Lecture #4: Decoding of linear block codes
Decoding of linear block codes

Basic idea:
- The received vector $r$ has $2^n$ possibilities, regardless of what codeword is transmitted.

Any decoding scheme used at the receiver is a rule to partition the $2^n$ possible received vectors into $2^k$ disjoint subsets $D_1, D_2, \cdots, D_{2^k}$, such that the codeword $v_i$ is contained in the subset $D_i$ for $1 \leq i \leq 2^k$. 
Decoding of linear block codes

Basic idea:
- The received vector $r$ has $2^n$ possibilities, regardless of what codeword is transmitted.
- Any decoding scheme used at the receiver is a rule to partition the $2^n$ possible received vectors into $2^k$ disjoint subsets $D_1, D_2, \cdots, D_{2^k}$, such that the codeword $v_i$ is contained in the subset $D_i$ for $1 \leq i \leq 2^k$.
- The partition is based on linear structure of the code.

Let $v_1 = 0, v_2, \cdots, v_{2^k}$ be the $2^k$ codewords in an $(n, k)$ linear block code.
Decoding of linear block codes

Let \( \mathbf{v}_1 = 0, \mathbf{v}_2, \cdots, \mathbf{v}_{2^k} \) be the \( 2^k \) codewords in an \((n, k)\) linear block code.

Form an array of vectors from vector space, \( V_n \) as follows:

(i) Arrange the \( 2^k \) codewords as the top row of the array with \( \mathbf{v}_1 = 0 \) as the first element.
Decoding of linear block codes

Let $\mathbf{v}_1 = \mathbf{0}, \mathbf{v}_2, \cdots, \mathbf{v}_{2^k}$ be the $2^k$ codewords in an $(n, k)$ linear block code.

Form an array of vectors from vector space, $V_n$ as follows:

(i) Arrange the $2^k$ codewords as the top row of the array with $\mathbf{v}_1 = \mathbf{0}$ as the first element.

(ii) Suppose $j - 1$ rows of the array have been formed. Choose a vector $\mathbf{e}_j$ from $V_n$ which is not in the previous $j - 1$ rows.

(iii) Form the $j^{th}$ row by adding $\mathbf{e}_j$ to each codeword $\mathbf{v}_i$ in the top row and placing $\mathbf{e}_j + \mathbf{v}_i$ under $\mathbf{v}_i$. 
Decoding of linear block codes

- Let $\mathbf{v}_1 = 0, \mathbf{v}_2, \cdots, \mathbf{v}_{2^k}$ be the $2^k$ codewords in an $(n, k)$ linear block code.
- Form an array of vectors from vector space, $V_n$, as follows:
  1. Arrange the $2^k$ codewords as the top row of the array with $\mathbf{v}_1 = 0$ as the first element.
  2. Suppose $j - 1$ rows of the array have been formed. Choose a vector $\mathbf{e}_j$ from $V_n$ which is not in the previous $j - 1$ rows.
  3. Form the $j^{th}$ row by adding $\mathbf{e}_j$ to each codeword $\mathbf{v}_i$ in the top row and placing $\mathbf{e}_j + \mathbf{v}_i$ under $\mathbf{v}_i$.
  4. Continue until all the vectors from $V_n$ appear in the array.

