

ELEC 519A

Selected Topics in Digital Communications:
Information Theory

Simple Encoding and Decoding

Equivalence of Binary Linear Codes

Two binary linear codes are called equivalent if one can be obtained from the other by permuting the positions of the code

Two $k \times n$ binary matrices generate equivalent linear (n, k, d) codes if one matrix can be obtained from the other by a sequence of the following operations:

- (a) permutation of the rows
- (b) addition of one row to another
- (c) permutation of the columns

Equivalent Codes

Distances between codewords are unchanged by the equivalence operations.

Consequently, equivalent linear codes have the same parameters (n,k,d) (and correct the same number of errors).

Therefore the form of the code can be chosen to best suit the application.

Systematic Codes

Let $\mathbf{G}$ be a generator matrix of an (n,k) code. Then by the previous operations, $\mathbf{G}$ can be transformed into the form

$$[\mathbf{I}_k | \mathbf{P}]$$

where $\mathbf{I}_k$ is the $k \times k$ identity matrix, and $\mathbf{P}$ is a $k \times (n - k)$ matrix.

Example

$$\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \rightarrow \begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array} \rightarrow$$

$$\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array} \rightarrow \begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array} \rightarrow ?$$

Systematic Codes

- For a systematic block code the data appears unaltered in the codeword – usually at the start
- The generator matrix has the structure

$$\mathbf{G} = \begin{array}{c} \xleftarrow{k} \qquad \qquad \qquad \xleftarrow{n-k} \\ \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} \\ 0 & 1 & \cdots & 0 & p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} \end{array} \right] \end{array} = [\mathbf{I} \mid \mathbf{P}]$$

- $\mathbf{P}$ is often referred to as the parity matrix

Encoding with a Systematic Code

- **vector** $\times$ **matrix** multiplication
- **Encoding** of a message $m = (m_0, m_1, \dots, m_{k-1})$

$$c = m\mathbf{G} = m[\mathbf{I}_k \mid \mathbf{P}] = (m \mid b)$$

Example Let C be a $(7,4)$ code with generator matrix

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

Example (Cont.)

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

A message (m_0, m_1, m_2, m_3) is encoded as:

$(0 \ 0 \ 0 \ 0)$ is encoded as 00000000

$(1 \ 0 \ 0 \ 0)$ is encoded as 1000101

$(1 \ 1 \ 1 \ 0)$ is encoded as ?

Equivalent Systematic Code

$$\mathbf{G} = \begin{bmatrix} 1000 & 011 \\ 0100 & 101 \\ 0010 & 110 \\ 0001 & 111 \end{bmatrix} = [\mathbf{I}_4 \quad \mathbf{P}]$$

$$m = 0111 \quad c = m\mathbf{G} = 0111100 = m100$$

$$m = 1011 \quad c = m\mathbf{G} = 1011010 = m010$$



Parity Check Matrix

- Define a parity check matrix $\mathbf{H}$ ($(n-k) \times n$) such that

$$\mathbf{GH}^T = \mathbf{0}$$

$\mathbf{H}$ is a basis for the dual space

- If $\mathbf{G}$ is in systematic form

$$\mathbf{G} = [\mathbf{I}_k \ \mathbf{P}]$$

$$\mathbf{H} = [-\mathbf{P}^T \ \mathbf{I}_{n-k}] = [\mathbf{P}^T \ \mathbf{I}_{n-k}] \text{ (binary)}$$

$$\mathbf{GH}^T = -\mathbf{P} + \mathbf{P} = \mathbf{0}$$

- Every codeword satisfies the parity check equations given by the rows of $\mathbf{H}$

$$\mathbf{cH}^T = \mathbf{mGH}^T = \mathbf{0}$$

Examples

- TRC (3,1,3)

$$\mathbf{G} = [1|11]$$

$$\mathbf{H} = \begin{bmatrix} 1|10 \\ 1|01 \end{bmatrix}$$

(3,2,2) code

- SPC (8,7,2)

$$\mathbf{G} = \begin{bmatrix} I_7 & 1 \\ & 1 \\ & 1 \\ & 1 \\ & 1 \\ & 1 \\ & 1 \end{bmatrix}$$

$$\mathbf{H} = [1111111|1]$$

(8,1,8) code

Dual Codes

If C is a linear (n,k) code, then the **dual code** $C^\perp$ is a linear $(n,n-k)$ code.

