Lesson 3

Linear Codes

If the set of codes is a subspace of Z_2^n, then the code is called linear. One way to construct a linear code of dimension m in Z_2^n is to use an $m \times n$ matrix of full row rank. This means the row vectors are linearly independent

Ex Let

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

The rows of G are linearly independent as seen by setting a linear combination of them equal to 0 and finding the coefficents are 0

Let r_1, r_2, r_3, r_4 be the rows. Then

$$c_1 r_1 + c_2 r_2 + c_3 r_3 + c_4 r_4 = 0$$

The last column is

$$c_1 0 + c_2 0 + c_3 0 + 1 c_4 = 0 \qquad c_4 = 0$$

The 6 th coulomn is

$$c_1 0 + c_2 0 + c_3 \cdot 1 = 0 \qquad c_3 = 0$$

The 5 th column is

$$c_1 \cdot 0 + c_2 \cdot 1 = 0 \qquad c_2 = 0$$

What is left shows $C_1 = 0$

Now G takes vectors v of length m into vectors in Z_2^n (of length n) by $vG = c$. Here

$$(1\ 1\ 0\ 1)\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} =$$

$(1\ 0\ 1\ 0\ 1\ 0\ 1) \in C$, the code space. The space Z_2^m is the space of information, G makes into longer vectors so that error correction is possible

The null space of G is ultra important for error correction. Compute it for G

$$G\begin{pmatrix} x_1 \\ \vdots \\ x_7 \end{pmatrix} = 0$$

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

Solving this set mod 2 gives a basis for the null space

$(0\ 0\ 0\ 1\ 1\ 1\ 1)^T$
$(0\ 1\ 1\ 0\ 0\ 1\ 1)^T$
$(1\ 0\ 1\ 0\ 1\ 0\ 1)^T$

let H be the matrix with these vectors as it's rows

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

By this solution, $GH^T = 0$ and $HG^T = 0$. The columns in G^T are a basis for the null space of H. Hence one could start with H, find its null space and a basis would be the rows of G (just the reverse process from where we started

G is called the generator matrix for the code and H is called the parity check matrix. The first use for H is checking if a vector r is a code vector. It is iff $Hr^T = 0$ (ie, it is in C)

This process can be done for any G of full row rank (or any H of full row rank; meaning linearly independent rows. The G and H we have been looking at are

special. They are for a Hamming code. H is always of size $n \times 2^n - 1$. Here $n=3$, but there are cases for each n. G will be $(2^n-1-n) \times 2^n-1$. Here G is 4×8. The next case, $n=4$, H is 4×15 and G is 11×15. Examples are in the book.

There is another feature for H that is special. The column entries are that column in binary. Here

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

The last row is for the 1 digit
The next row is for the 2 digit
The next row is for the $2^2=4$ digit

So
$$\begin{aligned} 1 &= 1\cdot 1 + 0\cdot 2 + 0\cdot 4 \\ 2 &= 0\cdot 1 + 1\cdot 2 + 0\cdot 4 \\ 3 &= 1\cdot 1 + 1\cdot 2 + 0\cdot 4 \\ 4 &= 0\cdot 1 + 0\cdot 2 + 1\cdot 4 \\ 5 &= 1\cdot 1 + 0\cdot 2 + 1\cdot 4 \\ 6 &= 0\cdot 1 + 1\cdot 2 + 1\cdot 4 \\ 7 &= 1\cdot 1 + 1\cdot 2 + 1\cdot 4 \end{aligned}$$

Gives us the rows. This will be useful in error correction

5

As always, we have $r = c + e$ where r is the received vector, c is the code vector and e is the error. As Always $Hc^T = 0$. Hence $Hr^T = He^T + Hc^T = He^T$. We know H and r. We want to find e for then we can find $c = r + e$. These facts are true for any linear code. Hamming codes have the advantage that the s'th column is s written in binary. Hamming codes, as we will see, are both 1 error correcting and perfect. So each e has 1 one and the rest 0. Whatever position the one is in, when we compute $Hr^T = He^T$, we get the column of H written in binary. Thus Hr^T will give us a column which reveals the position of the 1, written in binary

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

If ~~r = (0101011~~ $r = (1010001)$,

$Hr^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ which is 5 written in binary $\rightarrow$ $e = (0000100)$ and

$c = r + e = (1010101)$

6

Appendix Find Null Space

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

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

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

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

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

$x_1 = x_6 + x_7$

$x_2 = x_5 + x_7$

$x_3 = x_5 + x_6$

$x_4 = x_5 + x_6 + x_7$

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

Problems p 90 2, 6, 8

Hamming Codes 9, 10, 11, 12, 13, 14, 20

P. 0 Homework Solution

p 89 1 $C = \{(00000000) = c_1,$
$(11100011) = c_2,$
$(00011111) = c_3,$
$(11111100) = c_4\}$

$d(c_1, c_2) = 5$ $d(c_2, c_3) = 6$
$d(c_1, c_3) = 5$ $d(c_2, c_4) = 5$
$d(c_1, c_4) = 6$ $d(c_3, c_4) = 5$

$d = \min d(x,y) = 5$
$t = 2$

1 Find 2 vectors, not in C which are guaranteed to be correctable

(10000000), (01000000)

They are 1 unit from c_1 so, since $1 < t$, they are uniquely correctable

2. Find 2 vector that are 3 bit errors from every vector in C but still are uniquely correctable

$x = (10001010)$

$d(x, c_1) = 3$ $d(x, c_3) = 4$
$d(x, c_2) = 4$ $d(x, c_4) = 5$

So x is correctable to c_1

Try $y = (01001001)$

p 1/2

3 Find 2 vectors that are not uniquely correctable

$x = (01110000)$

$d(x, c_1) = 3$ $\quad$ $d(x, c_3) = 6$

$d(x, c_2) = 4$ $\quad$ $d(x, c_4) = 3$

x is the same distance from c_1 and from c_4

4. $|C| = 4$ $\quad$ $\binom{8}{0} + \binom{8}{1} + \binom{8}{2} = 1 + 8 + 28$

$|C|(1 + 8 + 28) = 148$

$256 - 148 = 108$

4 of these are code words

Non code words in balls

$= 148 - 4 = 144$