Digital Communication
Channel coding, linear block codes, Hamming and cyclic codes
Lecture - 8

Ir. Muhamad Asvial, MSc., PhD
Center for Information and Communication Engineering Research (CICER)
Electrical Engineering Department - University of Indonesia
E-mail: asvial@ee.ui.ac.id
http://www.ee.ui.ac.id/cicer
What is channel coding?

• Channel coding:
  – Transforming signals to improve communications performance by increasing the robustness against channel impairments (noise, interference, fading, ..)
  – Waveform coding: Transforming waveforms to better waveforms
  – Structured sequences: Transforming data sequences into better sequences, having structured redundancy.
    • “Better” in the sense of making the decision process less subject to errors.
Error control techniques

• Automatic Repeat reQuest (ARQ)
  – Full-duplex connection, error detection codes
  – The receiver sends a feedback to the transmitter, saying that if any error is detected in the received packet or not (Not-Acknowledgement (NACK) and Acknowledgement (ACK), respectively).
  – The transmitter retransmits the previously sent packet if it receives NACK.

• Forward Error Correction (FEC)
  – Simplex connection, error correction codes
  – The receiver tries to correct some errors

• Hybrid ARQ (ARQ+FEC)
  – Full-duplex, error detection and correction codes
Why using error correction coding?

– Error performance vs. bandwidth
– Power vs. bandwidth
– Data rate vs. bandwidth
– Capacity vs. bandwidth

Coding gain:
For a given bit-error probability, the reduction in the $E_b/N_0$ that can be realized through the use of code:

$$G \,[\text{dB}] = \left( \frac{E_b}{N_0} \right)_u \,[\text{dB}] - \left( \frac{E_b}{N_0} \right)_c \,[\text{dB}]$$
Channel models

• Discrete memory-less channels
  – Discrete input, discrete output
• Binary Symmetric channels
  – Binary input, binary output
• Gaussian channels
  – Discrete input, continuous output
Some definitions

• Binary field:
  - The set \{0,1\}, under modulo 2 binary addition and multiplication forms a field.

<table>
<thead>
<tr>
<th>Addition</th>
<th>Multiplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 \oplus 0 = 0</td>
<td>0 \cdot 0 = 0</td>
</tr>
<tr>
<td>0 \oplus 1 = 1</td>
<td>0 \cdot 1 = 0</td>
</tr>
<tr>
<td>1 \oplus 0 = 1</td>
<td>1 \cdot 0 = 0</td>
</tr>
<tr>
<td>1 \oplus 1 = 0</td>
<td>1 \cdot 1 = 1</td>
</tr>
</tbody>
</table>

- Binary field is also called Galois field, GF(2).
Some definitions…

• Fields:
  – Let F be a set of objects on which two operations ‘+’ and ‘.’ are defined.
  – F is said to be a **field** if and only if
    1. F forms a commutative group under + operation. The additive identity element is labeled “0”.
      \[ \forall a, b \in F \implies a + b = b + a \in F \]
    2. F-{0} forms a commutative group under . Operation. The multiplicative identity element is labeled “1”.
    3. The operations “+” and “.” distribute:
      \[ \forall a, b \in F \implies a \cdot b = b \cdot a \in F \]
      \[ a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]
Some definitions…

• Vector space:
  – Let V be a set of **vectors** and F a fields of elements called **scalars**. V forms a vector space over F if:

  **Commutative:**
  \[ \forall u, v \in V \implies u + v = v + u \in F \]

  **Distributive:**
  \[ \forall a \in F, \forall v \in V \implies a \cdot v = u \in V \]

  **Associative:**
  \[ (a + b) \cdot v = a \cdot v + b \cdot v \quad \text{and} \quad a \cdot (u + v) = a \cdot u + a \cdot v \]
  \[ \forall a, b \in F, \forall v \in V \implies (a \cdot b) \cdot v = a \cdot (b \cdot v) \]
  \[ \forall v \in V, 1 \cdot v = v \]
Linear block codes

- Linear block code \((n,k)\)
  - A set \(C \subseteq V^n\) with cardinality \(2^k\) is called a linear block code if, and only if, it is a subspace of the vector space \(V^n\).
  
  \[
  V_k \rightarrow C \subseteq V^n
  \]

- Members of \(C\) are called code-words.
- The all-zero codeword is a codeword.
- Any linear combination of code-words is a codeword.
Linear block codes – cont’d

$V_k \rightarrow \text{mapping} \rightarrow V_n$

Bases of $C$
Linear block codes – cont’d

- The information bit stream is chopped into blocks of $k$ bits.
- Each block is encoded to a larger block of $n$ bits.
- The coded bits are modulated and sent over channel.
- The reverse procedure is done at the receiver.

$$R_c = \frac{k}{n} \quad \text{Code rate}$$
Linear block codes – cont’d

• The Hamming weight of vector $\mathbf{U}$, denoted by $w(\mathbf{U})$, is the number of non-zero elements in $\mathbf{U}$.

