This is a customised assignment for ag14774.

1 Generator Matrices

Consider the set

$$\begin{aligned} S = \{ \quad & (1,0,1,0,1,0,1,0,1,1,1,0,1,1,0,1,0,0,1,0,1), \\ & (0,1,0,0,0,0,1,1,1,0,1,1,1,1,1,1,1,0,0,0,0), \\ & (0,0,0,1,0,1,1,0,1,0,0,0,1,0,0,0,0,1,0,0,0), \\ & (0,0,0,0,0,1,0,1,1,1,0,0,1,0,0,1,0,0,1,0,0), \\ & (0,0,0,0,0,0,1,0,0,0,0,1,1,0,1,1,1,0,1,0,1), \\ & (0,0,0,0,0,0,0,1,0,1,1,0,1,1,0,0,0,1,0,1,1), \\ \} & \end{aligned}$$

and the linear code $C = Span(S)$.

1. Determine a generator matrix G for C (show the SAGE code used):

2. Let $v = (1,1,0,0,0,1,0,0,0,0,0,1,1,1,0,0,0,1,1,0,0)$. Determine if v is a codeword of C using a parity-check matrix of C. Show the SAGE code used.

2 $GF(5)$ codes

1. Using SAGE, verify if the following matrix

```
G=Matrix(GF(5), 9,  [0, 0, 0, 0, 0, 0, 0, 0, 1, 1,
2, 1, 2, 3, 1, 4, 4, 1, 0, 0, 0, 0, 0, 0, 0, 0, 3,
1, 4, 4, 3, 2, 3, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1,
4, 0, 2, 1, 4, 3, 2, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1,
3, 4, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
3, 3, 2, 1, 3, 3, 2, 0, 0, 0, 0, 0, 1, 0, 0, 0, 3,
1, 1, 3, 2, 2, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4,
0, 3, 3, 1, 1, 2, 3, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1,
4, 2, 0, 4, 1, 3, 3, 0, 0, 0, 0, 1, 0, 0, 0, 0, 3,
1, 2, 1, 3, 4, 1, 4])
```

is a generator matrix for a $[17, 9]_5$ linear code containing the codeword

$$c = (3, 3, 4, 3, 4, 2, 0, 3, 2, 3, 3, 4, 3, 0, 0, 1, 1)$$

2. How many codewords are there in this code?

3. Given a parity-check matrix H, give an upper bound on the distance d.

3 Parity-check matrices

Given a linear code C with parity check matrix

```
H=matrix(GF(2),5,[1,0,0,0,0,1,0,1,1,0,1,
                  0,1,0,0,0,0,1,0,1,0,0,
                  0,0,1,0,0,0,0,1,0,0,0,
                  0,0,0,1,0,1,0,1,0,1,1,
                  0,0,0,0,1,0,0,0,0,1,1])
```

1. Give at least two generator matrices for C.

2. Using the SAGE command `hamming_weight()`, give the weight distribution of C. What is the distance of C?

3. Write a SAGE function `SystematicEncoding()` that given an $[n, k, d]_q$ linear code and a message $\vec{m} \in \mathbb{F}_q^k$ outputs a systematic encoding of $\vec{m}$.

4. Given the following correspondence between letters and elements in $\mathbb{F}_2^6$

L	H	E	O
101001	011100	110100	001011

give a systematic encoding of the message HELLO using the code from 3.1. Show your SAGE code.

4 Linear decoding

1. Write a SAGE function `DecodeLinear()` that given a linear code $[n, k, d]_q$ an a received vector $r \in \mathbb{F}_q^n$, decodes to the nearest codeword using the corresponding coset leader.

2. Given the code of the previous problem, decode the following words if possible.

$$r = (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$$
$$r_1 = (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$$
$$r_2 = (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$$

5 Binary Hamming Code

Let r be a positive integer and H be a $r \times 2^r - 1$ matrix whose columns are the distinct nonzero vectors of $\mathbb{F}_2^r$. Then the code having H as its parity-check matrix is called the Binary Hamming Code $H_2(r)$.

1. Write a SAGE function that given r, outputs a parity-check matrix for the $H_2(r)$ Hamming code.

2. Write a simple SAGE decoding function `DecHamming()` for Hamming codes.

3. Given $r = 4$ and $v = (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$, decode v using `DecHamming`.

6 More on Hamming Codes

Write down a parity-check matrix and a syndrome lookup table for the binary Hamming code $H_2(4)$.

7 Reed-Solomon

For this exercise you can use the following SAGE commands: `C.check_mat()`, `C.gen_mat()`, `LinearCode(G)`.

1. Determine a generator and parity check matrices for the Reed-Solomon code $[11, 4]$ over $GF(3^3)$ defined by the set of points

   $$\{0, \alpha, \alpha^2, \alpha+2, \alpha^2+2\alpha, 2\alpha^2+\alpha+2, \alpha^2+\alpha+1, \alpha^2+2\alpha+2, 2\alpha^2+2, \alpha+1, \alpha^2+\alpha\}$$

   where

   $$\alpha^3 + 2\alpha + 1 = 0$$

2. What is the distance of this code?

3. Decode the following vector using `DecodeLinear` (exercise 4). How many errors occurred?

   $v = (2 \cdot \alpha, \alpha^2 + 2 \cdot \alpha + 1, 2 \cdot \alpha, 2 \cdot \alpha^2 + 2 \cdot \alpha + 2, \alpha^2 + \alpha + 1, \alpha + 1, 2 \cdot \alpha^2 + 2 \cdot \alpha, \alpha^2 + 1, 2 \cdot \alpha^2 + 1, 2, \alpha^2 + 2)$

This is the end of exercise sheet 6.