# E2 205 Error-Control Coding
# Lecture 2

Scribe - Biswadip Chakraborti

August 16, 2019

## 1 Hamming Weight

**Definition 1** *The Hamming weight $w_H(\underline{x})$ of a vector $\underline{x} \in \mathbb{F}_2^n$ is the number of non-zero elements in $\underline{x}$.*

### 1.1 Properties of Hamming Weight

1. $w_H(\underline{x}) \geq 0$ with equality iff $\underline{x} = \underline{0}$.
2. $w_H(\underline{x} + \underline{y}) \leq w_H(\underline{x}) + w_H(\underline{y})$ (Triangle inequality).
3. $w_H(\underline{x} + \underline{y}) = w_H(\underline{x}) + w_H(\underline{y}) - 2w_H(\underline{x} \bigodot \underline{y})$, where $\underline{x} \bigodot \underline{y}$ is the schur product of $\underline{x}$ and $\underline{y}$.

The following is an example (and verification) of the triangle inequality in $\mathbb{F}_2^4$ .

$$\underline{x} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} ; \underline{y} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} ; \underline{x} + \underline{y} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$w_H(\underline{x}) = 3, w_H(\underline{y}) = 3, w_H(\underline{x} + \underline{y}) = 2$
$w_H(\underline{x}) + w_H(\underline{y}) = 3 + 3 = 6 \geq 2 = w_H(\underline{x} + \underline{y})$.

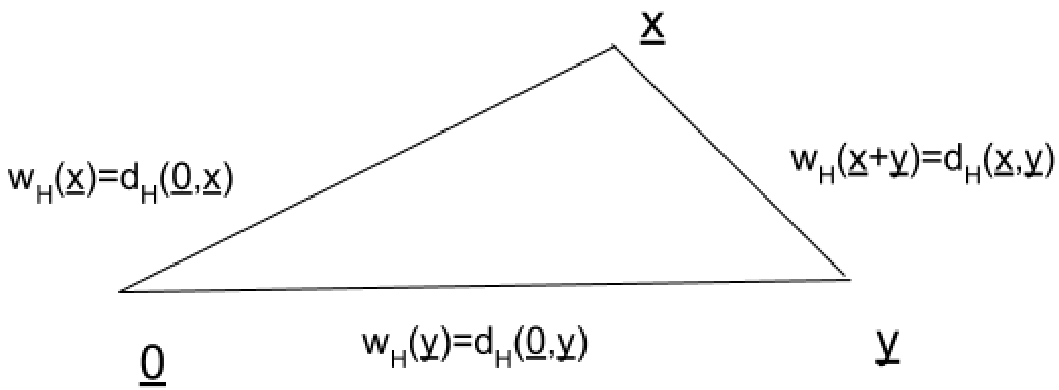


Figure 1: Triangular Inequality of Hamming Weight

# 2 Hamming Distance

**Definition 2** *The Hamming distance* $d_H(\underline{x}, \underline{y})$ *between two vectors* $\underline{x}, \underline{y} \in \mathbb{F}_2^n$ *is the number of coordinates such that* $x_i \neq y_i$, $1 \leq i \leq n$ *.*

Clearly, $d_H(\underline{x}, \underline{y}) = w_H(\underline{x} + \underline{y})$

## 2.1 Properties

1. $d_H(\underline{x}, \underline{y}) \geq 0$, equality hold iff $\underline{x} = \underline{y}$
2. $d_H(\underline{x}, \underline{y}) = d_H(\underline{y}, \underline{x})$
3. $d_H(\underline{x}, \underline{y}) \leq d_H(\underline{x}, \underline{z}) + d_H(\underline{z}, \underline{y})$

# 3 Binary Block Code

**Definition 3** *A binary block code* $\mathbb{C}$ *of block length* $n$ *is simply any subset of* $\mathbb{F}_2^n$*. The elements of* $\mathbb{C}$ *are called codewords.*