• The Hamming distance between two vectors $\mathbf{U}$ and $\mathbf{V}$, is the number of elements in which they differ.

• The minimum distance of a block code is

$$d(\mathbf{U}, \mathbf{V}) = w(\mathbf{U} \oplus \mathbf{V})$$

$$d_{\text{min}} = \min_{i \neq j} d(\mathbf{U}_i, \mathbf{U}_j) = \min_i w(\mathbf{U}_i)$$
Linear block codes – cont’d

- Error detection capability is given by

\[ e = d_{\text{min}} - 1 \]

- Error correcting-capability \( t \) of a code, which is defined as the maximum number of guaranteed correctable errors per codeword, is

\[ t = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor \]
Linear block codes – cont’d

• For memory less channels, the probability that the decoder commits an erroneous decoding is

\[ P_M \leq \sum_{j=t+1}^{n} \binom{n}{j} p^j (1 - p)^{n-j} \]

– \( p \) is the transition probability or bit error probability over channel.

• The decoded bit error probability is

\[ P_B \approx \frac{1}{n} \sum_{j=t+1}^{n} j \binom{n}{j} p^j (1 - p)^{n-j} \]
Linear block codes – cont’d

- Discrete, memoryless, symmetric channel model

\[
\begin{bmatrix}
1 \\
0
\end{bmatrix} \xrightarrow{1-p} \begin{bmatrix}
1 \\
0
\end{bmatrix} \quad \begin{bmatrix}
1 \\
0
\end{bmatrix} \xrightarrow{p} \begin{bmatrix}
1 \\
0
\end{bmatrix}
\]

Tx. bits \quad \xrightarrow{p} \quad \xrightarrow{1-p} \quad \xrightarrow{p} \quad \xrightarrow{1-p} \quad Rx. bits

- Note that for coded systems, the coded bits are modulated and transmitted over channel. For example, for M-PSK modulation on AWGN channels (M>2):

\[
p \approx \frac{2}{\log_2 M} Q \left( \sqrt{\frac{2(\log_2 M)E_c}{N_0}} \sin \left( \frac{\pi}{M} \right) \right) = \frac{2}{\log_2 M} Q \left( \sqrt{\frac{2(\log_2 M)E_b R_c}{N_0}} \sin \left( \frac{\pi}{M} \right) \right)
\]

where \( E_c \) is energy per coded bit, given by \( E_c = R_c E_b \).
A matrix $G$ is constructed by taking as its rows the vectors on the basis, $\{V_1, V_2, \ldots, V_k\}$.
Linear block codes – cont’d

• Encoding in (n,k) block code

\[ U = mG \]

\[ (u_1, u_2, \ldots, u_n) = (m_1, m_2, \ldots, m_k) \cdot \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_k \end{bmatrix} \]

\[ (u_1, u_2, \ldots, u_n) = m_1 \cdot V_1 + m_2 \cdot V_2 + \ldots + m_k \cdot V_k \]

– The rows of G, are linearly independent.
Linear block codes – cont’d

- Example: Block code (6,3)

\[
G = \begin{bmatrix}
V_1 \\
V_2 \\
V_3
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}
\]

<table>
<thead>
<tr>
<th>Message vector</th>
<th>Codeword</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0000000</td>
</tr>
<tr>
<td>100</td>
<td>110100</td>
</tr>
<tr>
<td>010</td>
<td>011010</td>
</tr>
<tr>
<td>110</td>
<td>101110</td>
</tr>
<tr>
<td>001</td>
<td>101001</td>
</tr>
<tr>
<td>101</td>
<td>011101</td>
</tr>
<tr>
<td>011</td>
<td>110011</td>
</tr>
<tr>
<td>111</td>
<td>000111</td>
</tr>
</tbody>
</table>
Linear block codes – cont’d

• Systematic block code \((n,k)\)
  – For a systematic code, the first (or last) \(k\) elements in the codeword are information bits.

