ELG 5372 Error Control Coding

Lecture 7: Fundamentals of Linear Block Codes

uOttawa

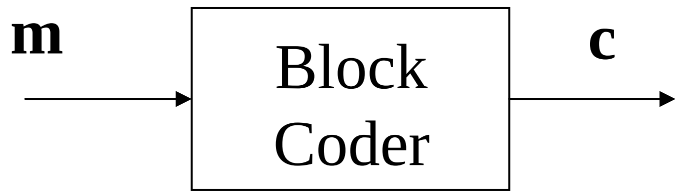
L'Université canadienne
Canada's university

Basic Definitions

- $\mathbf{m} = (m_0, m_1, \ldots, m_{k-1})$ is the q-ary k-tuple information vector.
- $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is the q-ary n-tuple codeword vector.
- We say that **c** is an element of code C. ($\mathbf{c} \in C$)

Definition 1

- An (n,k) block code C over an alphabet of q symbols is a set of q^k n-tuples called codewords. Associated with the code is an encoder which maps a message $\mathbf{m}_i$, which is a q-ary k-tuple to its associated codeword, $\mathbf{c}_i$.



Definition 2

- The vector space of all *n*-tuples from over field F_q is denoted as F_q^n.
  - Since F_q^n is the set of all possible *n*-tuples, then the dimension of F_q^n is *n*.
  - Let W be a *k* dimensional vector subspace of F_q^n.
  - Let W' be the set of all codewords in F_q^n that are orthogonal to all codewords in W. (**w'**.**w** = 0).
  - W' is called the dual space of W and it can be shown that it has dimension *n*-*k*. (see text page 79-80).

Definition 3

- The (n, k) block code C is a linear block code only if and only if its q^k codewords form a k dimensional vector subspace of F_q^n. The rate of the code is $R = k/n$.
  - This means that C is a closed set. Therefore the sum of any two codewords in C produces another codeword in C.

Definition 4

- The hamming weight of a codeword **c** is equal to the number of non-zero elements in the codeword.
  - Example: Hamming (7,4) code

codeword	HW(**c**)	codeword	HW(**c**)
0000000	0	1000110	3
0001101	3	1001011	4
0010111	4	1010001	3
0011010	3	1011100	4
0100011	3	1100101	4
0101110	4	1101000	3
0110100	3	1110010	4
0111001	4	1111111	7

Definition 5: Hamming Distance

- The hamming distance between two codewords in C is the number of positions in which the two codewords differ.
- $HD(\mathbf{c}_i, \mathbf{c}_j) = HW(\mathbf{c}_i - \mathbf{c}_j)$
- For codes that form vector spaces on $GF(2^m)$, $\mathbf{c}_i - \mathbf{c}_j = \mathbf{c}_i + \mathbf{c}_j$.

Definition 6: Minimum Hamming Distance

- The minimum Hamming distance of code C is the smallest Hamming distnace between two distinct codewords in the code.
  - Since HD($\mathbf{c}_i$, $\mathbf{c}_j$) = HW($\mathbf{c}_i$ - $\mathbf{c}_j$), then for linear block codes, $\mathbf{c}_i$-$\mathbf{c}_j$= another non-zero codeword. Therefore, the minimum Hamming distance of the code is the minimum non-zero Hamming weight of the code.
  - For Hamming (7,4) example, d_{min} = 3.

Generator Matrix Description of Linear Block Codes

- Since a linear block code C is a *k*-dimensional vector space, there exist *k* linearly independent vectors which form a basis for C.
  - $\{\mathbf{g}_0, \mathbf{g}_2, \ldots, \mathbf{g}_{k-1}\}$ form a basis for C.
  - All q^k codewords in C can be expressed as a linear combination of these basis vectors.
  - $\mathbf{c}_i = m_0\mathbf{c}_0 + m_1\mathbf{c}_1 + \ldots + m_{k-1}\mathbf{c}_{k-1}$, where m_i are elements in GF(q).
- Let $\mathbf{m} = [m_0\ m_1\ \ldots\ m_{k-1}]$ and $\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix}$, then $\mathbf{c}=\mathbf{m}\mathbf{G}$.

Generator Matrix Description of Linear Block Codes (2)

- There are q^k distinct vectors for **m**, therefore there are q^k distinct codewords.
- There are q^k distinct information sequences, therefore, **m** is the information vector (or message).
- **G** provides the transformation from information to codeword, thus **G** is referred to as the code generator matrix.

Example

$$\mathbf{G}_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

m	**c**	**m**	**c**
000	000000	100	110110
001	111111	101	001001
010	011011	110	101101
011	100100	111	010010

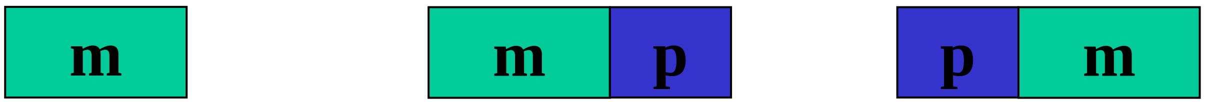
Example 2

$$\mathbf{G}_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

m	c	m	c
000	000000	100	110110
001	100100	101	010010
010	011011	110	101101
011	111111	111	001001

Systematic Codes

- A code C is said to be systematic if the original message appears explicitly in the codeword.



- For a systematic linear block code, the generator matrix is called a systematic generator.

Systematic Generators

- $\mathbf{G}_{syst}$ takes the form $[\mathbf{I}_k \mid \mathbf{P}]$ or $[\mathbf{P} \mid \mathbf{I}_k]$, where $\mathbf{I}_k$ is a $k \times k$ identity matrix and $\mathbf{P}$ is a $k \times (n\text{-}k)$ matrix which generates parity symbols.
- For any given $\mathbf{G}$, we can find $\mathbf{G}_{syst}$ by linear combinations of rows.

Example

$$\mathbf{G}_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

3=1+3

$$\mathbf{G}_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{2=2+3} \mathbf{G}_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

1=1+2

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

Example

m	**c**	**m**	**c**
000	000000	100	100100
001	001001	101	101101
010	010010	110	110110
011	011011	111	111111

Generator of Dual Code

- Let C be a (n,k) linear block code with generator **G**.
- Let C' be the dual of C. In other words, C' is made up of all n-tuples that are orthogonal to all n-tuples in C.
- The basis vectors in C' are orthogonal to the basis vectors in C.
- C' will be a (n, n-k) linear block code.

How to find the generator of Dual Code

- Let **H** be the (n-k) × n generator matrix of C'.
- $\mathbf{G}\mathbf{H}^T = k \times (n\text{-}k)$ all 0 matrix.
- Recall that $\mathbf{G}_{syst}$ produces the same code as **G**.
- $\mathbf{G}_{syst} = [\mathbf{I}_k \mid \mathbf{P}]$
- If $\mathbf{H} = [\mathbf{P}^T \mid \mathbf{I}_{n\text{-}k}]$, then $\mathbf{G}_{syst}\mathbf{H}^T = \mathbf{P}+\mathbf{P} = 0$.
- This means $\mathbf{G}\mathbf{H}^T = 0$.

Example

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

$$\mathbf{G}_{syst} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \ \mathbf{P} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \ \mathbf{GH}^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$