Math3302 Assignment 1

Dominic Scocchera

March 2023

Q1

a)

b)

Q2

a)

We will use algorithm 4.3.1 to find a basis for the linear code $C = \langle S \rangle$.

$$
\begin{aligned}
A = &\begin{pmatrix} 2 & 1 & 0 & 2 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 1 & 0 & 1 \end{pmatrix} \\
\to &\begin{pmatrix} 2 & 1 & 0 & 2 & 1 & 2 \\ 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}, \quad R_2 = R_2 + R_3 \\
\to &\begin{pmatrix} 0 & 1 & 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}, \quad R_1 = R_1 + R_2 \\
\to &\begin{pmatrix} 0 & 1 & 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 1 \end{pmatrix}, \quad R_3 = R_3 + R_1 \\
\to &\begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 \end{pmatrix}, \quad R_1 \leftrightarrow R_2 \\
\to &\begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{pmatrix}, \quad R_3 = R_3 + R_3
\end{aligned}
$$

So a basis for C is thus $\{100211, 010120, 001112\}$ and hence the generating matrix is:

$$G_C = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{pmatrix}$$

b)

Now from a) we see that as $G_C = \begin{pmatrix} I & X \end{pmatrix}$ that C is a systematic code and hence:

$$\begin{aligned} H_C &= \begin{pmatrix} -X \\ I \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 0 \\ 2 & 2 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

c)

H_C has no rows of zeros so $\delta > 1$. H_C has no pair of identical rows so $\delta > 2$. Rows 1, 3 and 5 sum to zero so $\delta = 3$.

d)

$$\begin{pmatrix} 1 & 2 & 1 \end{pmatrix} G_c = \begin{pmatrix} 1 & 2 & 1 & 2 & 0 & 0 \end{pmatrix}$$

e)

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 2 & 2 \end{pmatrix} H_C = \begin{pmatrix} 1 & 2 & 0 \end{pmatrix}$$

So the syndrome is $\begin{pmatrix} 1 & 2 & 0 \end{pmatrix}$. From H_C we get that an SDA is as follows (note we are assuming there is at most a single error):

Coset Leader	Syndrome
000000	000
100000	122
010000	210
001000	221
000100	100
000010	010
000001	001
200000	211
020000	120
002000	112
000200	200
000020	020
000002	002

So the error is a 2 in position 2. So the most likely codeword is $011022 - 020000 = 021022$. Hence the codeword that was sent was 021.

Q3

The Griesmer bound for a linear (n, k, δ) code is:

$$n \geq \sum_{j=0}^{k-1} \left\lceil \frac{\delta}{2^j} \right\rceil$$

We also have that a Reed-Muller code is a linear $(2^m, m+1, 2^{m-1})$ code. Plugging these values into the Griesmer bound we get:

$$\begin{aligned}
\sum_{j=0}^{k-1} \left\lceil \frac{\delta}{2^j} \right\rceil &= \sum_{j=0}^{(m+1)-1} \left\lceil \frac{2^{m-1}}{2^j} \right\rceil \\
&= \sum_{j=0}^{m} \left\lceil 2^{m-j-1} \right\rceil \\
&= (2^{m-1} + 2^{m-2} + ... + 2^1 + 2^0) + \left(\left\lceil 2^{-1} \right\rceil \right) \\
&= (2^m - 1) + (1) \\
&= 2^m \\
&= n
\end{aligned}$$

So the Reed-Muller code achieves the Griesmer bound with equality.

Q4

a)

We first see that we are dealing with a binary linear (15,k,6) code. From the notes we have that the Hamming bound is:

$$k \leq 15 - \left\lceil \log_2 \left(\sum_{j=0}^{\lfloor \frac{6-1}{2} \rfloor} \binom{15}{j} \right) \right\rceil = 8$$

For the Griesmer bound we have:

$$15 \geq \sum_{j=0}^{k-1} \left\lceil \frac{6}{2^j} \right\rceil$$

We see that the RHS is an increasing function of k and the inequality only holds for $k \leq 7$ (for k=7 the RHS equals 15). The Griesmer bound is better as it rules out the existance of codes of dimension 8 unlike the Hamming bound.

b)

We know from class that a (23,12,7) code exists and that if an (n, k, δ) code exists then both an $(n-1, k-1, \delta)$ and a $(n-1, k, \delta-1)$ code exist. If we apply $(n-1, k-1, \delta)$ seven times and $(n-1, k, \delta-1)$ once to the (23,12,7) code we get a $(15, 5, 6)$ code. We also know that if a (n, k, δ) code exists then a (n, j, δ) code exists for $j \in \{1, ..., k\}$. Hence there also exists a $(15, 4, 6)$, $(15, 3, 6)$, $(15, 2, 6)$ and a $(15, 1, 6)$ code. This is what we wanted to show.

Q5

Q6

Q7

a)

b)