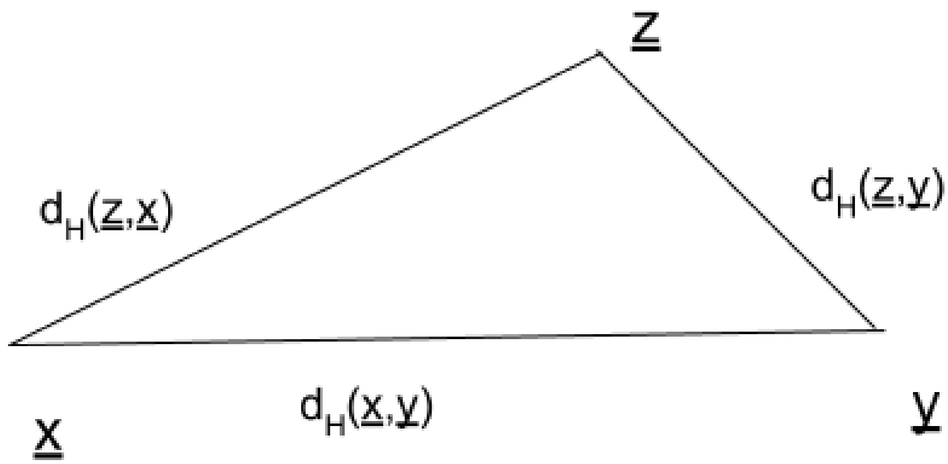


Figure 2: Triangular Inequality of Hamming Distance

## 3.1 Parameters of Binary Block code $\mathbb{C}$

1. Block length = n,
2. Size $M = \mid \mathbb{C} \mid$,
3. Rate $R = \frac{(\log_2 |C|)}{n}$ of the code in bits per channel use,
4. The minimum distance $d_{min}(\mathbb{C}) = min\{d_H(\underline{c_1}, \underline{c_2}) \mid \underline{c_1}, \underline{c_2} \in \mathbb{C}, \underline{c_1} \neq \underline{c_2}\}$.

## 3.2 Some Examples of Block Codes

- **Repetition Code** :

$$\mathbb{C} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\}$$

  The parameters of repetition code are:

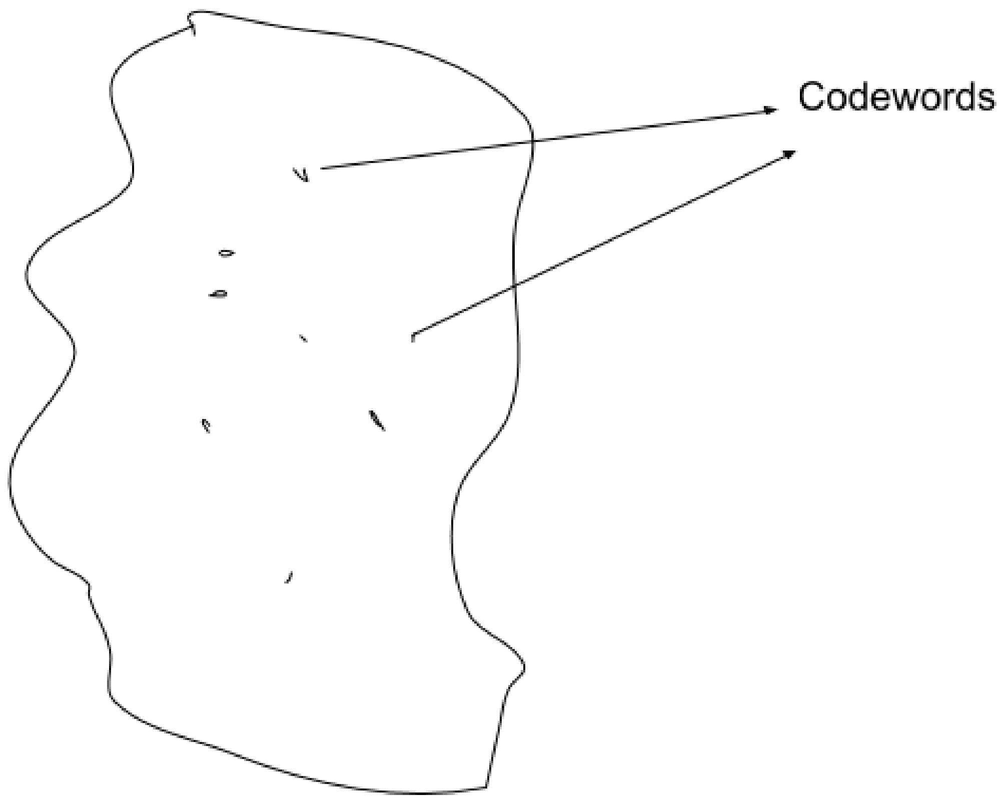


Figure 3: $\mathbb{F}_n^2$

1. $n = 7$
2. $M = 2$
3. R=$\frac{1}{7}$ bits/channel use
4. $d_{min} = 7$

- **Single Parity Check code**:

$$\mathbb{C} = \left\{ \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} \right\} \text{ such that } c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 = 0$$

  1. $n = 7$
  2. $M = 2^6 = 64$
  3. $R = \frac{6}{7}$
  4. $d_{min} = 2$

- **Hamming Code**:

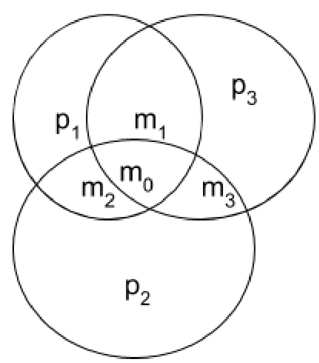


Figure 4: Hamming Code

$$\mathbb{C} = \left\{ \begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} \right\}$$

1. $n = 7$
2. $M = 2^4 = 16$
3. $R = \frac{4}{7}$
4. $d_{min} = 3$

# 4 $(t_c, t_d)$ code

**Definition 4** *A $(t_c, t_d)$ block code is a code $\mathbb{C}$ of block length $n$ having the properties that*
*i) any error pattern of $\leq t_c$ errors can be detected and corrected,*
*ii)if the number of errors $t$ is such that $t_c < t \leq t_d$, then the code is able to declare the presence of uncorrected error.*

**Lemma 5** *A code $\mathbb{C}$ of block length $n$ and minimum distance $d_{min}$ is a $(t_c, t_d)$ code iff $t_c + t_d + 1 \leq d_{min}$.*

*Proof:* We will first prove the if part using a decoding algorithm.
Let $\underline{x} \in \mathbb{F}_2^n, t \geq 0$.

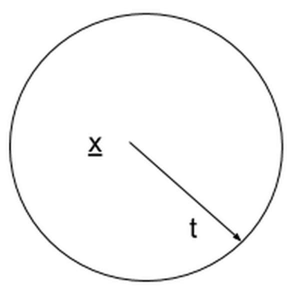


Figure 5: A ball of radius t centered at $\underline{x}$

Define $B(\underline{x}, t) = \{\underline{y} \in \mathbb{F}_2^n \mid d_H(\underline{x}, \underline{y}) \leq t\}$.

**The proposed decoding algorithm:** Let $\underline{y}$ denote the received vector. Consider the ball $B(\underline{y}, t_c)$. If this ball contains a codeword $\underline{c} \in \mathbb{C}$, then we declare $\underline{c}$ as the transmitted codeword else we declare an uncorrected error.

