

ECE4601

Communication Systems

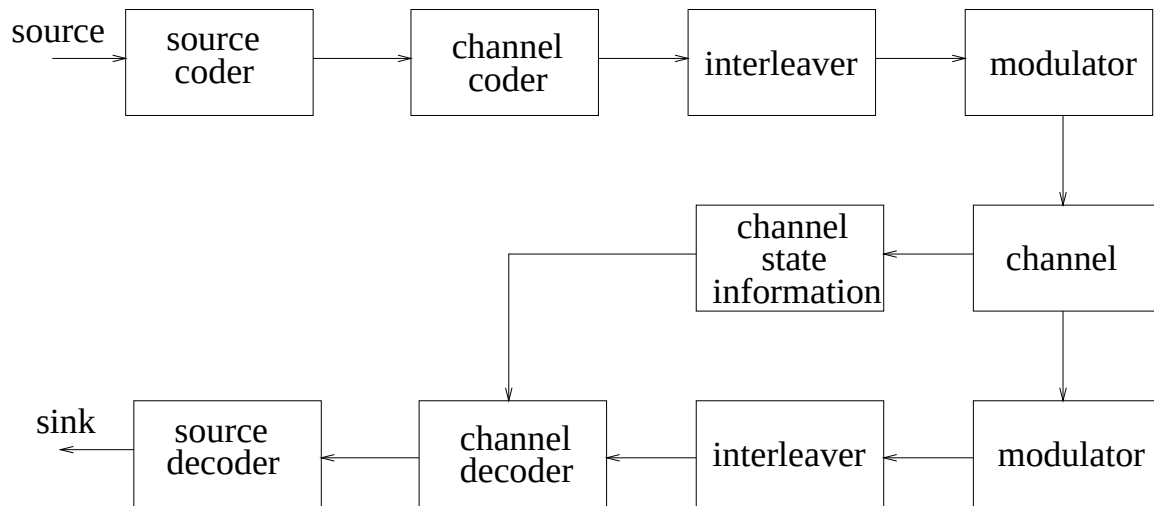
Week 14

Binary Block Codes

Error Detection and Correction

Standard Array and Syndrome Decoding

Basis Coded Communication System



Noisy Channel Coding Theorem

- Noisy Channel Coding Theorem: Every channel has a **channel capacity** C and information may be transmitted over the channel with an arbitrarily low bit error probability at any rate $R < C$.
 - In practice, this is accomplished by using channel coding.
 - Channel coding introduces controlled redundancy that allows the receiver to correct and/or detect errors that occur during transmission.
- There are two basic categories of codes:
 - Block codes – Hamming codes, BCH codes, Golay codes Reed-Solomon codes.
 - Convolutional codes – convolutional codes, trellis-coded modulation.

Block Codes

- A block encoder accepts as input a length k vector $\mathbf{a} = (a_1, a_2, \dots, a_k)$. and generates a length n codeword $\mathbf{c} = (c_1, c_2, \dots, c_n)$ through the linear mapping

$$\mathbf{c} = \mathbf{a}\mathbf{G}$$

- The rate of the code is $R = k/n$, and there are 2^k codewords.
- $\mathbf{G}$ is a $k \times n$ matrix, called the generator matrix.

$$\mathbf{G} = [g_{ij}]_{k \times n}$$

- A *systematic block code* has the generator matrix

$$\mathbf{G} = [\mathbf{I}_{k \times k} \mid \mathbf{P}]$$

where $\mathbf{P}$ is a $k \times (n - k)$ matrix.

- The whole task of block code design is to find the generator matrices, $\mathbf{G}$, of codes that are both powerful and easily decodable.

The Parity Check Matrix

- For any block code with generator matrix $\mathbf{G}$, there exists an $(n - k) \times n$ parity check matrix $\mathbf{H}$

$$\mathbf{H} = [h_{ij}]_{(n-k) \times n}$$

such that

$$\mathbf{GH}^T = \mathbf{0}_{k \times (n-k)}$$

- The parity check matrix is orthogonal to all codewords, i.e, $\mathbf{cH}^T = \mathbf{0}$.
- A systematic block code has the parity check matrix

$$\mathbf{H} = \left[-\mathbf{P}^T \mid \mathbf{I}_{(n-k) \times (n-k)} \right]$$

