Lecture 21: Linear Codes

Summary:
We examine linear codes and their representation through generator and parity-check matrices. We prove that the minimum distance of a linear code equals its minimum weight, and establish the Singleton bound. We demonstrate how to construct parity-check matrices from generator matrices and explore their role in error detection and correction.

Topics Covered: generator matrix, linear code, parity-check matrix, singleton bound, subspace

Proposition:

For a linear code C, we have

$$d(C) = \min\{w(y) \ : \ y \in C, \ y \neq 0\}$$

Today:

- Linear codes
- Generator matrix
- Parity-check matrix $\to$ decoding
    - This has nothing to do with parity-check code

$n \leq m$, n lengths of the messages, $\dim C = n$, m is the length of code words.

Definition:

Let C be an $[m, n)$ code and let G be an $n \times m$ matrix.

G is a generator matrix for C is $C = \text{rowspace}(G)$.

Since $\dim C = n, \text{rank}(G) = n \implies G$ is a full rank matrix, meaning the rows are linearly independent.

$$\tilde{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$x \mapsto xG$$

$$\text{im}(\tilde{T}) = C, \quad \text{by definition}$$

Example:

$$C = \{0000, 1101, 1010, 0111\} \subseteq \mathbb{F}_2^4$$

Note that this is a linear code, meaning it is a vector subspace.

Here, $m = 4$ and $n = 2$. n is the length of messages and m is the lengths of codewords.

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

The rows form a basis for C.

Definition:

Let C be an $[m, n]$ code and let H be an $(m-n) \times m$ matrix. We say that H is a **parity check matrix** for C when $C = \text{null}(H)$.

H will be our way of decoding.

$$\text{row}(G) = C = \text{null}(H)$$

$$C = \text{null}(H) = \{y \in \mathbb{F}_q^m \ : \ Hy = 0\} \subseteq \mathbb{F}_q^m$$

$$\dim C = n, \ \dim(\text{null}(H)) = n$$

A $n \times m$ matrix with $n \leq m$ and $\text{rank}(A) = n$. Rows are a basis of $\text{row}(A)$.

$$\tilde{\text{null}} = 0$$

is the kernel of $\tilde{T} : \mathbb{F}^n \to \mathbb{F}^m$. $\tilde{T}$ is injective.

Problem:

Given a full rank $n \times m$ matrix A, find a matrix B such that

$$\text{row}(A) = \text{null}(B)$$

We will use row operations to get from A to A', where

$$A = \{\underbrace{I_n}_{n} \; : \; \underbrace{M}_{m-n}\}$$

$$B = \left[\underbrace{-M^t}_{n} \mid \underbrace{I_{m-n}}_{m-n}\right]$$

Claim:

$$\text{null}(B) = \text{row}(A') = \text{row}(A)$$

For example, we have the following generator:

$$H = [-M^t \; : \; I_{m-n}] = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Theorem:

Let H be a parity check matrix for a linear code C.

Then,

$$d(C) = \text{the smallest size of a linearly dependent set of columns of H}$$

Proof:

We proved that for a linear code C, $d(C) = \min\{w(y) \; : \; y \in C, y \neq 0\}$. By assumption $y \in C \iff Hy = 0$.

Corollary - Singleton bound:

Let C be an $[m, n]$ code. Then,

$$d(C) \leq m - n + 1$$

Proof:

$$\text{rank}(H) = m - n$$

$$\implies \text{any m - n + 1 columns are linearly dependent}$$

$$\text{QED}$$

Lemma:

Let C be a linear code and H be a parity check matrix for it. When receiving the word z, we detect an error exactly when $Hz \neq 0$.

Proof:

$$C = \text{null}(H), \; z \in C \iff Hz \neq 0$$

$$\text{QED}$$

How do we decode: we pick the closest codeword to z!

Recall that given a finite group G and finite subgroup H, we have

$$x \sim_H y \iff xy^{-1} \in H$$

is an equivalence relation on G. Thus, it partitions G, and we proved while proving Lagrange's theorem, that we get classes of the form Hx.

We will apply the previous to $(C, +)$ viewed as a finite subgroup of a finite group $(\mathbb{F}_q^m, +)$.

$$C = \{0000, 1101, 1010, 0111\}$$

$$1000 + C = \{1000, 0101, 0010, 1111\}$$

$$0100 + C = \{0100, 1001, 1110, 0011\}$$

$$0001 + C = \{0001, 1100, 1011, 0110\}$$