The **dual code** is just the **dual subspace**.

Example

$$C_6 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$C_6^\perp = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Dual Codes

For the $(n,1)$ repetition code C with generator matrix

$$\mathbf{G} = [1 \ 1 \ \dots \ 1]$$

the dual code $C^\perp$ is an $(n,n-1)$ SPC code with generator matrix described by

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

The rows of $\mathbf{G}$ are orthogonal to the rows of $\mathbf{H}$

Systematic Parity Check Matrices

If $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{P}]$ is the standard form (systematic) generator matrix of a binary (n,k) code C , then a parity check matrix for C is $\mathbf{H} = [\mathbf{P}^T \mid \mathbf{I}_{n-k}]$

Example:

$$\mathbf{G} = \left[\mathbf{I}_4 \mid \begin{array}{ccc} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{array} \right] \Rightarrow \mathbf{H} = \left[\begin{array}{cccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array} \mid \mathbf{I}_3 \right]$$

Dual of the (5,2,3) Code

- Consider two equivalent (5,2,3) codes - nonsystematic and systematic

$$\mathbf{G} = \begin{bmatrix} 00111 \\ 11100 \end{bmatrix} \rightarrow \mathbf{G}' = \begin{bmatrix} 10110 \\ 01101 \end{bmatrix}$$

$$\mathbf{H} = \begin{bmatrix} 01101 \\ 00011 \\ 11000 \end{bmatrix} \quad \mathbf{H}' = \begin{bmatrix} 11100 \\ 10010 \\ 01001 \end{bmatrix}$$

- $\mathbf{H}$ and $\mathbf{H}'$ both generate (5,3,2) codes

Decoding Linear Codes

- One possibility is a ROM look-up table
- In this case the received word $\mathbf{r}$ is used as an address
- Example – Even single parity check code

Address	Entry
00000000	0
00000001	1
00000010	1
00000011	0
.....	.

- The output is an error flag, i.e., 0 – codeword valid
- If there is no error, the data is the first k codeword bits
- For an error correcting code, the ROM can also store the data after correction

TRC Decoding

With majority vote or nearest neighbor decoding

000, 001, 010, 100 → 000

111, 110, 101, 011 → 111

Address	Entry
---------	-------

000	0
-----	---

001	1
-----	---

010	0
-----	---

011	0
-----	---

100	0
-----	---

101	1
-----	---

110	1
-----	---

111	1
-----	---

Standard Array

- The standard array is formed by initially choosing $\mathbf{e}$ to be the
 - All zero pattern
 - All 1 bit error patterns
 - All 2 bit error patterns
 -
- Ensure that each new error pattern is not already in the array
- All correctable error patterns will appear as **coset leaders**

Standard Array

c_1 (all zero)	c_2		c_{M-1}	c_M
e_1	$c_2 + e_1$		$c_{M-1} + e_1$	$c_M + e_1$
e_2	$c_2 + e_2$		$c_{M-1} + e_2$	$c_M + e_2$
e_3	$c_2 + e_3$		$c_{M-1} + e_3$	$c_M + e_3$
....				
$e_{2^{n-k}-1}$	$c_2 + e_{2^{n-k}-1}$		$c_{M-1} + e_{2^{n-k}-1}$	$c_M + e_{2^{n-k}-1}$