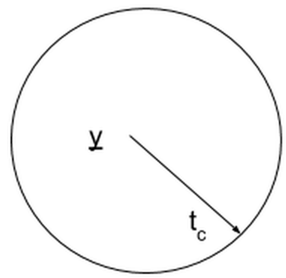


Figure 6: A ball of radius $t_c$ centered at $\underline{y}$

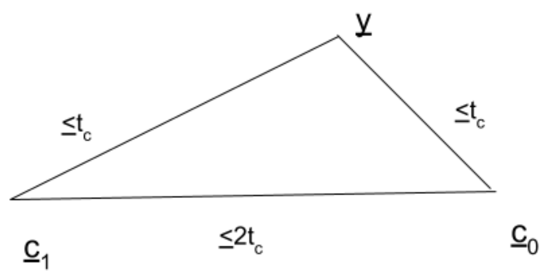


Figure 7: Triangle Inequality

**Proof of 'if' part:**

**case(i):** Let the number of errors be t $\leq t_c$ and $\underline{c_0}$ be the transmitted codeword. $\implies d_H(\underline{y}, \underline{c_0}) \leq t_c$.
Suppose $d_H(\underline{y}, \underline{c_1}) \leq t_c$, where $\underline{c_1} \neq \underline{c_0}$ is a codeword. Then by triangle inequality $d_H(\underline{c_0}, \underline{c_1}) \leq 2t_c \leq t_c+t_d \leq t_c+t_d+1 < d_{min}$ which is a contradiction. Hence, the ball $B(\underline{y}, t_c)$ contains only the transmitted codeword $\underline{c_0}$ and we have identified the correct codeword.

**case(ii):** Let the number of errors $t$ be such that $t_c < t \leq t_d$. Let $\underline{c_o}$ be the transmitted codeword. $\implies t_c < d_H(\underline{y}, \underline{c_0}) \leq t_d$.
Suppose there exists a codeword $\underline{x} \in \mathbb{C}$ such that $d_H(\underline{y}, \underline{x}) \leq t_c$. Then, by triangle inequality $d_H(\underline{c_0}, \underline{x}) \leq t_d + t_c \leq t_d + t_c + 1 < d_{min}$ which is a contradiction. Thus, there is no codeword in $\mathbb{B}(\underline{y}, \underline{t_c})$ and the decoder will declare an uncorrectable error.

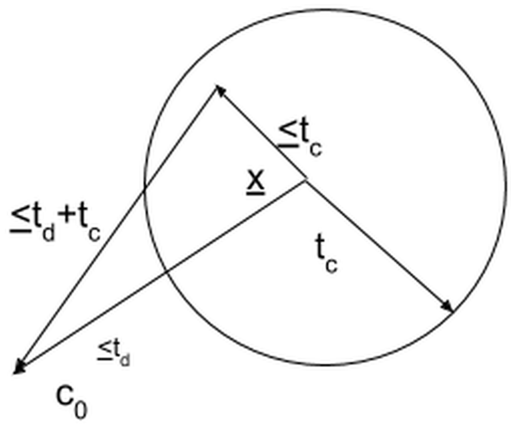


Figure 8: Triangle Inequality

**Proof of 'only if' part:** Suppose $d_{min} \leq t_c + t_d$ and let $\underline{c_1}, \underline{c_2} \in \mathbb{C}$ be such that $d_H(\underline{c_1}, \underline{c_2}) = d_{min}$.
Find u,v such that $d_{min} = u + v$, $u \leq t_c$ and $t_c < v \leq t_d$.
Let $\underline{y}$ be such that $d_H(\underline{y}, \underline{c_1}) = u$ and $d_H(\underline{y}, \underline{c_2}) = v$.
$\implies d_H(\underline{y}, \underline{c_1}) \leq t_c$, $d_H(\underline{y}, \underline{c_2}) \leq t_d$.

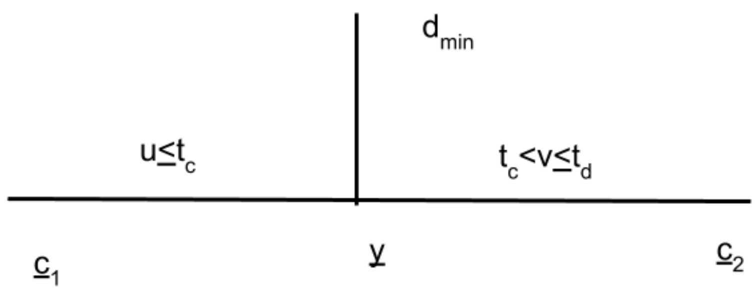


Figure 9: Decoder in unresolvable dilemma

If $\underline{y}$ is received, on the one hand, the decoder should decode to $\underline{c_1}$ and on the other hand, it should declare an uncorrectable error (corresponding to transmitted codewords $\underline{c_1}, \underline{c_2}$ respectively).
Clearly, no decoder will work to make this a $(t_c, t_d)$ code. $\square$