Review:

1. Error detection using $H$
   \[ \tilde{V} = \tilde{Y} + \tilde{e} \]
   \[ \tilde{S} = \tilde{Y} - H^T = (\tilde{Y} + \tilde{e}) - H^T = \tilde{Y} - H^T + \tilde{e} - H^T \]
   \[ = e \times 0 \]

2. Weight distribution
   Minimum weight
   probability of undetected error

3. Minimum distance
   and its connection to minimum weight and $H$

New:

1. Decoding:
   \[ \tilde{S} = \tilde{e} \cdot H^T \]
   \[ \Rightarrow \text{(n-k) equations, n unknown in } \tilde{e} \]
   \[ \text{1x(n-k) } \Rightarrow 2^k \text{ solutions} \]
   \[ \Rightarrow \text{pick the most likely one among } 2^k \text{ possible solutions.} \]
   \[ \text{eg: } (1111111) \text{ } \tilde{e} = p^6 \approx 10^{-12} \text{ } p = 10^{-1} \]
   \[ (000001) \text{ } \tilde{e} = p^5 \cdot (-p)^5 \approx 10^{-2} \text{ } \text{more likely.} \]
   \[ \Rightarrow \text{depends on channel model} \]

    \[ \tilde{V} = \tilde{e}^* + \tilde{V} \]

Eg: (7,3) code

\[ H = \begin{bmatrix} 00 & 10 & 11 \\ 01 & 10 & 11 \\ 00 & 01 & 011 \end{bmatrix}, \quad \tilde{V} = (1001011), \quad \tilde{V} = (1001001) \]

Find $\tilde{V}$.

A: \[ \tilde{S} = \tilde{V} \cdot H^T = (100) + (110) + (101) = (111) \]

\[ \tilde{S} = \tilde{e} \cdot H^T \Rightarrow (111) = (e_1, e_2, \ldots, e_7) \]

\[ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \]
\[ l = e_0 + e_3 + e_5 + e_6 \]
\[ 2^k = 2^4 = 16 \] solutions of \( e'. \)

possible solution: \((0000010) = \hat{e'} \in P \quad \text{(t-P)}^{n-\text{w(e')}} \)
\((01101100) \quad \text{Most likely} \)

\[
\hat{v} = y + \hat{e'}
\]
\[
= (1001001) + (\star\star\star\star1010)
\]
\[
= (1001011)
\]
\[
= v
\]

This approach is not used in practice, as \(2^k\) solutions is needed to find, too much work.

2) Another way for decoding

- These two columns are needed to be stored
- \( \hat{v}_1, \hat{v}_2, \ldots, \hat{v}_k \) \( \text{set of code word } C \)
- \( \hat{v}_1 + \hat{e}_2, \ldots, \hat{v}_k + \hat{e}_2 \) \( \text{of } C \)
- \( \hat{v}_1 + \hat{e}_3, \ldots, \hat{v}_k + \hat{e}_3 \) \( \text{of } C \)
- Suppose after \( m \) steps, all \( 2^n \) vectors are here.

Properties:
1. The sum of any two vectors in the same row will be a codeword.
2. Every two vectors in the same row are different.
3. Every two vectors in different rows are different.
4. All vectors in the same row have the same syndrome, \( \hat{e}_i \cdot H \)

Proof: Suppose a vector \( y \) appears in row \( s_1 \) and \( s_2 \) \( (s_1 < s_2) \)

\[
\hat{y} = \hat{e}_{s_1} + \hat{v}_i = \hat{e}_{s_2} + \hat{v}_j
\]

\[
\hat{e}_{s_2} = \hat{e}_{s_1} + \hat{v}_i + \hat{v}_j
\]
\[ \Rightarrow \mathbf{v}_i \oplus \mathbf{v}_j \text{ is a codeword and } \mathbf{e}_{s_1} = \mathbf{e}_{s_2} + \mathbf{v} \Rightarrow S_2 \text{ in row } s_1 \]

Contradict with the way the table was constructed.

Properties:

(5) Different rows have different syndromes.

