Lecture 7 (Standard array decoding, Syndrome decoding)

Standard Array

A standard array for a linear code is a listing of the code & all its cosets in the form of any array.

Decoding using the standard array (Minimum Distance decoding)

→ Find the coset to which the received vector belongs to

→ Find the coset leader & call it $\underline{e}$

→ $\hat{\underline{c}} = \underline{y} - \underline{e}$.

Unique Coset Leader

Any nonzero vector of Hamming weight $\leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ is always a unique coset leader in that coset

Proof by Contradiction:- If there are two nonzero vector of Hamming wt $\leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ in the same coset.

$$w_H(\underline{e}_1) \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$$

$$w_H(\underline{e}_2) \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$$

$\underline{e}_1$ and $\underline{e}_2$ belong to the same coset

$$w_H(\underline{e}_1 - \underline{e}_2) \leq w_H(\underline{e}_1) + w_H(-\underline{e}_2) \quad \text{(Triangle Inequality)}$$

$$= \left\lfloor \frac{d_{min}-1}{2} \right\rfloor \cdot 2$$

$$< d_{min}. \quad \text{(Contradicts the definition of } d_{min}\text{)}.$$

$$\underline{e}_1 - \underline{e}_2 \in \mathbb{C}.$$

Correctable Error Patterns.

Coset Leaders are the only error patterns which can be corrected.

Probability of error if $\underline{c}$ is transmitted.

$$P_e(\underline{c}) = \sum_{\substack{\underline{y}:\ \underline{y}-\underline{c} \text{ is not a} \\ \text{coset leader.}}} P(\underline{y} \mid \underline{c}).$$

$$= \sum_{\substack{\underline{e}:\ \underline{e} \text{ is not} \\ \text{a coset leader.}}} P(\underline{e}+\underline{c} \mid \underline{c}).$$

$$= \sum_{\substack{\underline{e}:\ \underline{e} \text{ is not a} \\ \text{coset leader}}} P(\underline{e}) \quad \left(\text{Because } \underline{e} \text{ is independent of } \underline{c}\right).$$

Number of $\underline{e}$ which are not coset leaders
(non zero $\underline{e}$).

$$q^n - q^{n-k}.$$

<u>Storage Complexity</u> $\sim q^n$.

If there is a better way of identifying a coset to which the received vector y belongs, then storage complexity will be better

<u>Syndrome Decoding</u>

Let H be a $(n-k) \times n$ matrix of $\mathbb{C}$.

<u>Defn</u>:- The syndrome of received vector $\underline{y}$ is defined as $\underline{s} = H\underline{y}$.

$$\underset{(n-k)\times 1}{\underline{s}} = H_{(n-k)\times n}\, \underline{y}_{n\times 1}.$$

No. of possible distinct syndromes are.

$$q^{n-k}.$$

Syndrome vector $\Longleftrightarrow$ Coset

uniquely maps

Two vectors $\underline{y}_1$ and $\underline{y}_2 \in \mathbb{F}^n$ are in the same coset of $\mathbb{C}$ iff they have the same syndrome.

$$H\underline{y}_2 - H\underline{y}_1 = H(\underline{y}_2 - \underline{y}_1) \rightarrow$$

$$= H\underline{c} = \underline{0}.$$

Property of parity check matrix.

$\underline{y}_2$ & $\underline{y}_1$ are in the same coset iff $\underline{y}_2 - \underline{y}_1 \in \mathbb{C}$.

Syndrome Decoding steps.

1. Compute $\underline{s} = H\underline{y}$.
2. Find out coset leader $\underline{e}$ corresponding to the syndrome vector $\underline{s}$ (Look Up Table).
   Size of the look up table is $2q^{n-k}$.
3. decode $\hat{c} = \underline{y} - \underline{e}$.

Lemma:- A linear code with minimum distance d is t-error correcting for any $t \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ (It can correct upto t errors).

Hamming Bound for Linear Codes

Theorem:-

Consider an (n, k) linear code over $\mathbb{F}$.

It is t-error correcting. Then,

$\left(t \le \left\lfloor \frac{d_{min}-1}{2} \right\rfloor\right)$ $$\boxed{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \le q^{n-k}.}$$

Proof:- Standard Array Table

We said that correctable error patterns are exactly the coset leaders.

LHS is a number corresponding to subset of correctable error patterns.

$$\binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \cdots + \binom{n}{t}(q-1)^t \le \underline{\underline{q^{n-k}}}$$

Perfect Code

A t-error correcting code is said to be a perfect code if it satisfies Hamming bound with equality.

→ To understand when there can be inequality in Hamming bound. - When the code can correct some error patterns of weight $t+1$.

→ For perfect code, the code can correct all error patterns upto weight t and it cannot correct any error pattern of weight $t+1$.

Examples of Perfect Codes

① $(n, 1, n)$ binary repetition code. (n odd)

$$\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} = \frac{1}{2} \sum_{i=0}^{n} \binom{n}{i} = 2^{n-1} = 2^{n-k}.$$

② $(7, 4, 3)$ Hamming Code.

$$\binom{7}{0} + \binom{7}{1} = 8 = 2^{7-4}.$$

Binary Hamming Codes (Family of Codes).

Binary Hamming Code parameterized by $m \geq 1$, is specified by a parity check matrix whose columns are all nonzero m tuples.

Question - What is the size of this parity check matrix?

$$(m \times (2^m - 1))$$

$$\begin{bmatrix} \underline{h}_1 & \underline{h}_2 & \cdots & \underline{h}_{2^m-1} \end{bmatrix}$$

$$\underline{h}_i \neq \underline{h}_j; \quad i \neq j$$

What is the minimum distance of this code?

Minimum distance $= 3$.

Any two columns are distinct

$\exists$ a set of 3 columns of H which are linearly independent.

Hamming Code $(2^m - 1, 2^m - 1 - m, 3)$.

Hamming Codes are perfect Codes

$$\left[2^m-1,\ 2^m-1-m,\ 3\right].$$

$$\binom{2^m-1}{0}+\binom{2^m-1}{1} = 2^m$$

$$\underline{1+2^m-1 = 2^m}$$

Hamming Codes,

Golay Codes

$(23, 12, 7)$ and $(11, 6, 5)$

are perfect

$\rightarrow$ No other Codes are perfect