Summary on Lecture 19, May 11th, 2016

The parity-check and generator matrices, more.

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 $\mathbf{c}$.

Matrix Codes: the general case

Let $n > m$, and we consider a function $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ given as $\alpha(\mathbf{w}) = \mathbf{w}G$, where G is $m \times n$-matrix over $\mathbf{Z}_2$. Furthemore, we assume that G has the form $G = [I_m|A]$, where I_m is the identity matrix, and A is $m \times (n-m)$-matrix over $\mathbf{Z}_2$. Then the matrix G is called a *generating matrix*. The code is given then as $C = \alpha(\mathbf{Z}_2^m) \subset \mathbf{Z}_2^n$. The matrix $H = [B, I_{n-m}]$, where $B = A^T$ is called the *parity check matrix*.

We have that if $\mathbf{w} = [w_1 \dots w_m]$, then

$$\alpha : [w_1 \dots w_m] \mapsto [w_1 \dots w_m \; w_{m+1} \dots w_n],$$

where $H[w_1 \dots w_m \; w_{m+1} \dots w_n]^T = \mathbf{0}$, where $\mathbf{0}$ is $(n-m)$-dimensional column zero vector.

Lemma 1. *Let $G = [I_m|A]$ be a generating matrix and $H = [B|I_{n-m}]$ be the corresponding parity check matrix. Assume that*

(i) *the matrix H does not contain a zero column;*
(ii) *the matrix H does not contain two identical columns.*

Then the distance $\delta(\mathbf{x}, \mathbf{y}) > 2$ for all $\mathbf{x}, \mathbf{y} \in C$ with $\mathbf{x} \neq \mathbf{y}$, and all single errors could be detected and corrected.

Proof. It is enough to show that a distance between different strings in C is greater than two.

Assume we have two strings $\mathbf{x}, \mathbf{y} \in C$ with $\delta(\mathbf{x}, \mathbf{y}) = 1$. Then $\mathbf{y} = \mathbf{x} + \mathbf{e}$, where $\mathbf{e}$ is a string with just one entry 1 and all other entries are zeros. Say, we have $\mathbf{e} = [0 \dots \; 0 \; 1 \; 0 \dots 0]$, where 1 is the k-th entry. Then

$$\mathbf{0} = H\mathbf{y}^T = H\mathbf{x}^T + H\mathbf{e}^T = H\mathbf{e}^T,$$

which is the k-th column of the matrix H. However, the matrix H does not have a zero column. Contradiction.

Assume we have two strings $\mathbf{x}, \mathbf{y} \in C$ with $\delta(\mathbf{x}, \mathbf{y}) = 2$. Then $\mathbf{y} + \mathbf{e}_1 = \mathbf{x} + \mathbf{e}_2$, where $\mathbf{e}_1$ and $\mathbf{e}_2$ are strings with just one entry 1 and all other entries are zeros. Then we have that $\mathbf{y} = \mathbf{x} + \mathbf{e}_1 + \mathbf{e}_2$, and we check:

$$\mathbf{0} = H\mathbf{y}^T = H\mathbf{x}^T + H\mathbf{e}_1^T + H\mathbf{e}_2^T = H\mathbf{e}_1^T + H\mathbf{e}_2^T.$$

We obtain that $H\mathbf{e}_1^T = H\mathbf{e}_2^T$: we rememeber that we work mod 2. However, the matrix H does not have equal columns. Contradiction. $\square$