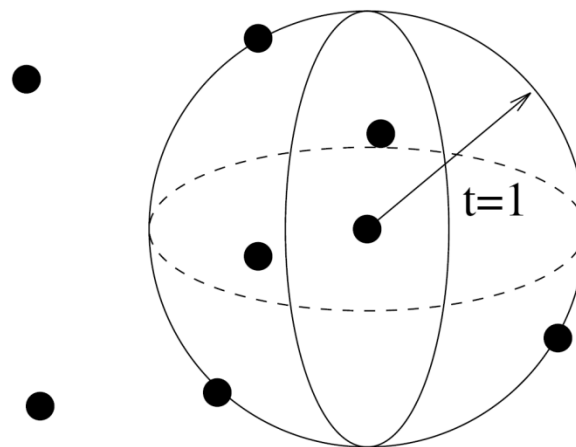
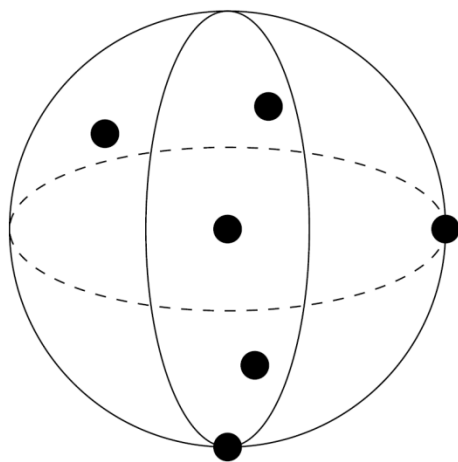
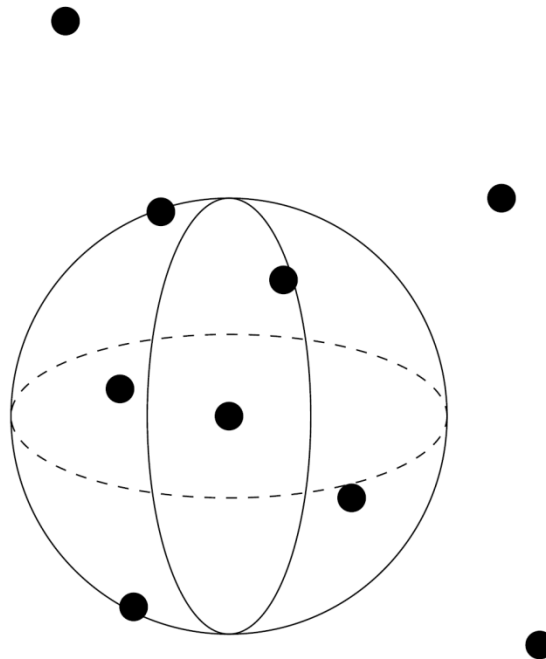
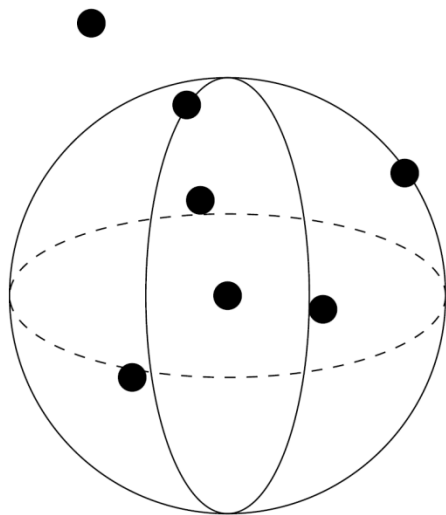
The array has 2^k columns (equal to the number of codewords) and 2^{n-k} rows (the number of correctable error patterns)

Standard Array Decoding

- Assume that the received word is $\mathbf{r} = \mathbf{c}_2 + \mathbf{e}_3$ (shown in bold in the standard array)
- The most likely codeword is the one at the top of the column containing $\mathbf{c}_2 + \mathbf{e}_3$
- The corresponding error pattern is the coset leader at the start of the row containing $\mathbf{c}_2 + \mathbf{e}_3$
- Can be implemented using a look-up table (ROM) which maps all words in the array to the most likely codeword (the one at the top of the column containing the received word).

Standard Array for the (5,2,3) Code

00000	10110	01101	11011
10000	00110	11101	01011
01000	11110	00101	10011
00100	10010	01001	11111
00010	10100	01111	11001
00001	10111	01100	11010
00011	10101	01110	11000
10001	00111	11100	01010



