Lecture 22: Syndrome Decoding, Single Errors

Summary:
We explore syndrome decoding for linear codes, establishing a systematic method for error correction. We prove that syndrome decoding identifies the closest codeword to a received word and examine conditions for detecting and correcting single errors. We demonstrate how the columns of a parity-check matrix determine the error-correcting capabilities of a code.

Topics Covered: coset decoding, generator matrix, parity-check matrix, single bit error in a linear code, syndrome decoding

Proposition:

Given word $z \in \mathbb{F}_q^m$, we do the following:

1. Locate the coset $c + C$ of C, such that $c + C \ni z$
2. Among the elements of $v + C$, find an element e of lowest weight
3. Decode $y' = z - e$

Then, $y' \in C$, and no other codeword is closer to z than y'

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

- y is what we send
- z is what receive
- y' is what we decode into

Proof:

$z, e \in v + C$, $z = x + y_1$, $e = x + y_2$, $x_1, y_2 \in C$.

$$y' = z - e = y_1 - y_2 \in C$$

Since $z \in v + C$ and $y'' \in C$, we know that

$$z - y'' \in v + C$$

$$d(z, y'') = w(z - y'')$$

Note that $z - y'' \in v + C$ and $e \in v + C$ is the lowest weight element. Therefore, we have

$$d(z, y'') = w(z - y'') \geq w(e) = d(z, y')$$

$$\text{QED}$$

Proposition (Syndrome decoding):

C is a linear code and H is a parity check matrix for C.

Let z, e as in previous proposition. Then,

$$Hz = He$$

and none of the lowest weight vectors e' coming from the cosets other than $v + C \in z$ satisfy $Hz = He'$.

Example:

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

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

$$Hz = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = He$$

$$He_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$He_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$He_3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Proof:

$$z - e \in C = \text{null}(H) \implies H(z-e) = 0 \implies Hz = He$$

Let e' be the lowest weight vector in the coset that doesn't contain z

$$\implies z - e' \notin C$$

$$H(z - e') \neq 0$$

$$\implies Hz \neq He'$$

$$\text{QED}$$

Proof:

Given a linear code C, we calculate the cosets and choose a lowest weight vector in each coset (those will do the decoding). For each lowest weight vector e (of which there are $\frac{q^m}{|C|}$ many), we calculate and store He. These are called the syndromes of the code.

When we receive a word $z \in \mathbb{F}_q^m$, we do the following to decode:

1. Compute Hz
2. Search through the syndromes to find e for which $Hz = He$
3. Decode to $y' = z - e$

> The rest of the lecture is over $\mathbb{F}_2$.

Denote the standard basis as:

$e_1 = (1, 0, \ldots, 0, e_2 = (0, 1, 0, \ldots, 0)$, ..., $e_m = (0, \ldots, 0, m)$.

This is a basis of $\mathbb{F}_2^m$.

Proposition:

Let C be a linear code with parity check matrix H. C detects a single error in bit $i \iff He \neq 0$.

He_i is the i^{th} column on H.

Proof:

$y \in C$. Suppose that, during transmission, exactly one error occurred and it is in bit i.

This implies that

$$z = y + e_i$$

We know that an error is detected $\iff Hz \neq 0$. This is because $C = \text{null}(H)$.

$$y \in C \implies Hy = 0$$

$$z \notin C = \text{null}(H)$$

$$Hz = H(y + e_i) = Hy + He_i \neq 0$$

Proposition:

Let C be a linear code with parity-check matrix H. Then, C can correct all single errors $\iff$ the columns of H are nonzero and distinct.

A single error means one bit is modified.

Proof:

We know that C corrects all single errors $\iff d(C) \geq 3$.