Hamming Code

- The parity check matrix of a systematic (7,4) Hamming code is

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

- The generator matrix is

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

- Codewords are $\mathbf{c} = (c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7)$

$$\begin{array}{llll} c_0 & = & a_0 & \quad c_1 = a_1 \quad \quad c_2 = a_2 \quad \quad c_3 = a_3 \\ c_4 & = & a_0 + a_2 + a_3 & \quad \quad \quad c_5 = a_0 + a_1 + a_2 \\ c_6 & = & a_1 + a_2 + a_3 & \end{array}$$

Syndromes

- Suppose that codeword $\mathbf{c}$ is transmitted and the vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{e}$ is an **error vector**.
- The **syndrome** of the received vector $\mathbf{y}$ is $\mathbf{s} = \mathbf{yH}^T$.
- If $\mathbf{s} = \mathbf{0}$, then $\mathbf{y}$ is a codeword; otherwise an error is detected if $\mathbf{s} \neq \mathbf{0}$.
- If $\mathbf{y}$ is a codeword, then $\mathbf{s} = \mathbf{0}$. Hence, $\mathbf{s} = \mathbf{0}$ does not mean that no errors have occurred – they may be undetectable. There are $2^k - 1$ undetectable error patterns.
- The syndrome only depends on the error vector $\mathbf{e}$ because

$$\mathbf{s} = \mathbf{cH}^T + \mathbf{eH}^T = \mathbf{eH}^T$$

- In general, $\mathbf{s} = \mathbf{eH}^T$ is $n - k$ equations in n variables.
- Fact: There are 2^k solutions for $\mathbf{e}$. The most likely error pattern is the one having minimum Hamming weight (smallest number of ones).

Minimum Distance

- The Hamming weight $w(\mathbf{c})$ of a codeword $\mathbf{c}$ is the number of nonzero components of $\mathbf{c}$. The Hamming distance between $\mathbf{c}_1$ and $\mathbf{c}_2$, denoted by $d(\mathbf{c}_1, \mathbf{c}_2)$ is the number of places where they differ. For binary codes

$$d(\mathbf{c}_1, \mathbf{c}_2) = w(\mathbf{c}_1 + \mathbf{c}_2)$$

- The *free Hamming distance* of a linear block code is equal to the minimum weight of its nonzero codewords

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{c}_1, \mathbf{c}_2), \quad \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}, \mathbf{c}_1 \neq \mathbf{c}_2\} \\ &= \min\{w(\mathbf{c}_1 + \mathbf{c}_2), \quad \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}, \mathbf{c}_1 \neq \mathbf{c}_2\} \\ &= \min\{w(\mathbf{c}), \quad \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\} \end{aligned}$$

- **Example:** The (7,4) Hamming code has $d_{\min} = 3$.

Singleton Bound

- For an (n, k) code we want to make $d_{\min}$ as large as possible.
- Consider the generator matrix $\mathbf{G}$ in systematic form $\mathbf{G} = [\mathbf{I}_{k \times k} | \mathbf{P}]$ where $\mathbf{P}$ is a $k \times (n - k)$ matrix.
- The number of nonzero elements in a row of $\mathbf{G}$ is at most $n - k + 1$. Hence, $d_{\min} \leq n - k + 1$.
- A code having $d_{\min} = n - k + 1$ is called **maximum distance separable** (MDS).
- **Example:** Binary repetition code

$$0 \longrightarrow \mathbf{c}_0 = (0, 0, \dots, 0)_n$$

$$1 \longrightarrow \mathbf{c}_1 = (1, 1, \dots, 1)_n$$

$$d_{\min} = d(\mathbf{c}_0, \mathbf{c}_1) = n = n - k + 1$$

This is the only MDS binary code. Reed-Solomon codes over $GF(2^k)$ are MDS.

Error Detection

- A linear block code can detect all error patterns of $d_{\min} - 1$ or fewer errors.
- If $\mathbf{y} = \mathbf{c} + \mathbf{e} \neq \mathbf{0}$ is a codeword, then no errors are detected.
- There are 2^{k-1} undetectable error patterns, but there are $2^n - 1$ possible nonzero error patterns.
- The number of detectable error patterns is

$$2^n - 1 - (2^k - 1) = 2^n - 2^k$$

- Usually, $2^k - 1$ is a small fraction of $2^n - 2^k$.
- **Example:** (7,4) Hamming code. There are $2^4 - 1 = 15$ undetectable error patterns and $2^7 - 2^4 = 112$ detectable error patterns.
- Good codes have a large $d_{\min}$ for a given code rate $R = k/n$ and block length n .