Syndromes

- For a received word $\mathbf{r}$, we need a simpler method to determine the codeword estimate
- To do this we use the **syndrome**, $\mathbf{s}$ of a received word $\mathbf{r}$

$$\mathbf{s} = \mathbf{rH}^T$$

- If $\mathbf{c}$ was corrupted by an error vector, $\mathbf{e}$, then

$$\mathbf{r} = \mathbf{c} + \mathbf{e}$$

and

$$\mathbf{s} = \mathbf{rH}^T = (\mathbf{c} + \mathbf{e})\mathbf{H}^T = \mathbf{cH}^T + \mathbf{eH}^T$$

$$\mathbf{s} = \mathbf{0} + \mathbf{eH}^T$$

- The syndrome depends only on the error vector $\mathbf{e}$

Syndromes

- We can add the same error pattern to different codewords and get the same syndrome.
- There are $2^{(n - k)}$ syndromes but 2^n received words
 - (5,2,3) code has 8 syndromes and 32 received words
 - (7,4,3) code has 8 syndromes and 128 received words
- Only need to determine which error pattern corresponds to the syndrome

Syndromes for the (5,2,3) Code

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array} \right]$$

$$H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array} \right]$$

$$s_0 = 00000H^T = 000$$

$$s_1 = 10000H^T = 110$$

$$s_2 = 01000H^T = 101$$

$$s_3 = 00100H^T = 100$$

$$s_4 = 00010H^T = 010$$

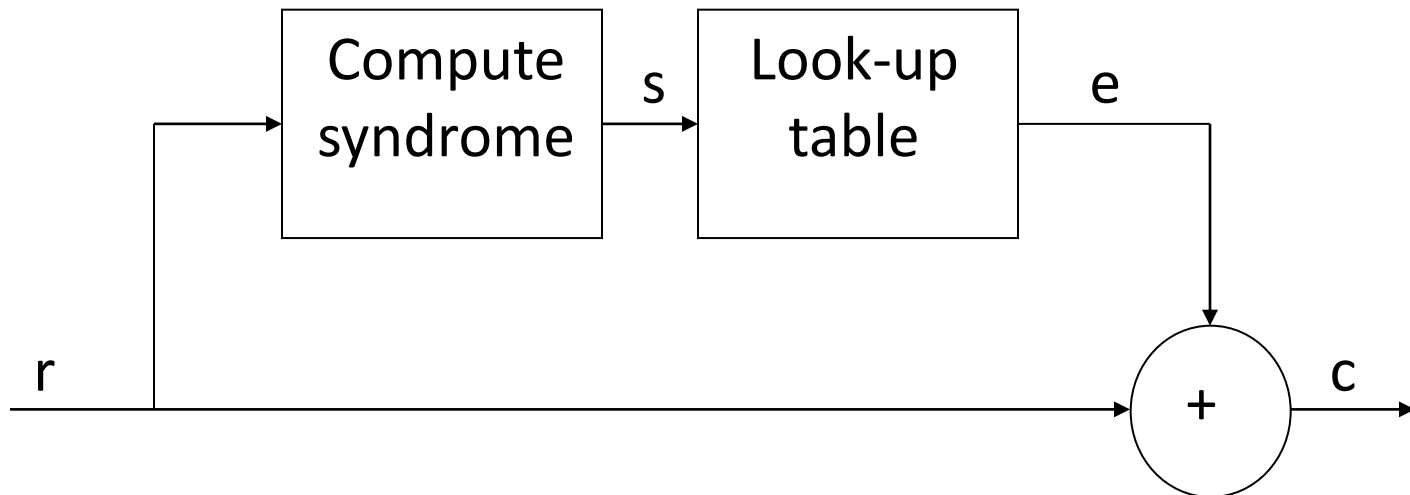
$$s_5 = 00001H^T = 001$$

$$s_6 = 00011H^T = 011$$

$$s_7 = 10001H^T = 111$$

Syndrome Decoding

- This block diagram shows the syndrome decoder implementation



Syndrome Decoding

- For systematic linear block codes

$$\mathbf{G} = [\mathbf{I} \mid \mathbf{P}] \quad \text{so} \quad \mathbf{H} = [-\mathbf{P}^T \mid \mathbf{I}]$$

- Example (7,4,3) code

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

$$\mathbf{H} = [-\mathbf{P}^T \mid \mathbf{I}] = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Syndrome Decoding – Example 1

- For a received word $r = (1101001)$

$$s = r\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

- So r is a valid codeword

Syndrome Decoding – Example 2

- The same codeword, this time with an error in the first bit position $r = (1101000)$

$$s = r\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$$

- Syndrome 001 indicates an error in bit 7 of the received word