The array is called a *standard array*.
Decoding of linear block codes

<table>
<thead>
<tr>
<th>( \mathbf{v}_1 = 0 )</th>
<th>( \mathbf{v}_2 )</th>
<th>( \cdots )</th>
<th>( \mathbf{v}_i )</th>
<th>( \cdots )</th>
<th>( \mathbf{v}_{2k} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbf{e}_2 )</td>
<td>( \mathbf{e}_2 + \mathbf{v}_2 )</td>
<td>( \cdots )</td>
<td>( \mathbf{e}_2 + \mathbf{v}_i )</td>
<td>( \cdots )</td>
<td>( \mathbf{e}<em>2 + \mathbf{v}</em>{2k} )</td>
</tr>
<tr>
<td>( \mathbf{e}_3 )</td>
<td>( \mathbf{e}_3 + \mathbf{v}_2 )</td>
<td>( \cdots )</td>
<td>( \mathbf{e}_3 + \mathbf{v}_i )</td>
<td>( \cdots )</td>
<td>( \mathbf{e}<em>3 + \mathbf{v}</em>{2k} )</td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( \mathbf{e}_{2^{n-k}} )</td>
<td>( \mathbf{e}_{2^{n-k}} + \mathbf{v}_2 )</td>
<td>( \cdots )</td>
<td>( \mathbf{e}_{2^{n-k}} + \mathbf{v}_i )</td>
<td>( \cdots )</td>
<td>( \mathbf{e}<em>{2^{n-k}} + \mathbf{v}</em>{2k} )</td>
</tr>
</tbody>
</table>

Standard array

For a \((6, 3)\) linear code generated by the following matrix,

\[
\mathbf{G} = \begin{bmatrix}
\mathbf{g}_0 \\
\mathbf{g}_1 \\
\mathbf{g}_2
\end{bmatrix} = \begin{bmatrix}
0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

standard array is shown in next two slides.
Decoding of linear block codes

<table>
<thead>
<tr>
<th>Coset Leader $\mathbf{v}_1$</th>
<th>$\mathbf{v}_2$</th>
<th>$\mathbf{v}_3$</th>
<th>$\mathbf{v}_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0 0 0 0 0 0)</td>
<td>(0 1 1 1 0 0)</td>
<td>(1 0 1 0 1 0)</td>
<td>(1 1 0 0 0 1)</td>
</tr>
<tr>
<td>(1 0 0 0 0 0)</td>
<td>(1 1 1 1 0 0)</td>
<td>(0 0 1 0 1 0)</td>
<td>(0 1 0 0 0 1)</td>
</tr>
<tr>
<td>(0 1 0 0 0 0)</td>
<td>(0 0 1 1 0 0)</td>
<td>(1 1 1 0 1 0)</td>
<td>(1 0 0 0 0 1)</td>
</tr>
<tr>
<td>(0 0 1 0 0 0)</td>
<td>(0 1 0 1 0 0)</td>
<td>(1 0 0 1 0 0)</td>
<td>(1 1 1 0 0 1)</td>
</tr>
<tr>
<td>(0 0 0 1 0 0)</td>
<td>(0 1 1 0 0 0)</td>
<td>(1 0 1 1 1 0)</td>
<td>(1 1 0 1 0 1)</td>
</tr>
<tr>
<td>(0 0 0 0 1 0)</td>
<td>(1 1 1 1 1 0)</td>
<td>(0 1 0 0 1 1)</td>
<td>(1 1 0 0 1 1)</td>
</tr>
<tr>
<td>(0 0 0 0 0 1)</td>
<td>(1 1 0 1 1 1)</td>
<td>(0 1 0 1 0 0)</td>
<td>(0 0 0 1 1 0)</td>
</tr>
<tr>
<td>(1 0 0 1 0 0)</td>
<td>(0 1 0 0 1 0)</td>
<td>(0 0 1 0 0 1)</td>
<td>(1 1 1 1 1 1)</td>
</tr>
</tbody>
</table>

Columns $\mathbf{v}_5 - \mathbf{v}_8$ are listed in the next page.

