I

Lesson 4

Review

Let

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

be the parity check matrix for a [7,4] Hamming code

To obtain a generating matrix, G we find the null space for $Hx=0$. Thus we row reduce H:

$$\rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$ is row reduced

So
$$\begin{aligned} x_1 + x_3 + x_5 + x_7 &= 0 \\ x_2 + x_3 + x_6 + x_7 &= 0 \\ x_4 + x_5 + x_6 + x_7 &= 0 \end{aligned}$$

or
$$\begin{aligned} x_1 &= x_3 + x_5 + x_7 \\ x_2 &= x_3 + x_6 + x_7 \\ x_4 &= x_5 + x_6 + x_7 \end{aligned}$$

Let $x_7 = 1$, $x_3 = x_5 = x_6 = 0$ get
$(1, 1, 0, 1, 0, 0, 1)$

Let $x_6 = 1$ $x_3 = x_5 = x_7 = 0$ get
$(0, 1, 0, 1, 0, 1, 0)$

Let $x_5 = 1$ $x_3 = x_6 = x_7 = 0$ get

$(1, 0, 0, 1, 1, 0, 0)$

let $x_3 = 1$, $x_5 = x_6 = x_7 = 0$ GeT

$(1, 1, 1, 0, 0, 0, 0)$

This basis for the null space make up the rows of G

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

Note: I have put the rows in this order to match the book. Any order is fine.

To find C, the code space we compute

$$(a, b, c, d) \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} =$$

$(a+b+d, a+c+d, a, b+c+d, b, c, d)$

where a, b, c, d are 0 or 1.

Thus any $c \in C$ is of that form

Suppose some c is sent and we get $r = (1\,0\,0\,0\,1\,0\,0)$

compute $Hr^t = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

This is 4 in binary so the error is in position 4
$e = (0001000)$ and
$c = r + e = (1001100)$

Hamming codes are perfect codes
To see this we use the Hamming bound

$$|C| = 2^{\dim C} = 2^{2^m - 1 - m}$$

$$\cancel{\binom{n}{0} + \binom{n}{1}}$$

$$\binom{\dim \text{space}}{0} + \binom{\dim \text{space}}{1} =$$

$$\binom{2^m - 1}{0} + \binom{2^m - 1}{1} = 1 + 2^m - 1$$

$$= 2^m$$

So $|C|(2^m) = 2^{2^m - 1 - m} 2^m = 2^{2^m - 1}$
= number of vectors in the space. Thus the Hamming bound is in fact an equality so all vectors are in some ball of radius 1

Hamming Codes and Linear Codes in general benefit from the fact the code is a subspace. First, it is easier to find the designed distance d. Recall that d is the shortest $d(x,y)$, $x, y \in C$. Since C is a subspace, $x-y \in C$ also. So $d(x,y) = d(x-y, 0) =$ length $x-y$. Instead of computing the distance between every pair of vectors in C, we only need to compute the shortest vector in C, not including 0. So if C has k vectors, we need $k-1$ computations instead of $\binom{k}{2} = \frac{k(k-1)}{2}$

Ex $C = \{(1\,0\,1\,0), (1\,1\,0\,1), (0,1,1,1), (0,0,0,0)\}$ The lengths of the non zero vectors are $2, 3, 3$. So $d=2$. $(t=0)$

There is an even better way of computing d.

Theorem Let C be a linear code with parity check matrix H. Let s be the minimum number of linearly dependent columns of H. Then $s = d$.

Proof Let $C_{i_1} \ldots C_{i_s}$ be linearly ~~ind.~~ dependent colums of H
Then $x_{i_1} C_{i_1} + \cdots + x C_{i_s} = 0$ each $x = 1$
~~if~~ since s is the minimum number
let x be the vector with 1 in the positions $i_1, \ldots i_s$ and 0 in the others
Then $Hx = C_{i_1} + \cdots + C_{i_s} = 0$ so x is a code word of length s
If x is a code word of length s, x = vector with 1 is s positions 0 in rest and
$0 = Hx$ since x is a code word
The corresponding column vectors in H are linearly dependent
Hence the result holds

Ex $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ in a [7,4] Hamming code

The first 3 colums are linearly dependent so $s = 3 = d$. Hence $t = 1$ and the code is one error correcting.

The 1-1 for any Hamming code has the first 3 columns linearly dependent. $\begin{pmatrix}0\\0\\1\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}$

So $d=3$, $t=1$. Hamming codes are 1 error correcting

We know how to correct errors in Hamming codes. What about other linear codes? Begin by determing t, the number of errors that are guaranteed to be correctable. The errors will have 1's in t or fewer positions. We also have $Hc^t=0$ for all $c \in C$, so $Hr^t = Hc^t + He^t = He^t$. We know He^t and want to find e. Given r and C, we know all $r+c$, with $c \in C$. In particular, we do not compute all $r+c$, $c \in C$. $r+C$ is a left coset of C. Since $e=r+c$, e and r are in the same left coset. If e_1 and e_2, both of length less than or equal to t, are in the same left coset, then $r=e_1+c_1$, $r=e_2+c_2$ and r is t units or less away from two code words. That can not happen

7

~~So each coset has at most one vector of length less than or equal to t. The error vector is in the same coset~~

So each coset has at most one vector of length less then or equal to t. That vector is the error vector and is called the coset leader for the coset

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

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

The code has 3 linearly dependent columns, $t=1$ Thus the error vectors are $(1\,0\,0\,0\,0)$, $(0\,1\,0\,0\,0)$, $(0\,0\,1\,0\,0)$, $(0\,0\,0\,1\,0)$, $(0\,0\,0\,0\,1)$. Suppose $r = (0\,0\,0\,1\,1)$. $Hr^t = (0\,1\,1)^t$ which error vector e has $He^t = (0\,1\,1)^t$? Computation shows $e = (0\,0\,1\,0\,0)$. Thus $c = r + e = (0\,0\,1\,1\,1)$. This is ok but too much work

work. The idea is to compute He^T for each error vector and list e and He^T in a table when we want to correct r, we compute Hr^T, remembering $Hr^T = He^T$. Then to find e for that Hr^T we look at the table for that Hr^T and the coset leader is the error

Ex Continue with the last example

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

Here $t = 1$ since the last 3 columns are linearly dependent.

Coset Leaders e	Syndrones He^T
(1 0 0 0 0)	(1 1 1)
(0 1 0 0 0)	(1 0 0)
(0 0 1 0 0)	(0 1 1)
(0 0 0 1 0)	(0 1 0)
(0 0 0 0 1)	(0 0 1)

TABLE 1

Suppose $v = (0\,0\,0\,1\,1)$.
Compute $Hv^t = (0\,1\,1)^t$
$\rightarrow e = e_3 = (0\,0\,1\,0\,0)$
$\rightarrow c = v + e = (0\,0\,1\,1\,1)$

Suppose $v = (0\,1\,0\,0\,1)$
$Hv^t = (1\,0\,1)^t$
This vector is not a syndrome in the table. v has more than one error and can not be corrected.

This code has $2^5 = 32$ ~~code words~~ vectors. There are 5 rows in the table, each representing $|C|$ elements in the coset. Hence $5|C| = 20$ elements can be corrected. There are also 4 code words. Hence $32 - 24 = 8$ vectors can not be corrected.

Notice that if $t = 2$, then the coset leader column will have not only all vectors with 1 one but also all vectors with 2 one's

Problems p. 90 9, 10, 15, 16, 17
Also 11, 12, 13, 14