Summary on Lecture 18, May 9th, 2016

We continue with an introduction to coding theory.

Recall we have defined the *Hamming metric* as follows. Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{Z}_2^n$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbf{Z}_2^n$. Then the distance between $\mathbf{x}$ and $\mathbf{y}$ is given as

$$\delta(\mathbf{x}, \mathbf{y}) = |\{ \ j \mid x_j \neq y_j \ \}| ,$$

i.e., $\delta(\mathbf{x}, \mathbf{y})$ is the number of corresponding entries of $\mathbf{x}$ and $\mathbf{y}$ which are different.

The pair $(\mathbf{Z}_2^n, \delta)$ is an example of a *metric space*.

Definition. Let $r \geq 1$ be a positive integer, and $\mathbf{x} \in \mathbf{Z}_2^n$. Then the set $B_r(\mathbf{x}) = \{ \ \mathbf{y} \mid \delta(\mathbf{x}, \mathbf{y}) \leq r \ \}$ is called a *closed ball of radius* r.

Theorem 2. *Let $m, n \in \mathbf{Z}_+$, and $m < n$. Assume $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ is an encoding function, such that $C = \alpha(\mathbf{Z}_2^m) \subset \mathbf{Z}_2^n$.*

(a) *If $\delta(\mathbf{x}, \mathbf{y}) > r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$, then a transmission τ with $\delta(\mathbf{c}, \tau(\mathbf{c})) \leq r$ can always be detected, i.e., a transmission with at most r errors can always be detected.*

(b) *If $\delta(\mathbf{x}, \mathbf{y}) > 2r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$, then a transmission τ with $\delta(\mathbf{c}, \tau(\mathbf{c})) \leq r$ can always be detected and corrected.*

Proof. (a) Let $\mathbf{c} \in C$ and we consider the ball $B_r(\mathbf{c})$. Then, since $\delta(\mathbf{x}, \mathbf{y}) > r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$, we have that $B_r(\mathbf{c}) \cap C = \{\mathbf{c}\}$: indeed, all other elements of C are further away from the center $\mathbf{c}$ of the ball. It means that for any transmission with number of errors between 1 and r we should have that $\tau(\mathbf{c}) \neq \mathbf{c}$, and $\tau(\mathbf{c}) \in B_r(\mathbf{c})$. We obtain that $\tau(\mathbf{c}) \notin C$. This means that such an error could be detected.

(b) As we have seen, the condition $\delta(\mathbf{x}, \mathbf{y}) > 2r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$ implies that for any transmission with number of errors between 1 and r we should have that $\tau(\mathbf{c}) \neq \mathbf{c}$, and $\tau(\mathbf{c}) \in B_r(\mathbf{c})$. On the other hand, for every $\mathbf{x} \in C$ such that $\mathbf{x} \neq \mathbf{c}$, $2r < \delta(\mathbf{c}, \mathbf{x}) \leq \delta(\mathbf{c}, \tau(\mathbf{c})) + \delta(\tau(\mathbf{c}), \mathbf{x})$. By assumption, $\delta(\mathbf{c}, \tau(\mathbf{c})) < r$. Then it means that $\delta(\tau(\mathbf{c}), \mathbf{x}) > r$, or that $\tau(\mathbf{c}) \notin B_r(\mathbf{x})$. Since $\tau(\mathbf{c}) \in B_r(\mathbf{c})$, it means that $\mathbf{c}$ is the only element of C which could be transmitted to $\tau(\mathbf{c})$. □

The parity-check and generator matrices.

Example. We consider the encoding function $\alpha : \mathbf{Z}_2^3 \to \mathbf{Z}_2^6$ given by the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}, \quad \alpha : [w_1, w_2, w_3] \mapsto [w_1, w_2, w_3]G$$

Since $\mathbf{Z}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$, we compute:

$$C = \alpha(\mathbf{Z}_2^3) = \{000000, 001101, 010011, 011110, 100110, 101011, 110101, 111000\}.$$

We notice that $\delta(x, y) > 2$ for all $x, y \in C$. It means that all single errors could be detected and corrected.

We examine closely the homomorphism $\alpha : \mathbf{Z}_2^3 \to \mathbf{Z}_2^6$:

$$\alpha : [w_1, w_2, w_3] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [w_1, w_2, w_3, w_4, w_5, w_6],$$

where

$$\left\{ \begin{array}{lcl} w_4 & = & w_1 + w_3 \\ w_5 & = & w_1 + w_2 \\ w_6 & = & w_2 + w_3 \end{array} \right. \quad \text{or} \quad \left\{ \begin{array}{lcl} w_1 + w_3 + w_4 & = & 0 \\ w_1 + w_2 + w_5 & = & 0 \\ w_2 + w_3 + w_6 & = & 0 \end{array} \right.$$

Here we keep in mind that we work mod 2. In matrix notations, we have:

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} [w_1, w_2, w_3, w_4, w_5, w_6]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

We denote:

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [B|I_3], \quad \text{where} \quad B = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We notice that

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [I_3|A], \quad \text{where} \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

We see that $B = A^T$. Let $\mathbf{c} \in C$, then

$$H\mathbf{c}^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Let $\mathbf{c} = 100110$, and $\tau(\mathbf{c}) = 101110$. Then we can check:

$$H\tau(\mathbf{c})^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} [1\ 0\ 1\ 1\ 1\ 0] = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

We notice that $H\tau(\mathbf{c})^T$ is exactly the third column of the matrix H. We also have that $\tau(\mathbf{c}) = 101110 = \mathbf{c} + \mathbf{e}$, where $\mathbf{e} = 001000$. We have:

$$H\tau(\mathbf{c})^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

We see that we can see immediately that the third digit of $\tau(\mathbf{c})$ should be corrected to recover $\mathbf{c}$.