Decoding of linear block codes

<table>
<thead>
<tr>
<th>Coset Leader $\mathbf{v}_1$</th>
<th>$\mathbf{v}_5$</th>
<th>$\mathbf{v}_6$</th>
<th>$\mathbf{v}_7$</th>
<th>$\mathbf{v}_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0 0 0 0 0 0)</td>
<td>(1 1 0 1 1 0)</td>
<td>(1 0 1 1 0 1)</td>
<td>(0 1 1 0 1 1)</td>
<td>(0 0 0 1 1 1)</td>
</tr>
<tr>
<td>(1 0 0 0 0 0)</td>
<td>(0 1 0 1 1 0)</td>
<td>(0 0 1 1 0 1)</td>
<td>(1 1 1 0 1 1)</td>
<td>(1 0 0 1 1 1)</td>
</tr>
<tr>
<td>(0 1 0 0 0 0)</td>
<td>(1 0 0 1 1 0)</td>
<td>(1 1 1 1 0 1)</td>
<td>(0 0 1 0 1 1)</td>
<td>(0 1 0 1 1 1)</td>
</tr>
<tr>
<td>(0 0 1 0 0 0)</td>
<td>(1 1 1 1 1 0)</td>
<td>(1 0 0 1 0 1)</td>
<td>(0 1 0 0 1 1)</td>
<td>(0 0 1 1 1 1)</td>
</tr>
<tr>
<td>(0 0 0 1 0 0)</td>
<td>(1 1 0 0 1 0)</td>
<td>(1 0 1 0 0 1)</td>
<td>(0 1 1 1 1 1)</td>
<td>(0 0 0 0 1 1)</td>
</tr>
<tr>
<td>(0 0 0 0 1 0)</td>
<td>(1 1 1 0 0 1)</td>
<td>(1 0 1 1 1 1)</td>
<td>(0 1 1 0 0 1)</td>
<td>(0 0 0 1 0 1)</td>
</tr>
<tr>
<td>(0 0 0 0 0 1)</td>
<td>(1 1 0 1 1 1)</td>
<td>(1 0 1 1 0 0)</td>
<td>(0 1 1 0 1 0)</td>
<td>(0 0 0 1 1 0)</td>
</tr>
<tr>
<td>(1 0 0 1 0 0)</td>
<td>(0 1 0 0 1 0)</td>
<td>(0 0 1 0 0 1)</td>
<td>(1 1 1 1 1 1)</td>
<td>(1 0 0 0 1 1)</td>
</tr>
</tbody>
</table>

Columns $\mathbf{v}_2 - \mathbf{v}_4$ are listed in the previous page.
Decoding of linear block codes

• Every vector in $V_n$ appears exactly once in the standard array.

This follows from the construction rule of the standard array. Proof by contradiction.
Decoding of linear block codes

- Every vector in $V_n$ appears exactly once in the standard array.
  - This follows from the construction rule of the standard array. Proof by contradiction.
- No two vectors in the same row of a standard array are identical.
  - This follows from the fact that all code vectors of $C$ are distinct.
Decoding of linear block codes

- Every vector in $V_n$ appears exactly once in the standard array.
  - This follows from the construction rule of the standard array. Proof by contradiction.
- No two vectors in the same row of a standard array are identical.
  - This follows from the fact that all code vectors of $C$ are distinct.
- Each row is called a coset.

There are exactly $2^{n-k}$ cosets.
Decoding of linear block codes

- Every vector in $V_n$ appears exactly once in the standard array.
  - This follows from the construction rule of the standard array. Proof by contradiction.
- No two vectors in the same row of a standard array are identical
  - This follows from the fact that all code vectors of $C$ are distinct.
- Each row is called a coset.
- There are exactly $2^{n-k}$ cosets.
- The first element of each coset is called the coset leader. (Any element in a coset can be used as its coset leader. This does not change the elements of the coset, it changes the order of them.)

- All $2^k$ elements of a coset have the same syndrome as their coset leader, since
  \[
  s = (e_j + v_i)H^T = e_jH^T + v_iH^T = e_jH^T
  \]
Decoding of linear block codes

- All $2^k$ elements of a coset have the same syndrome as their coset leader, since

$$s = (e_j + v_i)H^T = e_jH^T + v_iH^T = e_jH^T$$

- The $2^k$ elements of a coset are the $2^k$ solutions to the syndrome equations.

- Each of the $2^{n-k}$ coset leaders has a different syndrome. Hence, there is one-to-one correspondence between a coset leader and a syndrome.
Decoding of linear block codes

- The $j^{th}$ column of a standard array.

\[ D_j = \{v_j, e_2 + v_j, e_3 + v_j, \ldots, e_{2^{n-k}} + v_j \} \]

contains exactly one codeword.

