Linear Block Codes

Telecommunications Laboratory
Alex Balatsoukas-Stimming

Technical University of Crete

October 23rd, 2008
Outline

1 Motivation

2 Linear Binary Codes
   - Hard decision (algebraic) decoding
   - Soft decision decoding
   - Error Probability
   - Systematic Codes
   - Error detecting and error correcting capabilities of a code
   - Standard array and syndrome decoding.

3 Hamming codes
   - Simulation results
Motivation

To achieve a given QoS (usually expressed as the bit error rate) using uncoded modulation, we require a certain SNR.

**Bandwidth limited channel**
1. Use higher order constellations, for example 8-PSK instead of 2-PSK.

**Power limited channel**
1. We can add redundancy (keeping symbol energy constant).
2. The modulator is forced to work at a higher rate to achieve the same information bit rate, increasing bandwidth occupation.

The difference between the SNR required for the uncoded and the coded system to achieve the same BER is called the *coding gain*.
There are two error correcting strategies:

- Forward error correction (FEC)
- Automatic repeat request (ARQ)
  - Stop-and-wait ARQ (e.g. ABP)
  - Continuous ARQ (e.g. SRP, Go-Back-N)

ARQ can only be used if there is a feedback channel.

When the transmission rate is high, retransmissions happen often, thus introducing delay into the communication.

For one way channels we can only use FEC.
Linear Binary Codes
If $C$ has the form:

$$C = \mathbb{F}_2^k G$$

where $G$ is a $k \times n$ binary matrix with $n \geq k$ and rank $k$, called the generator matrix of $C$, then $C$ is called an $(n, k, d)$ linear binary code.

The code words of a linear code have the form $uG$ where $u$ is any binary $k$-tuple of binary source digits.

For any $c_1, c_2 \in C$ it can be shown that $c_1 + c_2 \in C$, as follows:

$$c_1 + c_2 = u_1 G + u_2 G = (u_1 + u_2)G = uG \in C$$

The ratio $r = \frac{k}{n}$ is called the rate of the code.
An alternative definition of a linear code is through the concept of an \((n - k) \times n\) parity-check matrix \(H\). A code \(C\) is linear if:

\[
Hc = 0 \quad \forall c \in C
\]

We define \(s = H\hat{c}\) as the syndrome of the received binary codeword \(\hat{c}\) which is the received vector \(\hat{x} \in \mathbb{R}^n\) after hard decisions have been made on each of its components.

If \(s \neq 0\) then we know that an error has occurred.
Consider the following \( k \times n \) generator matrix \((k = 3, n = 4)\):

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

Each one of the \( 2^k = 8 \) code words have the form \( uG \)

For example, for \( u_1 = [1 \ 0 \ 1] \) we get the codeword:

\[
c_1 = u_1G = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
\end{bmatrix} = [1 \ 0 \ 1 \ 0]
\]
In algebraic decoding, ‘hard’ decisions are made on each component of the received signal $y$ forming the vector

$$x' = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)$$

e.g. for BPSK we have:

$$\hat{x}_i = \text{sign}(y_i)$$

If the vector $x'$ is a codeword of $C$, then the decoder selects $\hat{x} = x'$, else the structure of the code is exploited to correct them.

The method is suboptimal because we discard potentially useful information before using it.
In soft decision decoding, a Maximum Likelihood (or MAP if codewords are not equally likely) estimation is performed on the whole received vector.

\[
\hat{x} = \arg \max_{x \in C} p(y|x) \quad (\text{ML})
\]

\[
\hat{x} = \arg \max_{x \in C} p(x|y) \quad (\text{MAP})
\]

Considerable improvement in performance (usually around 3dB), but more complex implementation.
• Assume that we have a \((3, 1)\) repetition code, that is:

\[ x = (x_1, x_2, x_3) \quad \text{where} \quad x_2 = x_3 = x_1 \]

• The codewords of this code (in the signal space) are:

\[ c_1 = (-1, -1, -1) \quad \text{and} \quad c_2 = (+1, +1, +1) \]

• Assume now that transmitted signal is \( x = (+1, +1, +1) \) and the corresponding received vector is \( y = (+0.8, -0.1, -0.2) \)
Hard decision vs. soft decision decoding example (2/2)

- Using hard decision decoding, we decide -1 if the majority of the demodulated signals is -1, and +1 otherwise.

