Coding Theory Homework

Week 12 (Section 3.2 - 3.4)

Exercise 3.2.5

> Show that for $n = 2^r - 1$, $\binom{n}{0} + \binom{n}{1} = 2^r$

Following $n = 2^r - 1$ we can see that n is always one less than 2^r. Meanwhile $\binom{n}{0} = 1$ and $\binom{n}{1} = n$ meaning that $\binom{n}{0} + \binom{n}{1} = 1 + n$.

$$1 + n = 2^r \equiv n = 2^r - 1$$

For example $r = 4$:

$$n = 2^4 - 1 = 15$$

$$\binom{15}{0} + \binom{15}{1} = 16 = 2^4$$

Exercise 3.2.6 (c)

> Can there exist perfect codes for these values of n and d:

> c. $n = 15, d = 5$

$t = \frac{d-1}{2} = \frac{4}{2} = 2$

$$|C| = \frac{2^{15}}{\binom{15}{0} + \binom{15}{1} + \binom{15}{2}} = \frac{23768}{1 + 15 + 105} = \frac{23768}{121} = 270.8$$

There can not exist perfect codes for the values of $n = 15$ and $d = 5$ as the hamming bound is not a power of 2.

Exercise 3.3.3

> Find a generator matrix in standard form for a Hamming code of length 15, then encode the message w = 11111100000

$$n = 15$$

$$r = \sqrt{n+1} = \sqrt{16} = 4$$

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

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

encoding w = 11111100000 using the above generator matrix gives us 111111000001100.

Exercise 3.3.4 (b, c, d)

> Construct an SDA for a Hamming code of length 7, and use it to decode the following words.

We can take the parity check matrix and generator matrix from example 3.3.1.

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

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

And with this build the SDA.

coset leader	syndrome
0000000	000
1000000	111
0100000	110
0010000	101
0001000	011
0000100	100
0000010	010
0000001	001

> b. 1111111

The syndrome of $wH = 000$ thus coset leader 0000000,
$w = w + v = 1111111$

> c. 0011010

The syndrome of $wH = 100$ thus coset leader 0000100,
$w = w + v = 0011110$

> d. 0101011

The syndrome of $wH = 110$ thus coset leader 0100000,
$w = w + v = 0001011$

Exercise 3.3.6 (H")

> Show that each of the following is a parity check matrix for a Hamming code of length 7, and that the codes are both equivalent to the one in Example 3.3.1.

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

In the book it says that:

> having a parity check matrix H whose rows consist of all nonzero vectors of length r is called a Hamming code of length $2^r - 1$.

The above parity check matrix consist of all nonzero vector of length 3 and can thus be called a Hamming code of length $2^3 - 1 = 7$

Exercise 3.3.7

> Prove that all Hamming codes of a given length are equivalent.

Exercise 3.3.8

> Is the following matrix the transpose of a parity check matrix for a Hamming code of length 15?

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

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

No because the code 0110 exists twice in the parity while the code 1000 is missing. The parity check matrix of Hamming code consists of *all* vectors in n^r.

Exercise 3.3.9

> Show that the Hamming code of length $2^r - 1$ for $r = 2$ is a trivial code.

$n = 2^2 - 1 = 3$

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

$$G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

The code of from the generator matrix would be $(000, 111)$ and is thus a trivial code.

Exercise 3.3.10 (use the message assignment of Exercise 2.6.12 not 2.6.11)

> Use the Hamming code of length 7 in Example 3.3.1 and the message assignment in Exercise 2.6.11. Decode the following message received:
>
> $1010111, 0110111, 1000010, 0010101, 1001011, 0010000, 1111100$

Words	Message
0000	A
1000	B
0100	C
0010	D
0001	E
1100	F
1010	G
1001	H
0110	I
0101	J
0011	K
1110	L
1101	M
1011	N
0111	O
1111	P

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

$$1010111 = 1 \cdot 1000111 + 0 \cdot 0100110 + 1 \cdot 0010101 + 0 \cdot 0001011 = 1010 = G$$
$$0110111 = 0 \cdot 1000111 + 1 \cdot 0100110 + 1 \cdot 0010101 + 0 \cdot 0001011 = 0110 = I$$
$$1000010 = 1 \cdot 1000111 + 0 \cdot 0100110 + 0 \cdot 0010101 + 0 \cdot 0001011 = 1000 = B$$
$$0010101 = 0 \cdot 1000111 + 0 \cdot 0100110 + 1 \cdot 0010101 + 0 \cdot 0001011 = 0010 = D$$
$$1001011 = 1 \cdot 1000111 + 0 \cdot 0100110 + 0 \cdot 0010101 + 1 \cdot 0001011 = 1001 = H$$
$$0010000 = 0 \cdot 1000111 + 0 \cdot 0100110 + 1 \cdot 0010101 + 0 \cdot 0001011 = 0010 = D$$
$$1111100 = 1 \cdot 1000111 + 1 \cdot 0100110 + 1 \cdot 0010101 + 1 \cdot 0001011 = 1111 = P$$

Exercise 3.4.3

> Find generating and parity check matrices for an extended Hamming code of length 8.

We can take the matrices from the Hamming code of length 7 from example 3.3.1

$$H^* = \left[\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

$$G^* = \left[\begin{array}{ccccccc|c} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

Exercise 3.4.4b

> Construct an SDA for an extended Hamming code of length 8, and use it to decode the following words:

Using the matrices from the previous exercise we can build the SDA:

coset leader	syndrome
00000000	0000
10000000	1111
01000000	1101
00100000	1011
00010000	0111
00001000	1001
00000100	0101
00000010	0011
00000001	0001

> b. $w = 11010110$

The syndrome of $wH = 0011$ thus coset leader 00000010,
$w = w + v = 11010100$

Exercise 3.4.5

> Show that an extended Hamming code of length 8 is a self-dual code, i.e.
> $C = C^{\perp}$