\[
\begin{align*}
  \mathbf{G} &= [\mathbf{P} : \mathbf{I}_k ] \\
  \mathbf{I}_k &= k \times k \text{ identity matrix} \\
  \mathbf{P}_k &= k \times (n - k) \text{ matrix}
\end{align*}
\]

\[
\mathbf{U} = (u_1, u_2, \ldots, u_n) = (p_1, p_2, \ldots, p_{n-k}, m_1, m_2, \ldots, m_k )
\]

\(\overset{\text{parity bits}}{\text{parity bits}}\) \(\overset{\text{message bits}}{\text{message bits}}\)
Linear block codes – cont’d

- For any linear code we can find an matrix $H_{(n-k) \times n}$, which its rows are orthogonal to rows of $G$:

$$GH^T = 0$$

- $H$ is called the parity check matrix and its rows are linearly independent.

- For systematic linear block codes:

$$H = [I_{n-k} \mid P^T]$$
Linear block codes – cont’d

- Syndrome testing:
  - $S$ is syndrome of $r$, corresponding to the error pattern $e$.

\[
S = rH^T = eH^T
\]
Linear block codes – cont’d

<table>
<thead>
<tr>
<th>Error pattern</th>
<th>Syndrome</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>000</td>
</tr>
<tr>
<td>000001</td>
<td>101</td>
</tr>
<tr>
<td>000010</td>
<td>011</td>
</tr>
<tr>
<td>000100</td>
<td>110</td>
</tr>
<tr>
<td>001000</td>
<td>001</td>
</tr>
<tr>
<td>010000</td>
<td>010</td>
</tr>
<tr>
<td>100000</td>
<td>100</td>
</tr>
<tr>
<td>010001</td>
<td>111</td>
</tr>
</tbody>
</table>

\[ \hat{r} = (001110) \] is received.

\[ \text{The syndrome of } \hat{r} \text{ is computed: } S = \hat{r}\mathbf{H}^T = (001110)\mathbf{H}^T = (100) \]

Error pattern corresponding to this syndrome is
\[ \hat{e} = (100000) \]

The corrected vector is estimated
\[ \hat{\mathbf{u}} = \hat{r} + \hat{e} = (001110) + (100000) = (101110) \]
Hamming codes

- Hamming codes are a subclass of linear block codes and belong to the category of *perfect codes*.
- Hamming codes are expressed as a function of a single integer $m$.

$$m \geq 2$$

<table>
<thead>
<tr>
<th>Code length</th>
<th>$n = 2^m - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of information bits</td>
<td>$k = 2^m - m - 1$</td>
</tr>
<tr>
<td>Number of parity bits</td>
<td>$n-k = m$</td>
</tr>
<tr>
<td>Error correction capability</td>
<td>$t = 1$</td>
</tr>
</tbody>
</table>

- The columns of the parity-check matrix, $H$, consist of all non-zero binary $m$-tuples.
Hamming codes

- Example: Systematic Hamming code (7,4)

\[ H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} = [I_{3 \times 3} \mid P^T] \]

\[ G = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [P \mid I_{4 \times 4}] \]
Cyclic block codes

- Cyclic codes are a subclass of linear block codes.
- Encoding and syndrome calculation are easily performed using feedback shift-registers.
  - Hence, relatively long block codes can be implemented with a reasonable complexity.
- BCH and Reed-Solomon codes are cyclic codes.
Cyclic block codes

- A linear \((n,k)\) code is called a Cyclic code if all cyclic shifts of a codeword are also a codeword.

\[
U = (u_0, u_1, u_2, \ldots, u_{n-1})
\]

\[
U^{(i)} = (u_{n-i}, u_{n-i+1}, \ldots, u_{n-1}, u_0, u_1, u_2, \ldots, u_{n-i-1})
\]

- Example:

\[
U = (1101)
\]

\[
U^{(1)} = (1110) \quad U^{(2)} = (0111) \quad U^{(3)} = (1011) \quad U^{(4)} = (1101) = U
\]
Cyclic block codes

• Syndrome decoding for Cyclic codes:
  – Received codeword in polynomial form is given by

\[ r(X) = U(X) + e(X) \]

  Received codeword \( \rightarrow \) Error pattern

  – The syndrome is the remainder obtained by dividing the received polynomial by the generator polynomial.

\[ r(X) = q(X)g(X) + S(X) \]

  Syndrome

  – With syndrome and Standard array, error is estimated.

• In Cyclic codes, the size of standard array is considerably reduced.
Example of the block codes

![Graph showing the performance of different modulation schemes (QPSK, 8PSK, uncoded) over SNR (Eb/N0) for a Hamming(7,4) and Hamming(15,11) code.]