- The demodulated vector corresponding to the received vector $\mathbf{y}$ is $\hat{\mathbf{y}} = (1, -1, -1)$. Using the majority rule, we decide that $\hat{\mathbf{y}} = \mathbf{c}_1 = (-1, -1, -1)$, thus making a decoding error.

- Using soft decision decoding, we will choose the codeword with the least Euclidean distance from the received vector:

  $$d_E^2(\mathbf{y}, \mathbf{c}_1) = (0.8 - 1)^2 + (-0.1 - 1)^2 + (-0.2 - 1)^2 = 2.69$$

  $$d_E^2(\mathbf{y}, \mathbf{c}_2) = (0.8 + 1)^2 + (-0.1 + 1)^2 + (-0.2 + 1)^2 = 4.69$$

- So, we correctly choose $\hat{\mathbf{y}} = \mathbf{c}_1 = (-1, -1, -1)$. 
Recall that:

\[ P(e|x) \leq \sum_{\hat{x} \neq x} e^{-||x - \hat{x}||^2/4N_0} \]

For the simple case of the binary elemental constellation \( \mathcal{X} = \{-x, +x\} \), we have:

\[ d_E^2(c, c') = \sum_i (c_i - c'_i)^2 \]

\[ = \sum_{c_i \neq c'_i} 4x^2 \]

\[ = 4x^2 d_H(c, c') \]

\[ = 4\epsilon d_H(c, c') \]
Because of the linearity of the code, we have that $c' + c'' = c \in C$ so, the Hamming distance between $c$ and $\hat{c}$ is:

$$d_H(c, \hat{c}) = w(c + \hat{c}) = w(c')$$

So, for the error probability of a single codeword, we have:

$$P(e|c) \leq \sum_{\hat{c} \neq c} e^{-d_H(c, \hat{c})E/No} = \sum_{c^* \neq 0} e^{-w(c^*)E/No}$$

The value of the above summation does not depend on $c$, and hence:

$$P(e|c) = P(e)$$
A linear code is called systematic if its generator matrix has the form

\[ G = [I_k : P] \]

where \( P \) is a \( k \times (n - k) \) matrix.

The words of these codes have the form

\[ c = uG = [u : uP] \]

The \( (n - k) \times n \) parity check matrix of a systematic code can be constructed as follows

\[ H = [P^T : I_{n-k}] \]
We observe that the generator matrix from the previous example can be written in the form

\[ G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = G = \begin{bmatrix} \mathbf{I}_k \\ 1 \\ 1 \\ 1 \end{bmatrix} = [\mathbf{I}_k : \mathbf{P}] \]

where \( \mathbf{P} = [1 \ 1 \ 1]^T \), so the code is in its systematic form.

The parity check matrix \( \mathbf{H} \) of the above code can be written as

\[ \mathbf{H} = [\mathbf{P}^T : \mathbf{I}_{n-k}] = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \]
The received codeword can be written as \( r = c + e \), where \( c \) is the transmitted codeword and \( e \) is called the error pattern.

A code with a minimum distance \( d_{\text{min}} \) is capable of detecting all error patterns of \( d_{\text{min}} - 1 \) or less errors.

For error patterns of \( d_{\text{min}} \) or more errors, there exists at least one pattern which transforms the transmitted codeword into another valid codeword, so the code is not capable of detecting all of them.

It can however detect a large fraction of them. If \( e \in C \), then (because of the linearity of the code) \( r = c + e \in C \). So, there exist \( 2^k - 1 \) error patterns of more than \( d_{\text{min}} \) errors which are undetectable, leaving a total of \( 2^n - 2^k + 1 \) detectable error patterns.
Let $t$ be a positive integer such that

$$2t + 1 \leq d_{\text{min}} \leq 2t + 2$$

Let $c$ and $r$ be the transmitted and the received codeword respectively.

