Summary on Lecture 20, May 13th, 2016

Decoding algorithm

Now we describe a decoding algorithm. We denote $\mathbf{e}_j = 00\ldots010\ldots$, where 1 is the j-th entry.

Decoding algorithm: `Assume we have received a message` $\mathbf{v} \in \mathbf{Z}_2^n$.

(1) `If` $H\mathbf{v} = \mathbf{0}$, `then the message is correct.`

(2) `If` $H\mathbf{v} = \mathbf{h}_j$, `where` $\mathbf{h}_j$ `is the` j`-th column of` H, `then we decode the message` $\mathbf{v} \mapsto \mathbf{v} + \mathbf{e}_j$.

(3) `If (1) and (2) do not apply, we ask to resend the message again since there are at least two errors, and we do not have a reliable way to decode` $\mathbf{v}$.

An encoding function $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ given by a generator matrix $G = [I_m|A]$, where $\alpha : \mathbf{w} \to \mathbf{w}G$, is an example of a group code, i.e., when the $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ is a group homomorphism.

Example. We consider the encoding function $\alpha : \mathbf{Z}_2^4 \to \mathbf{Z}_2^7$ given by the matrix

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

Then we obtain the parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We notice that if we add any non-zero column to H, than we will have to repeat one of the columns of H. Indeed, there are 3 elements in each column, and there are $2^3 = 8$ binary strings of the length 3. Since H cannot have a zero column, it means that $2^3 - 1 = 7$ is the maximal number of non-zero columns for such a matrix H.

Let $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ given by a generator matrix $G = [I_m|A]$, then we denote $k = n - m$, and then $H = [B|I_k]$. Since H should have different columns, the maximal number of columns in H is $2^k - 1$. In that case B is $k \times (2^k - 1 - k)$-matrix. In the case when the parity-check matrix H has maximal number of columns, we call H a *Hamming matrix*.

Examples. With $k = 4$, a possible Hamming matrix is

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

With $k = 5$, a possible Hamming matrix is

$$H = \left[\begin{array}{cccccccccccccccccccccccccc|ccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Clearly, we can use any of these matrices for a parity-check.

Lemma 2. *Assume $G = [I_m|A]$ is a generator matrix, and $H = [B|I_k]$ is the corresponding parity-check matrix with maximal number of columns $2^k - 1 - k$. Let $C = \alpha(\mathbf{Z}_2^m)$. Then there exist two strings $\mathbf{x}, \mathbf{y} \in C$ such that $\delta(\mathbf{x}, \mathbf{y}) = 3$.*

Proof. Let $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ be the corresponding encoding function. We have that $n - m = k$, and $n = 2^k - 1$. Thus $m = 2^k - 1 - k$. Let $\mathbf{x} \in C = \alpha(\mathbf{Z}_2^m)$. We consider a ball $B_1(\mathbf{x})$. Since there are exactly $n = 2^k - 1$ strings $\mathbf{z} \in \mathbf{Z}_2^n$ such that $\delta(\mathbf{x}, \mathbf{z}) = 1$, the ball $B_1(\mathbf{x})$ contains $n + 1 = 2^k - 1 + 1 = 2^k$ elements.

Now let $\mathbf{x}, \mathbf{y} \in C$. We choose any two elements $\mathbf{z} \in B_1(\mathbf{x})$ and $\mathbf{u} \in B_1(\mathbf{y})$. From Lemma 1, $\delta(\mathbf{x}, \mathbf{y}) \geq 3$. We notice:

$$3 \leq \delta(\mathbf{x}, \mathbf{y}) \leq \delta(\mathbf{x}, \mathbf{z}) + \delta(\mathbf{z}, \mathbf{u}) + \delta(\mathbf{u}, \mathbf{y}) \leq 1 + \delta(\mathbf{z}, \mathbf{u}) + 1.$$

We obtain that $\delta(\mathbf{z}, \mathbf{u}) \geq 1$. In particular, $\mathbf{z} \neq \mathbf{u}$, and $B_1(\mathbf{x}) \cap B_1(\mathbf{y}) = \emptyset$.

Since the balls $B_1(\mathbf{y})$ are disjoint, and we have 2^m elements in C, we obtain that the union

$$\bigcup_{\mathbf{x} \in C} B_1(\mathbf{x})$$

contains $2^m \cdot 2^k = 2^{m+k} = 2^n$ elements. This means that

$$\bigcup_{\mathbf{x} \in C} B_1(\mathbf{x}) = \mathbf{Z}_2^n.$$

Now we choose any $\mathbf{x} \in C$ and take $\mathbf{e}_{ij} \in \mathbf{Z}_2^n$, a binary sequence with 1's in i-th and j-th places, and zeros otherwise. Let $\mathbf{z} = \mathbf{x} + \mathbf{e}_{ij}$. Clearly, $\delta(\mathbf{x}, \mathbf{z}) = 2$, so $\mathbf{z} \notin B_1(\mathbf{x})$. However, $\mathbf{z} \in B_1(\mathbf{y})$ for some $\mathbf{y} \in C$. Assume that $\mathbf{z} = \mathbf{y}$, then we would have that $\mathbf{z} \in C$, however, $\delta(\mathbf{x}, \mathbf{z}) \geq 3$ by Lemma 1. Contradiction. Then we have that $\mathbf{z} \neq \mathbf{y}$, and $\delta(\mathbf{y}, \mathbf{z}) = 1$. Then we have

$$\delta(\mathbf{x}, \mathbf{y}) \leq \delta(\mathbf{x}, \mathbf{z}) + \delta(\mathbf{z}, \mathbf{y}) = 2 + 1 = 3$$

We obtain that $\delta(\mathbf{x}, \mathbf{y}) \leq 3$, and Lemma 1 gives us that $\delta(\mathbf{x}, \mathbf{y}) \geq 3$. This means $\delta(\mathbf{x}, \mathbf{y}) = 3$. $\square$