Digital Communication Systems
ECS 452

Asst. Prof. Dr. Prapun Suksompong

prapun@siit.tu.ac.th

Channel Coding (A Revisit)

Office Hours:
BKD 3601-7
Monday 14:00-16:00
Wednesday 14:40-17:00

Review of Section 4

- We looked at the general form of channel coding over BSC.
- In particular, we looked at the general form of **block codes**.
  - **(n,k) codes**: n-bit blocks are used to conveys k-info-bit block over BSC.
  - **Rate**: $R = \frac{k}{n}$.
- We showed that the minimum distance decoder is the same as the ML decoder.
- This section: less probability analysis; more on explicit codes.

GF(2)

- The construction of the codes can be expressed in matrix form using the following definition of addition and multiplication of bits:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- These are modulo-2 addition and modulo-2 multiplication, respectively.
- The operations are the same as the **exclusive-or** (**XOR**) operation and the **AND** operation, but we will simply call them addition and multiplication so that we can use a matrix formalism to define the code.
- The two-element set {0, 1} together with this definition of addition and multiplication is a number system called a **finite field** or a **Galois field**, and is denoted by the label **GF(2)**.

GF(2)

- The construction of the codes can be expressed in matrix form using the following definition of addition and multiplication of bits:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Note that

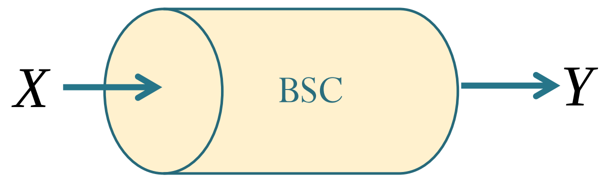
$$x \oplus 0 = x$$

$$x \oplus 1 = \overline{x}$$

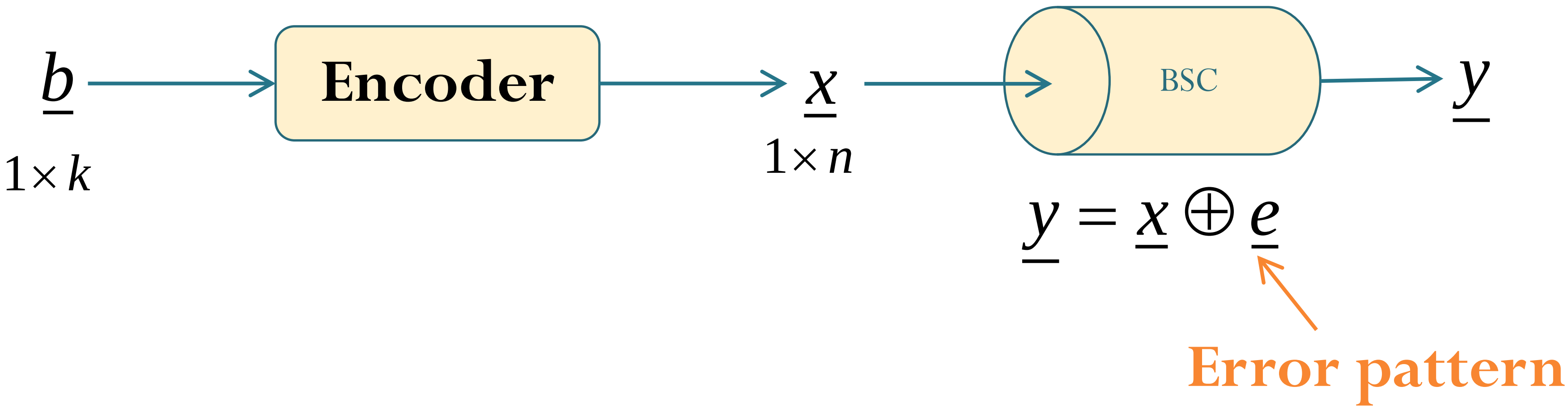
$$x \oplus x = 0$$

$$-x = x$$

Channel



- Again, to transmit *k* information bits, the channel is used *n* times.



