Lecture 18.

The topic of this lecture is binary Hamming codes Ham$(r, 2)$. I followed the first half of Chapter 8 in the text quite closely. Here are the highlights.

**Definition and basic properties**

The Hamming code Ham$(r, 2)$ is defined by its parity matrix $H$. The columns of $H$ are the non-zero binary columns of length $r$. For example, for $r = 2$, we have

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

and for $r = 3$,

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$  

Note that $H$ has $r$ rows and $2^r - 1$ columns. The order of the columns can vary, so Ham$(r, 2)$ is not a single code but a family of equivalent codes. To work with Ham$(r, 2)$, one needs to specify the parity check matrix $H$.

One particular ordering is to choose column $j$ so that it spells $j$ in binary. This is what I did in the examples above. For example, 001 is the binary representation of 1, 010 is the binary representation of 2, 101 is the binary representation of 5, etc.

Another convenient way to order the columns of $H$ is to form the identity matrix in front, so that $H$ is in standard form (as a generator matrix), e.g.,

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$
for $r = 2$ and
\[
H = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1
\end{pmatrix}
\]
for $r = 3$. In particular, for this ordering of the columns (and thus for any other), we see that the rows of $H$ are linearly independent. This is important because it shows that $H$ is a legitimate parity check matrix for any $r$.

**Theorem.** (a) Ham($r$, 2) is a linear code of length $n = 2^r - 1$ and dimension $k = n - r = 2^r - r - 1$.
(b) Ham($r$, 2) has minimal distance 3.
(c) Ham($r$, 2) is a perfect code.

For a proof, see Theorem 8.2 in the text.

**Decoding with a binary Hamming code**

Since the minimal distance of Ham($r$, 2) is 3, the goal of our decoding scheme will be to correct up to one error.

If the received word is $\overline{y}$, we begin by computing the syndrome $S(\overline{y}) = \overline{y} \cdot H^T = (a_1, \ldots, a_r)$. If $S(\overline{y}) = \overline{0}$, we will assume that no error occurred.

Now suppose $S(\overline{y}) \neq \overline{0}$. Let us try to match it to an error vector $\overline{e}$ of weight 1. An error vector of weight 1 has the form
\[
\overline{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0),
\]
where 1 is in position $j$. Note that here
\[1 \leq j \leq 2^r - 1.\]
The syndrome $S(\overline{e}_j) = \overline{e}_j \cdot H^T = (s_1, \ldots, s_r)$, where $(s_1, \ldots, s_r)$ is the transpose of the $j$th column of $H$. 

2
Thus our decoding scheme is as follows. If $S(\overline{y}) = \overline{0}$, assume no error occurred and decode $\overline{y}$ as $\overline{x} = \overline{y}$.

If $S(\overline{e}_j) = (s_1, \ldots, s_r)$, assume that one error occurred in position $j$, where $(s_1, \ldots, s_r)^T$ is column $j$ of $H$. Decode $\overline{y}$ as $\overline{x} = \overline{y} - \overline{e}_j$.

Note that this is a complete decoding scheme; we can decode $\overline{y}$ no matter what the syndrome is. The reason for this is that Ham($r$, 2) is perfect.

Examples for $r = 3$ with

\[
H = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}.
\]

(1) Received vector: $\overline{y} = (1, 1, 1, 1, 1, 1, 1)$. Here $S(\overline{y}) = (0, 0, 0)$, so assume no error. Decode $\overline{y}$ as $\overline{x} = \overline{y}$.

(2) Received vector: $\overline{y} = (1, 1, 0, 0, 0, 0, 0)$.

Calculate the syndrome: $S(\overline{y}) = (0, 1, 1)$. Since 011 is the binary representation of 3, we assume the error is in position 3, i.e., the error vector is $\overline{e} = (0, 0, 1, 0, 0, 0, 0)$. Decode $\overline{y}$ as $\overline{x} = \overline{y} - \overline{e} = (1, 1, 1, 0, 0, 0, 0)$.

(3) Received vector $\overline{y} = (0, 0, 0, 0, 1, 1, 1)$.

Match the syndrome: $S(\overline{y}) = (0, 0, 1)$ to column 1 of $H$. Thus the error is in position 1. Decode $\overline{y}$ as $\overline{x} = \overline{y} - \overline{e} = (1, 0, 0, 0, 0, 1, 1)$. 
Extended binary Hamming code $\text{Ham}(r, 2)$

$\text{Ham}(r, 2)$ is obtained by extending $\text{Ham}(r, 2)$, i.e., adding a parity check digit to each codeword. That is, for each codeword $\bar{x} = (x_1, \ldots, x_n)$ in $\text{Ham}(r, 2)$, we create a new codeword $\bar{x}' = (x_1, \ldots, x_n, x_{n+1})$, where $x_1 + \cdots + x_n + x_{n+1} = 0$ in $F_2$. Here $n = 2^r - 1$.

One readily sees that $\text{Ham}(r, 2)$ is a linear code of length $n+1 = 2^r$. It has the same number of words as $\text{Ham}(r, 2)$ and thus the dimension remains the same, $n - r = 2^r - r - 1$. Finally, the minimal distance goes up by 1, from 3 to 4; see Theorem 2.7 in the book.

Note that $\text{Ham}(r, 2)$ is not perfect; a perfect code has to have odd minimal distance. It also cannot correct more than one error. So, for the purpose of error correction, there is no advantage to using $\text{Ham}(r, 2)$ over $\text{Ham}(r, 2)$. However, $\text{Ham}(r, 2)$ is better suited to error detection. I will discuss the decoding scheme for $\text{Ham}(r, 2)$ in the next lecture.