

1. Prove that the vectors 11001, 01110 and 10111 are linearly dependent over $\{0, 1\}$ but linearly independent over $\{0, 1, 2\}$.

Proof : Let $a, b, c \in \mathbb{F}$ such that

$$a(11001) + b(01110) + c(10111) = 00000$$

Then

$$\begin{cases} a + c = 0 \\ a + b = 0 \\ b + c = 0 \\ b + c = 0 \\ a + c = 0 \end{cases}$$

Suppose first that $\mathbb{F} = \{0, 1\}$. Since $a + c = 0 = a + b$, we get that $a = b = c$. Hence we see that $a = b = c = 1$ is a solution. So 11001, 01110 and 10111 are linearly dependent over $\{0, 1\}$.

Suppose next that $\mathbb{F} = \{0, 1, 2\}$. Since $a + c = 0$, we get that $c = -a$. Since $a + b = 0$, we find that $b = -a$. But $b + c = 0$. So $-a - a = 0$. Thus $-2a = 0$. Hence $a = 0$ and so $b = c = 0$. This implies that 11001, 01110 and 10111 are linearly independent over $\{0, 1, 2\}$. \square

2. Let C be the binary code with generator matrix $\begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$.

- (a) Write down all the codewords in C .
- (b) Find a generator matrix in standard form for C .
- (c) Find a parity check matrix for C .
- (d) Find all the parameters for C (so n , k and d).

Solution : (a) We need to find all the linear combinations of rows of the generator matrix. Hence there are eight codewords (abc underneath the codeword stands for $a \cdot \text{row1} + b \cdot \text{row2} + c \cdot \text{row3}$):

$$C = \{ \begin{array}{cccccc} 00000 & , & 00101 & , & 11011 & , & 10110 & , & 11110 & , & 10011 & , & 01101 & , & 01000 \\ & & 000 & & 100 & & 010 & & 001 & & 110 & & 101 & & 011 & & 111 \end{array} \}$$

(b) Either by performing elementary row operations on the given generator matrix or by selecting the correct codewords from (a), we find that

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

is a generator matrix for C in standard form.

(c) Using (b) and Proposition 3.7, we get that

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

is a parity check matrix for C .

(d) Since the generator matrix for C is a 3×5 -matrix, we have that $n = 5$ and $k = 3$. From (a), we get that $w(C) = 1$. So $d(C) = 1$. Note that we could have deduced that $d(C) = 1$ from Proposition 3.8 : the parity check matrix contains no zero-columns but contains two identical columns. \square

3. Let C be the ternary code with parity check matrix $\begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 1 \end{bmatrix}$. Find the parameters of C (so n , k and d) without writing down all the codewords in C .

Solution : In general, a parity check matrix for an $[n, k]$ -code is an $(n - k) \times n$ -matrix. Hence $n = 4$ and $k = 2$. We use Proposition 3.8 to find $d(C)$. Note that the parity check matrix contains no zero-columns. So $d(C) \geq 2$. Since no column is a multiple of another column (be careful : we are working over $\{0, 1, 2\}$), we get that any two columns in the parity check matrix are linearly independent. So $d(C) \geq 3$. But the first three columns are linearly dependent:

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} + \begin{bmatrix} 2 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Hence $d(C) = 3$. □

4. Let $r \in \mathbb{N}$. Prove that a binary $[2^r - 1, 2^r - 1 - r, 3]$ -code is perfect.

Proof : Let C be a binary $[2^r - 1, 2^r - 1 - r, 3]$ -code. Then $|C| = 2^{2^r - 1 - r}$ and C is one-error correcting. So we need to check that

$$|C| = \frac{m^n}{\sum_{i=0}^t \binom{n}{i} (m-1)^i}$$

We get that

$$\frac{m^n}{\sum_{i=0}^t \binom{n}{i} (m-1)^i} = \frac{2^n}{\binom{n}{0}(2-1)^0 + \binom{n}{1}(2-1)^1} = \frac{2^n}{1+n} = \frac{2^{2^r-1}}{1+(2^r-1)} = \frac{2^{2^r-1}}{2^r} = 2^{2^r-1-r} = |C|$$

So C is perfect. □

5. If \mathbf{x} and \mathbf{y} are binary vectors of length n , then we put $\mathbf{x} * \mathbf{y} = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$. So if $\mathbf{x} = 10111$ and $\mathbf{y} = 11001$ then $\mathbf{x} * \mathbf{y} = 10001$.

Prove that $w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} * \mathbf{y})$ for all binary vectors \mathbf{x}, \mathbf{y} of length n .

