INFORMATION THEORY & CODING

Week 14 : Channel Coding 2

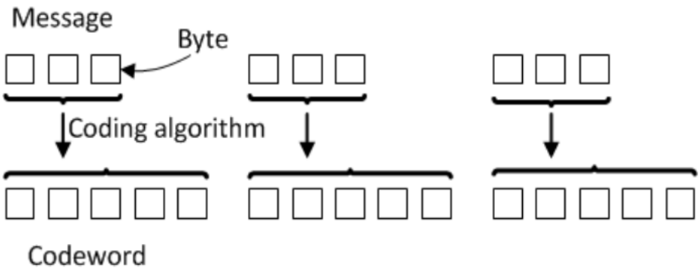
Dr. Rui Wang

Department of Electrical and Electronic Engineering
Southern Univ. of Science and Technology (SUSTech)

Email: wang.r@sustech.edu.cn

December 14, 2020

Linear block code



- Consider an (n, k) linear block code:
  - n denotes the codeword length
  - k is the number of message bits
  - $n-k$ is the number of parity-check bits

Linear block code

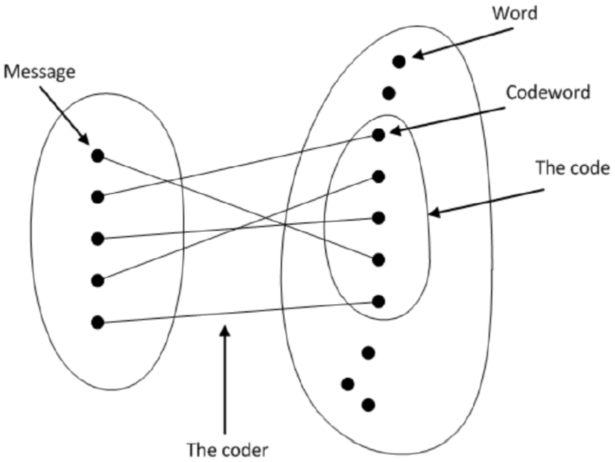
- Since $n > k$, there are more n-tuples (words) than messages. There are two basic questions:
  - How are the codewords selected among the set of all words?
  - How are codewords assigned to messages?

The set of codewords is called the code, and the function that assigns codewords to messages is called the coder.

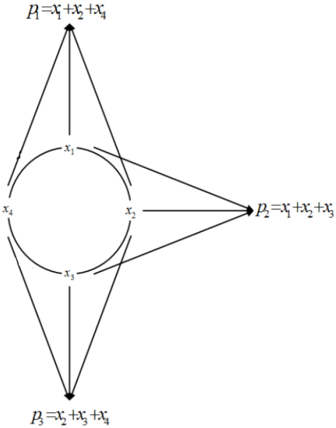
The code has to be injective (one-to-one), why?

uniquely decoding

Linear block code



Linear block code: $(7,4)$ Hamming code



$$p_1 = x_1 + x_2 + x_4$$
$$p_2 = x_1 + x_2 + x_3$$
$$p_3 = x_2 + x_3 + x_4$$

In matrix form,

$$(p_1 \ p_2 \ p_3) = (x_1 \ x_2 \ x_3 \ x_4) \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$(x_1 \ x_2 \ x_3 \ x_4 \ p_1 \ p_2 \ p_3) = (x_1 \ x_2 \ x_3 \ x_4) \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

Linear block code: Encoding

- Every generation matrix can be equivalently transformed into standard form $\mathbf{G} = [\mathbf{I}_k|\mathbf{A}]$.
- In standard form, the message appears at the beginning of the codeword.

$$\mathbf{G} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & p_{11} & p_{12} & p_{13} \\ 0 & 1 & 0 & 0 & p_{21} & p_{22} & p_{23} \\ 0 & 0 & 1 & 0 & p_{31} & p_{32} & p_{33} \\ 0 & 0 & 0 & 1 & p_{41} & p_{42} & p_{43} \end{array}\right].$$