Proof: Suppose row i and j have the same syndrome.

\[ \Rightarrow \mathbf{e}_i \cdot H^T = \mathbf{e}_j \cdot H^T \]

\[ \Rightarrow (\mathbf{e}_i + \mathbf{e}_j) \cdot H^T = 0 \]

\[ \Rightarrow \mathbf{e}_i + \mathbf{e}_j \text{ is a codeword: } \mathbf{e}_i + \mathbf{e}_j = \mathbf{v}_i \]

\[ \Rightarrow \mathbf{e}_j = \mathbf{e}_i + \mathbf{v}_i \]

\[ \Rightarrow \mathbf{e}_j \text{ is in row } i, \text{ contradict with our construction.} \]

(2) Decoding method (Rule)

\[ S_i = \mathbf{v}^T \cdot H^T \rightarrow \text{go to corresponding row } i \text{ that has syndrome } S_i \]

\[ \rightarrow \text{find } \mathbf{e}_i \]

\[ \rightarrow \mathbf{v} = \mathbf{v}^T + \mathbf{e}_i \]

Compute all the syndromes \( S_i = \mathbf{e}_i \cdot H^T \) beforehand for standard array.

(3) Decoding ability of this rule.

\( \mathbf{v} \) was sent, \( \mathbf{\tilde{v}} = \mathbf{v} + \mathbf{x} \) \( \mathbf{v} \) was received.

a. If \( \mathbf{\tilde{x}} \) is one of the coset leaders

\[ \mathbf{\tilde{v}} \cdot H^T = (\mathbf{\tilde{v}} + \mathbf{\tilde{x}}) \cdot H^T = \mathbf{\tilde{x}} \cdot H^T \]

we will find the value of \( \mathbf{\tilde{x}} \) correctly.

b. If \( \mathbf{\tilde{x}} \) is not a coset leader

\[ \mathbf{\tilde{x}} = \mathbf{e}_i + \mathbf{v}_i \]

\[ \mathbf{\tilde{v}} \cdot H^T = (\mathbf{\tilde{v}} + \mathbf{e}_i + \mathbf{v}_i) \cdot H^T = \mathbf{e}_i \cdot H^T \]

\[ \mathbf{\tilde{v}} = \mathbf{\tilde{v}}^T + \mathbf{e}_i = \mathbf{\tilde{v}}^T + \mathbf{e}_i + \mathbf{v}_i + \mathbf{\tilde{e}_i} = \mathbf{\tilde{v}}^T + \mathbf{v}_i \]
We should pick \( \varepsilon \)'s that are more likely happen. Pick \( \varepsilon \)'s with small weight.

Eq. (6.3) code

\[
\frac{1}{2} = 1 \cdot \mathbf{\varepsilon}
\]

\[
\mathbf{C} = \mathbf{\varepsilon} \cdot \mathbf{G}
\]

Error detection \( \mathbf{S} = \mathbf{Y} \cdot \mathbf{H}^T \)

Error decoding

\[
\mathbf{G} = \begin{bmatrix}
\mathbf{P}_{\text{rx}(n-k)} & \mathbf{I}_k
\end{bmatrix}
\]

Next Question: How to construct \( \mathbf{P}_{\text{rx}(n-k)} \)?

\[\Rightarrow\text{Chap 5. Cyclic code } \mathbf{G} = \begin{bmatrix}
\mathbf{P}_{\text{rx}(n-k)} & \mathbf{I}_k
\end{bmatrix}\]

Reduce design space.

Chap 5

5.1 Definitions

- Right cyclic-shift (or simply cyclic-shift)

\[
\mathbf{V} = (V_0, V_1, \ldots, V_{m})
\]

\[
\mathbf{V}^{(1)} = (V_{m}, V_0, V_1, \ldots, V_{m-2})
\]

\[
\mathbf{V}^{(2)} = (V_{m-1}, V_m, V_0, V_1, \ldots, V_{m-3})
\]

\[
\vdots
\]

\[
\mathbf{V}^{(i)} = (V_{m-i}, V_{m-i+1}, \ldots, V_{m-1}, V_0, \ldots, V_{m-i-1})
\]
2 Cyclic code

An \((n,k)\) linear code is called a cyclic code if every cyclic shift of a codeword in \(C\) is also a codeword in \(C\).