Proof : Note that

$$(\mathbf{x} + \mathbf{y})_i = 1 \iff (x_i = 1 \text{ and } y_i = 0) \text{ or } (x_i = 0 \text{ and } y_i = 1)$$

Hence

$$\begin{aligned} w(\mathbf{x} + \mathbf{y}) &= |\{1 \leq i \leq n : (x_i = 1 \text{ and } y_i = 0) \text{ or } (x_i = 0 \text{ and } y_i = 1)\}| \\ &= |\{1 \leq i \leq n : x_i = 1 \text{ and } y_i = 0\}| + |\{1 \leq i \leq n : x_i = 0 \text{ and } y_i = 1\}| \end{aligned}$$

Note that

$$w(\mathbf{x}) = |\{1 \leq i \leq n : x_i = 1\}| = |\{1 \leq i \leq n : x_i = 1 \text{ and } y_i = 0\}| + |\{1 \leq i \leq n : x_i = 1 \text{ and } y_i = 1\}|$$

Since $(\mathbf{x} * \mathbf{y})_i = 1 \iff x_i = y_i = 1$, we get that

$$|\{1 \leq i \leq n : x_i = 1 \text{ and } y_i = 0\}| = w(\mathbf{x}) - |\{1 \leq i \leq n : x_i = 1 \text{ and } y_i = 1\}| = w(\mathbf{x}) - w(\mathbf{x} * \mathbf{y})$$

Similarly, we find that

$$|\{1 \leq i \leq n : x_i = 0 \text{ and } y_i = 1\}| = w(\mathbf{y}) - w(\mathbf{x} * \mathbf{y})$$

Putting everything together, we get

$$\begin{aligned} w(\mathbf{x} + \mathbf{y}) &= |\{1 \leq i \leq n : x_i = 1 \text{ and } y_i = 0\}| + |\{1 \leq i \leq n : x_i = 0 \text{ and } y_i = 1\}| \\ &= w(\mathbf{x}) - w(\mathbf{x} * \mathbf{y}) + w(\mathbf{y}) - w(\mathbf{x} * \mathbf{y}) \\ &= w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} * \mathbf{y}) \end{aligned} \quad \square$$

6. Let $n \geq 2$ and C the binary code consisting of all words of length n containing an even number of ones (see HW 1 #5).

- (a) Prove that C is linear over $\{0, 1\}$ (Ex. 5 might be useful).
- (b) Find the parameters of C (so n , k and d).
- (c) Find a parity check matrix for C .

Proof : (a) Let $\mathbf{x}, \mathbf{y} \in C$ and $a, b \in \{0, 1\}$. We need to show that $a\mathbf{x} + b\mathbf{y} \in C$. Since $\mathbb{F} = \{0, 1\}$, we may assume that $a = b = 1$. From Ex #5, it follows that

$$w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} * \mathbf{y})$$

Since $\mathbf{x}, \mathbf{y} \in C$, we have that $w(\mathbf{x})$ and $w(\mathbf{y})$ are even. Hence $w(\mathbf{x} + \mathbf{y})$ is even. So $\mathbf{x} + \mathbf{y} \in C$. Hence C is linear.

(b) We showed in HW 1 #5 that $|C| = 2^{n-1}$ and $d(C) = 2$. If C is a binary linear code of dimension k then $|C| = 2^k$. Hence $k = n - 1$.

(c) Note that a parity check matrix for C is a $1 \times n$ -matrix. We claim that $H = [1 \ \cdots \ 1]$ does the job. So we need to show that $H\mathbf{x}^T = 0$ for all $\mathbf{x} \in C$. Let $\mathbf{x} = x_1 \dots x_n \in C$. Then we have that

$$H\mathbf{x}^T = [1 \ \cdots \ 1] \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1 + \cdots + x_n = 0$$

since \mathbf{x} contains an even number of ones. □

Remark : Another way of finding a parity check matrix for C is to find a generator matrix in standard form for C . Note that such a generator matrix G in standard form looks like $G = [I_{n-1} \ A]$ where A is an $(n - 1) \times 1$ -matrix. By Proposition 3.7, we get that $[A^T \ 1]$ is a parity check matrix for C . So we still need to find A . But every row of G is a codeword and so has an even number of ones. Hence $A = [1 \ \cdots \ 1]^T$ (so an $(n - 1) \times 1$ -matrix containing all ones). Again we find that $h = [1 \ \cdots \ 1]$ (a $1 \times n$ -matrix containing all ones).