The four rows are L.I. and $y_1 = x_1$, $y_2 = x_2$, $y_3 = x_3$, $y_4 = x_4$ and

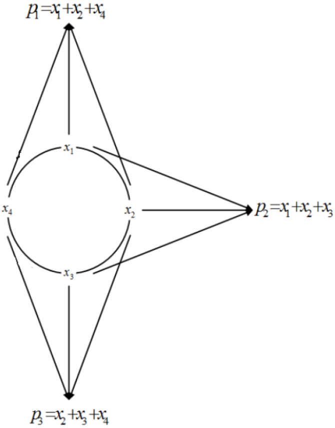
$$y_5 = x_1p_{11} + x_2p_{21} + x_3p_{31} + x_4p_{41}$$
$$y_6 = x_1p_{12} + x_2p_{22} + x_3p_{32} + x_4p_{42}$$
$$y_7 = x_1p_{13} + x_2p_{23} + x_3p_{33} + x_4p_{43}$$

Linear block code: Parity-Check Matrix

$$\mathbf{G} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & p_{11} & p_{12} & p_{13} \\ 0 & 1 & 0 & 0 & p_{21} & p_{22} & p_{23} \\ 0 & 0 & 1 & 0 & p_{31} & p_{32} & p_{33} \\ 0 & 0 & 0 & 1 & p_{41} & p_{42} & p_{43} \end{array}\right].$$

$$y_1p_{11} + y_2p_{21} + y_3p_{31} + y_4p_{41} + y_5 = 0$$
$$y_1p_{12} + y_2p_{22} + y_3p_{32} + y_4p_{42} + y_6 = 0$$
$$y_1p_{13} + y_2p_{23} + y_3p_{33} + y_4p_{43} + y_7 = 0$$

$$\left[\begin{array}{cccc|ccc} p_{11} & p_{21} & p_{31} & p_{41} & 1 & 0 & 0 \\ p_{12} & p_{22} & p_{32} & p_{42} & 0 & 1 & 0 \\ p_{13} & p_{23} & p_{33} & p_{43} & 0 & 0 & 1 \end{array}\right] (y_1\ y_2\ \ldots\ y_7)^T = 0.$$



Generator matrix

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

Parity-check matrix

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

Linear code

Linear independent rows of generator matrix

Using the $k \times n$ generator matrix $\mathbf{G}$, the codeword $\mathbf{y}$ is computed by
$\mathbf{y} = \mathbf{x}\mathbf{G}$
All the rows in $\mathbf{G}$ must be L.I., why?

If not, there exist vector $c = (c_1\ c_2\ \ldots\ c_k) \neq \mathbf{0}$ such that $c_1\mathbf{g}_1 + c_2\mathbf{g}_2 + \cdots + c_k\mathbf{g}_k = \mathbf{0}$. Then the codewords corresponding to $\mathbf{x}$ and $\mathbf{x} + \mathbf{c}$ would be the same!

Parity-check matrix

Theorem

If $\mathbf{G} = [\mathbf{I}_k|\mathcal{A}]$ *is a generator matrix for the* $[n,k]$ *code* $\mathcal{C}$ *in standard form, then* $\mathbf{H} = [-\mathbf{A}^{\mathrm{T}}|\mathbf{I}_{n-k}]$ *is a parity-check matrix for* $\mathcal{C}$*.*

Proof.

