Lecture 4: Hamming codes and beyond

We shall now construct a family of linear 1-error correcting codes. We shall do this by constructing the parity check matrices for the codes.

Let $r \geqslant 2$.

We let H be the $r \times (2^r - 1)$ matrix whose columns are all possible binary strings of length r written in increasing binary no. form.

Example

(1) $r = 2$. Then $H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

(2) $r = 3$. Then

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

The codewords determined by H which is an $r \times (2^r - 1)$ matrix have length $2^r - 1$.

The number of message bits is $2^r - 1 - r$.

Thus we obtain a family of

$$(2^r - 1,\ 2^r - 1 - r) - \text{codes called}$$

the <u>Hamming codes</u>.

The columns of H are distinct and none of them is zero. Thus these codes can correct 1 error (at most).

If y is the received vector then Hy^T will be column i, say, of H. Then the error bit will be the ith bit of y.

I conclude with the following result which tells us where to start looking if we want to find linear codes that correct more than 1 error.

<u>Theorem</u> Let C be a linear (n,k)-code with parity check matrix H. Then the min. distance of C is d iff

- any $d-1$ columns of H are linearly <u>independent</u>, but
- some d columns are linearly dependent.

<u>Proof</u> Since the code is linear, the minimum distance is equal to the minimum weight.

Let $\underline{x}$ be a codeword of min weight d.

Then $H\underline{x}^T = \underline{0}$. Let $\underline{x} = (x_1, \dots, x_n)$

and let $H = \left(\underline{h}_1^T \dots \underline{h}_n^T \right)$ where the $\underline{h}_i$ are column vectors.

Then $H \underline{x}^T = \underline{0} \iff$

$$\sum_{i=1}^{n} x_i \, \underline{h}_i^T = \underline{0}$$

$\Rightarrow$ d columns of H are linearly dep.
(corresponding to the positions in $\underline{x}$ where $x_i \neq 0$).

Now observe that if some $d-1$ columns of H were linearly dependent then this would imply the existence of a non-zero codeword of weight d which contradicts the fact that the min. weight of C is d.

S'pose now that the two conditions hold. We see that this implies that there is a codeword of weight d and that there are no non-zero codewords of smaller weight. $\blacksquare$