- If $r$ belongs to column $D_j$, then $r$ is decoded into codeword $v_j$. 
Decoding of linear block codes

- The $j^{\text{th}}$ column of a standard array.

\[ D_j = \{ v_j, e_2 + v_j, e_3 + v_j, \cdots, e_{2^n-k} + v_j \} \]

contains exactly one codeword.

- If $r$ belongs to column $D_j$, then $r$ is decoded into codeword $v_j$.

- If $v_j$ is the transmitted codeword, and the error pattern is a coset leader $e_i$, then $r = v_j + e_i$ is in column of $D_j$, which contains $v_j$ (Correct decoding).

Decoding of linear block codes

- If the error pattern is not a coset leader, then $r$ is not in column $D_j$. (incorrect decoding)
Decoding of linear block codes

- If the error pattern is not a coset leader, then \( r \) is not in column \( D_j \). (incorrect decoding)

- Let’s say the error pattern \( x \) caused by the channel is in \( l^{\text{th}} \) coset and and under the code vector \( v_i \neq 0 \). Then \( x = e_l + v_i \) and the received vector is

\[
    r = v_j + x = e_l + v_i + v_j = e_l + v_s.
\]

The received vector is in \( D_s \), and decoded as \( v_s \), which is not the transmitted code vector \( v_j \).

Therefore, decoding is correct if and only if the error pattern is a coset leader, and the \( 2^{n-k} \) coset leaders are all the correctable error patterns.
Decoding of linear block codes

- To minimize the probability of error, the error patterns most likely to happen should be chosen as coset leaders.

- For BSC, an error pattern of smaller weight is more probable than an error pattern of higher weight.
Decoding of linear block codes

- To minimize the probability of error, the error patterns most likely to happen should be chosen as coset leaders.
- For BSC, an error pattern of smaller weight is more probable than an error pattern of higher weight.
- Each coset leader should be chosen to be a vector of least weight from the available vectors.

This way coset leader has minimum weight in its coset.
Decoding of linear block codes

- To minimize the probability of error, the error patterns most likely to happen should be chosen as coset leaders.
- For BSC, an error pattern of smaller weight is more probable than an error pattern of higher weight.
- Each coset leader should be chosen to be a vector of least weight from the available vectors.
- This way coset leader has minimum weight in its coset.
- The decoding based on standard array is minimum distance decoding (i.e. ML decoding).

Assume that the received vector $r$ is found in the $i^{th}$ column, and $i^{th}$ coset of the standard array. Then $r$ is decoded as code vector $v_i$. 

Decoding of linear block codes

- Assume that the received vector $r$ is found in the $i^{th}$ column, and $i^{th}$ coset of the standard array. Then $r$ is decoded as code vector $v_i$.

- Since $r = e_l + v_i$, distance between $r$ and $v_i$ is

$$d(r, v_i) = w(r + v_i) = w(e_l + v_i + v_i) = w(e_l)$$

Now consider the distance between $r$ and any other code vector, say $v_j$,

$$d(r, v_j) = w(r + v_j) = w(e_l + v_i + v_j) = w(e_l + v_s)$$

where $v_s = v_i + v_j$
Decoding of linear block codes

- Since $e_l$ and $e_l + v_s$ are in the same coset, and since $w(e_l) \leq w(e_l + v_s)$, it follows that
  
  $$d(r, v_i) \leq d(r, v_j)$$

- Hence if coset leader is chosen to have minimum weight in its coset, the decoding based on the standard array is the ML decoder.
Decoding of linear block codes

Summary:
Step 1: Compute the syndrome \( s = rH^T \).
Step 2: Find the coset leader \( \hat{e} \) whose syndrome is equal to \( s \).
Step 3: Decode \( r \) into the estimated codeword

\[
\hat{v} = r + \hat{e}
\]

Syndrome decoding can be implemented using a look-up table that consists of \( 2^{n-k} \) correctable error patterns (coset leaders) and their corresponding syndromes.