Let $w \in \{C - \{c, r\}\}$

Since the Hamming distance satisfies the triangle inequality, we get

$$d_H(c, r) + d_H(r, w) \geq d_H(c, w)$$

Since $c$ and $w$ are codewords of $C$, we have that

$$d_H(c, w) \geq d_{\text{min}} \geq 2t + 1$$
Suppose that $d_H(c, r) = t'$. 

From the above we get that

$$d_H(r, w) \geq 2t + 1 - t'$$

If $t' \leq t$, then

$$d_H(r, w) > t$$

The above tells us that if an error pattern of $t$ or less errors occurs, the received codeword $r$ is closer to the transmitted codeword $c$ than to any other codeword $w$ in $C$. 
An array containing all $2^n$ binary $n$-tuples which is constructed as follows:

\[
\begin{array}{cccc}
\mathbf{c}_1 = \mathbf{0} & \mathbf{c}_2 & \ldots & \mathbf{c}_{2^k} \\
\mathbf{e}_1 & \mathbf{c}_2 + \mathbf{e}_1 & \ldots & \mathbf{c}_{2^k} + \mathbf{e}_1 \\
\mathbf{e}_2 & \mathbf{c}_2 + \mathbf{e}_2 & \ldots & \mathbf{c}_{2^k} + \mathbf{e}_2 \\
\vdots & \vdots & \ddots & \vdots \\
\mathbf{e}_{2^{n-k}} & \mathbf{c}_2 + \mathbf{e}_{2^{n-k}} & \ldots & \mathbf{c}_{2^k} + \mathbf{e}_{2^{n-k}} \\
\end{array}
\]

where $\mathbf{c}_i \in \mathcal{C}$ and $\mathbf{e}_i$ are all $2^{n-k}$ possible error patterns.

The first column consists of elements called *coset leaders*.
Syndrome decoding (1/2)

- Recall that the syndrome of a received vector is defined as:
  \[ s = rH^T \]
  and that for every codeword \( c \in S \) it holds that:
  \[ s = cH^T = 0 \]

- All elements of a row of the standard array have the same syndrome:
  \[ (e_1 + c_i)H^T = e_1H^T + c_iH^T = e_1H^T \]
By computing the syndrome of the received codeword, we can estimate which error pattern occurred, namely the error pattern which has the same syndrome as the received vector.

It is optimal to choose the most likely error patterns as the coset leaders.

In the case of the AWGN with BPSK modulation, the most likely error patterns for large enough SNR are those with minimum weight.

After estimating the error pattern, we can correct the error as follows:

\[ \hat{c} = r + e_i = (c + e) + e = c \]
Hamming codes
Hamming codes

For any positive integer $m \geq 2$, there exists a Hamming code with the following parameters:

1. Code length: $n = 2^m - 1$
2. Number of information symbols: $k = 2^m - m - 1$
3. Number of parity symbols: $m = n - k$
4. Error correcting capability: $t = 1$ ($d_{\text{min}} = 3$)

Different code lengths can be chosen to achieve a wide variety of rates and performances.

The parity check matrix $H$ of a Hamming code consists of all nonzero $m$-tuples as its columns.
A Hamming code example

- For example, let $m = 3$. We get:
  1. $m = 3$ parity symbols
  2. $n = 2^m - 1 = 2^3 - 1 = 7$ codeword length
  3. $k = 2^m - m - 1 = 2^3 - 3 - 1 = 4$ information symbols

which is a $(7, 4, 1)$ linear code.

- The parity check matrix $H$ of this code is:

\[
H = \begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\text{I}_m & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1
\end{bmatrix}
\]

\[
= [\text{I}_m \cdot \text{P}^T]
\]

- The generator matrix for this Hamming code can be constructed as follows:

\[
G = [\text{I}_k \cdot \text{P}]
\]
Simulation results

BER vs SNR for the AWGN channel

- Uncoded BPSK
- (7,4) Hamming coded BPSK
- (15,11) Hamming coded BPSK
- (31,26) Hamming coded BPSK

Bit Error Rate vs SNR (dB)