Clearly, we have $\mathbf{HG}^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}} + \mathbf{A}^{\mathrm{T}} = \mathbf{0}$. Thus C is contained in the kernel of the linear transformation $\mathbf{x} \to \mathbf{Hx}^{\mathrm{T}}$. As H has rank $n-k$, this linear transformation has kernel of dimension k, which is also the dimension of C. $\square$

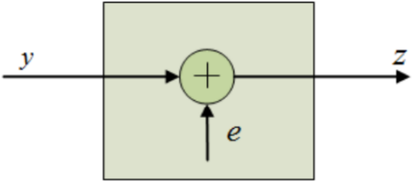
Discussions

- A linear block code is a vector subspace spanning the generator matrix $\mathbf{G}$.
- Rows of generator matrix $\mathbf{G}$ are L.I.
- Every vector in the subspace generated by the row vectors of $\mathbf{G}$ is a codeword.
  - Hence, a codeword plus another codeword yields a codeword.
- Every row vector of parity-check matrix $\mathbf{H}$ is orthogonal to $\mathbf{G}$ and the corresponding code (vector subspace).
- For an (n, k) code, we should choose $n - k$ L.I. rows for $\mathbf{H}$.

南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Error detection and correction

- If $\mathbf{y} = (y_1 \ y_2 \ \dots \ y_n)$ was sent but $z = (z_1 \ z_2 \ \dots \ z_n)$ was received, the channel introduced the error $\mathbf{e} = \mathbf{z} - \mathbf{y} = (e_1 \ e_2 \dots \ e_n)$.



- Errors cannot be detected if $\mathbf{e}$ is a codeword.
- How many error bits can be detected / corrected, wherever their positions are?

The weight of a codeword is defined as the number of its nonzero elements.

$$\mathbf{H}\mathbf{y}^{\mathrm{T}} = \mathbf{0}$$

To detect t errors: any set of up to t columns is L.I. In other words, $w_{\min} = t + 1$, where $w_{\min}$ is the minimum weight among all the codewords.

To correct t errors: any linear combination of t columns must be always different from any other combination of t columns. Thus, $w_{\min} = 2t + 1$.

Error detection and correction

- For an (n, k) code, the parity-check matrix $\mathbf{H}$ has n columns and $n-k$ L.I. rows.
- The only factor for correction (or detection) is the number of L.I. columns of $\mathbf{H}$, which is at most $n-k$.
- Hence, a $(7, 4)$ linear block code can at most correct 1 bit error or detect 3 bits error.
- The following three elementary row operations do not change the code generated by $\mathbf{H}$:
    - Interchanging two rows
    - Multiplying a row by a nonzero constant
    - Adding two rows
- The parity-check matrix $\mathbf{H}$ can always be transformed into the form of $[\mathbf{B}|\mathbf{I}_{n-k}]$

Linear block code: Decoding

For simplicity, consider a $(5,2)$ linear code whose generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$ are

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

The $2^5 = 32$ words are classified by syndrome.

000	00000	01101	10011	11110
001	00001	01100	10010	11111
010	00010	01111	10001	11100
011	10000	11101	00011	01110
100	00100	01001	10111	11010
101	01000	00101	11011	10110
110	00110	01011	10101	11000
111	00111	01010	10100	11001

Linear block code: Decoding

000	00000	01101	10011	11110
001	00001	01100	10010	11111
010	00010	01111	10001	11100
011	10000	11101	00011	01110
100	00100	01001	10111	11010
101	01000	00101	11011	10110
110	00110	01011	10101	11000
111	00111	01010	10100	11001

The 32 possible error patterns are classified based on the standard array.

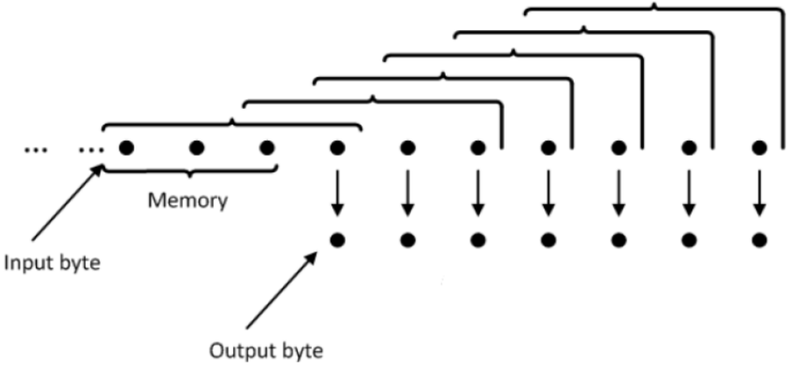
- No error ...... 1 pattern
- Errors corrected ...... 5 patterns
- Undetectable errors ...... 3 patterns
- Erroneous decoding ...... 15 patterns
- Errors detected ...... 8 patterns