\[
\begin{align*}
    s_1 &= 0 &\rightarrow& e_1 &= 0 \\
    s_2 &\rightarrow& e_2 \\
    \vdots &\vdots& \vdots \\
    s_{2^{n-k}} &\rightarrow& e_{2^{n-k}}
\end{align*}
\]
Syndrome decoding can be implemented using a look-up table that consists of $2^{n-k}$ correctable error patterns (coset leaders) and their corresponding syndromes.

\[
\begin{align*}
  s_1 &= 0 \rightarrow e_1 = 0 \\
  s_2 &\rightarrow e_2 \\
  \vdots &\vdots \\
  s_{2^{n-k}} &\rightarrow e_{2^{n-k}}
\end{align*}
\]

Syndrome decoding can also be used to perform a combination of error correction and error detection.

Coset leaders corresponding to the lowest weight error patterns are used for error correction. These are the most likely error patterns.
Decoding of linear block codes

- Syndrome decoding can be implemented using a look-up table that consists of $2^{n-k}$ correctable error patterns (coset leaders) and their corresponding syndromes.

\[
\begin{align*}
    s_1 &= 0 \quad \rightarrow \quad e_1 = 0 \\
    s_2 \quad &\rightarrow \quad e_2 \\
    \vdots \quad &\vdots \\
    s_{2^{n-k}} \quad &\rightarrow \quad e_{2^{n-k}}
\end{align*}
\]

- Syndrome decoding can also be used to perform a combination of error correction and error detection.
- Coset leaders corresponding to the lowest weight error patterns are used for error correction. These are the most likely error patterns.
- Syndrome corresponding to higher weight (less likely) error patterns are used to declare a detected error rather than for correction.

Example 3.2: Consider a $(6,3)$ linear systematic code generated by

\[
G = \begin{bmatrix}
    0 & 1 & 1 & 1 & 0 & 0 \\
    1 & 0 & 1 & 0 & 1 & 0 \\
    1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix} = [P \mid I]
\]

Its parity-check matrix is

\[
H = \begin{bmatrix}
    1 & 0 & 0 & 0 & 1 & 1 \\
    0 & 1 & 0 & 1 & 0 & 1 \\
    0 & 0 & 1 & 1 & 1 & 0
\end{bmatrix} = [I_3 \mid P^T]
\]
Decoding of linear block codes

Encoding:

\[(u_0, u_1, u_2) \leftrightarrow (v_0, v_1, v_2, u_0, u_1, u_2)\]

where

\[
\begin{align*}
v_0 &= u_1 + u_2 \\
v_1 &= u_0 + u_2 \\
v_2 &= u_0 + u_1
\end{align*}
\]

Syndrome look-up table

<table>
<thead>
<tr>
<th>Syndromes ((s_0, s_1, s_2))</th>
<th>Correctable Error Patterns ((e_0, e_1, e_2, e_3, e_4, e_5))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0 0 0)</td>
<td>(0 0 0 0 0 0)</td>
</tr>
<tr>
<td>(1 0 0)</td>
<td>(1 0 0 0 0 0)</td>
</tr>
<tr>
<td>(0 1 0)</td>
<td>(0 1 0 0 0 0)</td>
</tr>
<tr>
<td>(0 0 1)</td>
<td>(0 0 1 0 0 0)</td>
</tr>
<tr>
<td>(0 1 1)</td>
<td>(0 0 0 1 0 0)</td>
</tr>
<tr>
<td>(1 0 1)</td>
<td>(0 0 0 0 1 0)</td>
</tr>
<tr>
<td>(1 1 0)</td>
<td>(0 0 0 0 0 1)</td>
</tr>
<tr>
<td>(1 1 1)</td>
<td>(1 0 0 1 0 0)</td>
</tr>
</tbody>
</table>
Decoding of linear block codes