Weight Distribution

- Let A_i be the number of codewords of weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the weight distribution.
- The weight distribution can be expressed as a **weight enumerator polynomial**

$$A(z) = A_0z^0 + A_1z^1 + \dots + A_nz^n$$

- **Example:** (7,4) Hamming code

$$A_0 = 1, A_3 = 7, A_4 = 7, A_7 = 1$$

$$A(z) = 1 + 7z^3 + 7z^4 + z^7$$

- Usually, the weight distribution is difficult to get in closed form. However, it is known for Hamming codes, Golay codes, BCH codes, quadratic residue codes, Reed Muller codes.

Probability of Undetected Error

- The probability of an undetected error is

$$\begin{aligned} P_e(U) &= P(\mathbf{e} \text{ is a nonzero codeword}) \\ &= \sum_{i=1}^n A_i P(w(\mathbf{e}) = i) \end{aligned}$$

- For a binary symmetric channel with cross over probability p , $P(w(\mathbf{e}) = i) = p^i(1-p)^{n-i}$ and

$$P_e(U) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- **Example:** For the (7,4) Hamming code

$$P_e(U) = 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7$$

- For $p = 10^{-2}$, the probability of undetected error is $P_e(U) = 7 \times 10^{-6}$.

Error Correction

- A linear block code can correct all error patterns of t or fewer errors, where

$$t < \lfloor \frac{d_{\min} - 1}{2} \rfloor$$

and $\lfloor x \rfloor$ is the largest integer $\leq x$.

- A code is usually capable of correcting many error patterns of $t + 1$ or more errors. Up to 2^{n-k} error patterns may be corrected, equal to the number of syndromes.
- The probability of error for a binary symmetric channel is

$$\begin{aligned} P(E) &\leq 1 - P(t \text{ or fewer errors}) \\ &= 1 - \sum_{i=0}^t \binom{n}{i} p^i (1-p)^{n-i} \end{aligned}$$

The Standard Array

1. Write out all 2^k codewords in a row starting with $\mathbf{c}_0 = \mathbf{0}$.
2. From the remaining $2^n - 2^k$ n -tuples, select an error pattern $\mathbf{e}_2$ of weight 1 and place it under $\mathbf{c}_0$. Under each codeword put $\mathbf{c}_i + \mathbf{e}_2$
3. Select a minimum weight error pattern $\mathbf{e}_3$ from the remaining unused n -tuples and place it under $\mathbf{c}_0 = \mathbf{0}$. Under each codeword put $\mathbf{c}_i + \mathbf{e}_3$.
4. Repeat 3) until all n -tuples have been used.

Example

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

$$\begin{bmatrix} & 0000 & 1100 & 0101 & 1001 \\ \mathbf{e}_2 & 0001 & 1101 & 0100 & 1000 \\ \mathbf{e}_3 & 0010 & 1110 & 0111 & 1011 \\ \mathbf{e}_4 & 0011 & 1111 & 0110 & 1010 \end{bmatrix}$$

Property: every n -tuple appears once and only once in the array.

Error Correction

- When $\mathbf{y}$ is received, find $\mathbf{y}$ in the standard array. If $\mathbf{y}$ is in row i and column j , then $\mathbf{e}_i$ is the most likely error pattern, and $\mathbf{y}$ is decoded into $\mathbf{y} + \mathbf{e}_i = \mathbf{c}_j$.
- A code is capable of correcting all the $\mathbf{e}_i$, called coset leaders. If the error pattern is not a coset leader, then erroneous decoding will result.
- Every (n, k) linear code can correct 2^{n-k} error patterns, including the $\mathbf{0}$ vector. Recall that the same code can detect $2^n - 2^k$ error patterns. For large n

$$\frac{2^{n-k}}{2^n - 2^k} \approx 2^{-k}$$

is a small number. Hence, the code can detect many more errors than it can correct.

Syndrome Decoding

- Fact: all 2^k n -tuples in the same row have the same syndrome.
1. Compute the syndrome $\mathbf{s} = \mathbf{y}\mathbf{H}^T$.
 2. Locate the coset leader $\mathbf{e}_\ell$, where $\mathbf{e}_\ell\mathbf{H}^T = \mathbf{s}$.
 3. Decode $\mathbf{y}$ into $\mathbf{y} + \mathbf{e}_\ell$.

(7,4) Hamming Code

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

e	s
0000000	000
0000001	101
0000010	111
0000100	011
0001000	110
0010000	001
0100000	010
1000000	100

Example: Receive $\mathbf{y} = (1110000)$. Compute $\mathbf{s} = \mathbf{yH}^T = (111)$. Decode $\mathbf{y}$ into $\mathbf{c} = (1110000) + (0000010) = (1110010)$.