Properties of syndrome:

- Syndrome depends only on error: $(\mathbf{y}+\mathbf{e})\mathbf{H}^{\mathrm{T}} = \mathbf{e}\mathbf{H}^{\mathrm{T}}$
- All error patterns that differ by a codeword have the same syndrome.

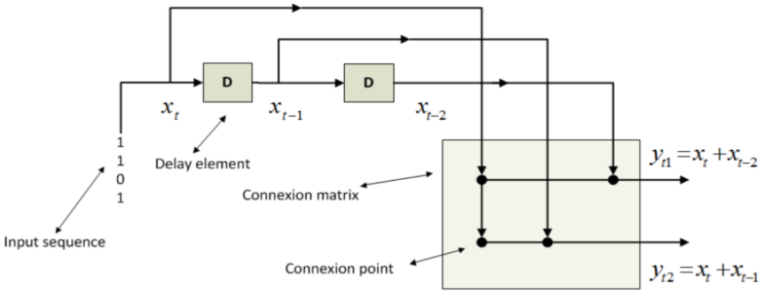
Continuous code

k_0 — the number of bits input
n_0 — the number of bits output
M — the size of memory



Continuous code

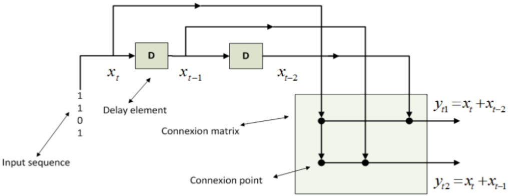
$$(n_0, k_0) = (2, 1),\ M = 2$$



State	Input	New State	Output
00	1	10	11
10	1	11	10
11	0	01	11
01	1	10	01
10	0	01	01
01	0	00	10

Appended zeros

Continuous code

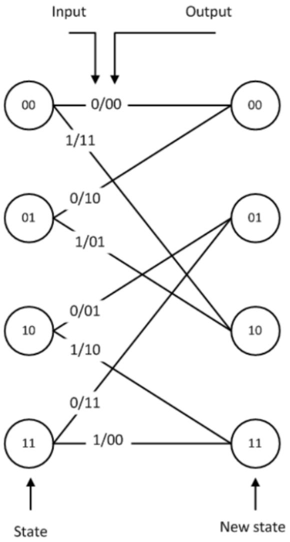


State	Input	New State	Output
00	1	10	11
10	1	11	10
11	0	01	11
01	1	10	01
10	0	01	01
01	0	00	10

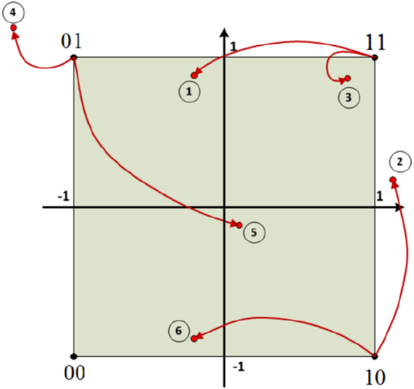
Appended zeros

Input: x_t
Output: $y_t = (y_t^{(1)}, y_t^{(2)}) = (x_t + x_{t-2}, x_t + x_{t-1})$
Memory(State): $s_t = (x_{t-1}, x_{t-2})$