<table>
<thead>
<tr>
<th>Coset Leader, $v_1$</th>
<th>$v_2$</th>
<th>$v_3$</th>
<th>$v_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0 0 0 0 0 0)</td>
<td>(0 1 1 1 0 0)</td>
<td>(1 0 1 0 1 0)</td>
<td>(1 1 0 0 0 1)</td>
</tr>
<tr>
<td>(1 0 0 0 0 0)</td>
<td>(1 1 1 1 0 0)</td>
<td>(0 0 1 0 1 0)</td>
<td>(0 1 0 0 1 1)</td>
</tr>
<tr>
<td>(0 1 0 0 0 0)</td>
<td>(0 0 1 1 0 0)</td>
<td>(1 1 1 0 1 0)</td>
<td>(1 0 0 0 1 1)</td>
</tr>
<tr>
<td>(0 0 1 0 0 0)</td>
<td>(0 1 0 1 0 0)</td>
<td>(1 0 0 0 1 0)</td>
<td>(1 1 1 0 1 1)</td>
</tr>
<tr>
<td>(0 0 0 1 0 0)</td>
<td>(0 1 1 0 0 0)</td>
<td>(1 0 1 1 1 0)</td>
<td>(1 1 0 1 0 1)</td>
</tr>
<tr>
<td>(0 0 0 0 1 0)</td>
<td>(0 1 1 1 1 0)</td>
<td>(1 0 1 0 0 0)</td>
<td>(1 1 0 1 1 0)</td>
</tr>
<tr>
<td>(0 0 0 0 0 1)</td>
<td>(0 1 1 1 0 1)</td>
<td>(1 0 1 0 1 1)</td>
<td>(1 1 0 0 0 0)</td>
</tr>
<tr>
<td>(1 0 0 1 0 0)</td>
<td>(1 1 1 0 0 0)</td>
<td>(0 0 1 1 1 0)</td>
<td>(0 1 0 1 0 1)</td>
</tr>
</tbody>
</table>

- Correctable error patterns: 7.
- Detectable error patterns: 8
### Decoding of linear block codes

<table>
<thead>
<tr>
<th>Coset Leader, ( v_1 )</th>
<th>( v_2 )</th>
<th>( v_3 )</th>
<th>( v_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0 0 0 0 0 0)</td>
<td>(0 1 1 1 0 0)</td>
<td>(1 0 1 0 1 0)</td>
<td>(1 1 0 0 0 1)</td>
</tr>
<tr>
<td>(1 0 0 0 0 0)</td>
<td>(1 1 1 1 0 0)</td>
<td>(0 0 1 0 1 0)</td>
<td>(0 1 0 0 1 1)</td>
</tr>
<tr>
<td>(0 1 0 0 0 0)</td>
<td>(0 0 1 1 0 0)</td>
<td>(1 1 1 0 1 0)</td>
<td>(1 0 0 0 1 1)</td>
</tr>
<tr>
<td>(0 0 1 0 0 0)</td>
<td>(0 1 0 1 0 0)</td>
<td>(1 0 0 1 0 1)</td>
<td>(1 1 0 0 1 1)</td>
</tr>
<tr>
<td>(0 0 0 1 0 0)</td>
<td>(0 1 1 0 0 0)</td>
<td>(1 0 1 1 1 0)</td>
<td>(1 1 0 1 0 1)</td>
</tr>
<tr>
<td>(0 0 0 0 1 0)</td>
<td>(0 1 1 1 1 0)</td>
<td>(1 0 1 0 0 0)</td>
<td>(1 1 0 0 1 1)</td>
</tr>
<tr>
<td>(0 0 0 0 0 1)</td>
<td>(0 1 1 1 0 1)</td>
<td>(1 0 1 0 1 1)</td>
<td>(1 1 0 0 0 0)</td>
</tr>
<tr>
<td>(1 0 0 1 0 0)</td>
<td>(1 1 1 0 0 0)</td>
<td>(0 0 1 1 1 0)</td>
<td>(0 1 0 1 0 1)</td>
</tr>
</tbody>
</table>

- Correctable error patterns: 7.
- Detectable error patterns: 8
- Undetected decoding errors: 49