Linear Block Codes

- **Generator matrix**:

$$\underline{x} = \underline{b}G = \sum_{j=1}^{k} b_j \underline{g}_j$$

mod-2 summation

Linear combination of the rows of **G**

$$G = \begin{bmatrix} \underline{g}_1 \\ \underline{g}_2 \\ \vdots \\ \underline{g}_k \end{bmatrix}_{k\times n}$$

- **Repetition code**: $G = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}$

$$\underline{x} = bG = \begin{bmatrix} b & b & \cdots & b \end{bmatrix} \qquad R = \frac{k}{n} = \frac{1}{n}$$

- **Single-parity-check code**: $G = \left[I_{k\times k}; \underline{1}^T \right]$

$$\underline{x} = \underline{b}G = \left[\underline{b} ; \sum_{j=1}^{k} b_j \right] \qquad R = \frac{k}{n} = \frac{k}{k+1}$$

parity bit

Error Detection

- Two types of **error control**:
  1. **error detection**
  2. **error correction**
- **Error detection**: the determination of whether errors are present in a received word.
- An error pattern is **undetectable** if and only if it causes the received word to be a valid codeword other than that which was transmitted.
  - Ex: In single-parity-check code, error will be undetectable when the number of bits in error is even.

Error Correction

- In **FEC** (**forward error correction**) system, when the decoder detects error, the arithmetic or algebraic **structure** of the code is used to determine which of the valid code words is **most likely to have been sent**, given the erroneous received word.
- It is possible for a detectable error pattern to cause the decoder to select a codeword other than that which was actually transmitted. The decoder is then said to have committed a **decoder error**.

Weight and Distance

- The **weight** of a codeword $\underline{x}$ or an error pattern $\underline{b}$ is the number of nonzero coordinates in the codeword or the error pattern.
  - The weight of a codeword $\underline{x}$ is commonly written as $\mathrm{w}(\underline{x})$.
- The **Hamming distance** between two n-bit blocks is the number of coordinates in which the two blocks differ.
- The **minimum distance** (d_{min}) of a block code is the minimum Hamming distance between all distinct pairs of codewords.
- A code with minimum distance d_{min} can
  - detect all error patterns of weight less than or equal to $d_{min}-1$.
  - correct all error patterns of weight less than or equal to $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$.

Systematic Encoding

- Code constructed with distinct information bits and check bits in each codeword are called **systematic codes**.
  - Message bits are "visible" in the codeword.
- We assume generator matrix of the form $G = \left[A_{k\times(n-k)} \;\vdots\; I_k \right]$

$$\underline{x} = \underline{b}G = \begin{bmatrix} b_1 & b_2 & \cdots & b_k \end{bmatrix} \left[P_{k\times(n-k)} \;\vdots\; I_k \right]$$

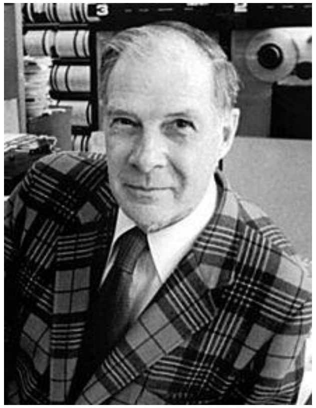
$$= \left[x_1 \quad x_2 \quad \cdots \quad x_{n-k} \;\vdots\; \underset{x_{n-k+1}}{b_1} \quad \underset{x_{n-k+2}}{b_2} \quad \cdots \quad \underset{x_n}{b_k} \right]$$

- Corresponding **parity check matrix:** $H = \left[I_{n-k} \;\vdots\; -A^T \right]$
  - Key property:

$$GH^T = \left[P \;\vdots\; I \right] \begin{bmatrix} I \\ -P \end{bmatrix} = P + (-P) = 0_{k\times(n-k)}$$