Continuous code

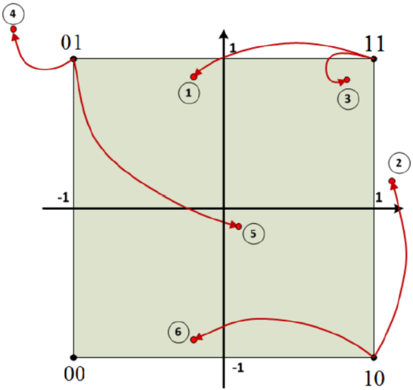


With initial state (00), $(1\ 1\ 0\ 1)$ is coded into $(11\ 10\ 11\ 01\ 01\ 10)$



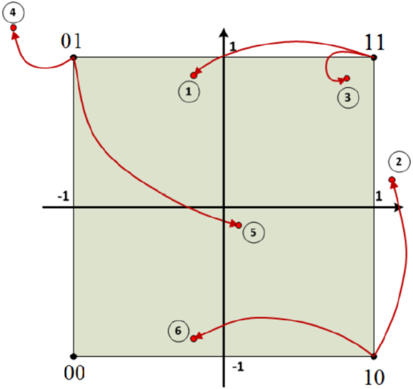
With initial state (00), $(1\ 1\ 0\ 1)$ is coded into
(11 10 11 01 01 10)— (11 1 -1 11 -11 -11 1 -1)

Continuous code: 4QAM modem



(11 10 11 01 01 10)— (11 1 -1 11 -11 -11 1 -1)
(-0.125 0.875) (1.125 0.125) (0.875 0.875) (-1.250 1.125) (0.125 -0.125) (-0.125 -0.875)

Continuous code: 4QAM modem



We would obtain
(-11 11 11 -11 1 -1 -1 -1)
which corresponds to
(01 11 11 01 10 00)
This would never happen since the first two bits has to be either 00 or 11.

(11 10 11 01 01 10)— (11 1 -1 11 -11 -11 1 -1)
(-0.125 0.875) (1.125 0.125) (0.875 0.875) (-1.250 1.125) (0.125 -0.125) (-0.125 -0.875)

Continuous code

Question: How to decode?

Soft decoding and decision by closeness.

Consider all 4-tuple, 16 in all, e.g., the sequence (00 00 00 00 00 00) corresponds to (0 0 0 0). Written as modem symbols as (-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1)
Compute the distance with (-0.125 0.875) (1.125 0.125) (0.875 0.875) (-1.250 1125) (0.125 -0.125) (-0.125 -0.875)

$$d^2 = [(-1+0.125)^2 + (-1-0.875)^2 \sim 4.3]$$

5.8, 7.0, 4.6, 2.0, and 0.8, sum them all to get 24.5. Then do this for all the other 15 cases, and decide the transmitted sequence is the one with the minimum metric.

Continuous code

Question: How to decode?

Soft decoding and decision by closeness.

Consider all 4-tuple, 16 in all, e.g., the sequence (00 00 00 00 00 00) corresponds to (0 0 0 0). Written as modem symbols as (-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1)
Compute the distance with (-0.125 0.875) (1.125 0.125) (0.875 0.875) (-1.250 1125) (0.125 -0.125) (-0.125 -0.875)

$$d^2 = [(-1+0.125)^2 + (-1-0.875)^2 \sim 4.3]$$

5.8, 7.0, 4.6, 2.0, and 0.8, sum them all to get 24.5. Then do this for all the other 15 cases, and decide the transmitted sequence is the one with the minimum metric.

Question: How to decode?

Soft decoding and decision by closeness.

Consider all 4-tuple, 16 in all, e.g., the sequence (00 00 00 00 00 00) corresponds to (0 0 0 0). Written as modem symbols as (-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1)
Compute the distance with (-0.125 0.875) (1.125 0.125) (0.875 0.875) (-1.250 1125) (0.125 -0.125) (-0.125 -0.875)

$$d^2 = [(-1 + 0.125)^2 + (-1 - 0.875)^2 \sim 4.3]$$

5.8, 7.0, 4.6, 2.0, and 0.8, sum them all to get 24.5. Then do this for all the other 15 cases, and decide the transmitted sequence is the one with the minimum metric.