Hamming codes

- One of the earliest codes studied in coding theory.
- Named after Richard W. Hamming
  - The IEEE Richard W. **Hamming Medal**, named after him, is an award given annually by Institute of Electrical and Electronics Engineers (IEEE), for "exceptional contributions to information sciences, systems and technology“.
    - Sponsored by Qualcomm, Inc
    - Some Recipients:
      - 1988 - Richard W. Hamming
      - 1997 - Thomas M. Cover
      - 1999 - David A. Huffman
      - 2011 - Toby Berger



- The simplest of a class of (algebraic) error correcting codes that **can correct one error in a block of bits**

Hamming codes: Parameters

- $m = n - k =$ number of parity bits
- $n = 2^m - 1 \in \{3,7,15,31,63,127, \ldots\}$
- $k = n - m = 2^m - m - 1$
- $d_{\min} = 3.$
- Error correcting capability: $t = 1$

Construction of Hamming Codes

- Here, we want Hamming code whose $n = 2^m - 1$.

1. Parity check matrix *H:*
   - Construct a matrix whose columns consist of *all* nonzero binary *m*-tuples.
   - The ordering of the columns is arbitrary.
     However, next step is easy when the columns are arranged so that $H = [I_m \mid P]$.
2. Generator matrix *G*:
   - When $H = [I_m \mid P]$, we have $G = [-P^T \mid I_k] = [P^T \mid I_k]$.

Example: (7,4) Hamming Codes

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

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

Syndrome Table Decoding

When $\underline{y}$ is observed at the decoder, decoding is performed by

1. Compute the **syndrome vector**: $\underline{s} = \underline{y}H^T$.
2. Find the corresponding error $\underline{e}$ pattern for $\underline{s}$, and subtracting the error pattern from $\underline{y}$.

- Note that $\underline{s} = \underline{y}H^T = (\underline{x} \oplus \underline{e})H^T = (\underline{b}G \oplus \underline{e})H^T = \underline{e}H^T$.

$$H = \begin{bmatrix} \underline{h}_1 \\ \underline{h}_2 \\ \vdots \\ \underline{h}_{n-k} \end{bmatrix}_{(n-k)\times n} = \begin{bmatrix} \underline{d}_1^T & \underline{d}_2^T & \cdots & \underline{d}_n^T \end{bmatrix}$$

$$\underline{s} = \underline{e}H^T = \sum_{j=1}^{n} e_j \underline{d}_j$$

Linear combination of the columns of **H**

Example: (7,4) Hamming Codes

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

$$\underline{s} = \underline{e}H^T = \underbrace{\sum_{j=1}^{n} e_j \underline{d}_j}$$

Linear combination of the columns of **H**

Note that for an error pattern with a single one in the jth coordinate position, the syndrome $\underline{s} = \underline{y}H^T$ is the same as the j^{th} column of H.

Syndrome decoding table:

Error pattern $\underline{e}$	Syndrome = $\underline{e}H^T$
(0,0,0,0,0,0,0)	(0,0,0)
(0,0,0,0,0,0,1)	(1,1,1)
(0,0,0,0,0,1,0)	(1,1,0)
(0,0,0,0,1,0,0)	(1,0,1)
(0,0,0,1,0,0,0)	(0,1,1)
(0,0,1,0,0,0,0)	(0,0,1)
(0,1,0,0,0,0,0)	(0,1,0)
(1,0,0,0,0,0,0)	(1,0,0)

Hamming Codes: Decoding Algorithm

1. Compute the syndrome $\underline{s} = \underline{y}H^T$ for the received word. If $\underline{s} = 0$, then go to step 4.
2. Determine the position j of the column of H that is the transposition of the syndrome.
3. Complement the j^{th} bit in the received word.
4. Output the resulting codeword and STOP.