Math3302 Assignment 1

Dominic Scocchera

March 2023

Q1

a)

We first see that as $\left\lfloor \frac{\delta-1}{2} \right\rfloor = 2$ we have $\delta = 5$ or $\delta = 6$. Now from the table we see that a (15,7,6) code is able to produce 128 message words which is the minimum for producing at least 120 message words for a (n,k,6) code. Using the result from the table $A_2(n-1, 2e-1) = A_2(n, 2e)$ we get that a $(14, 7, 5)$ code exists. 14 is the minimum n that satisfies what we need. We can't decrease it further as decreasing by 1 we get, $64 = A_2(14, 6) = A_2(13, 5)$.

b)

As our (14,7,6) code is a 2-error correcting code we transmit over a binary symmetric channel of reliability p = 0.9995, for each codeword we can correct 0,1 or 2 errors, thus giving:

$$Q(c) = p^{14} + \binom{14}{1} p^{14-1}(1-p) + \binom{14}{2} p^{14-2}(1-p)^2 = 0.999999954687$$

This is the same for each codeword so:

$$Q_C = 0.999999954687$$

$$F_C = 1 - Q_C = 4.5312686603 \times 10^{-8} < 4.531 \times 10^{-8}$$

Which is what we wanted to show.

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 $G_C = (I \quad X)$ 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

We want to show that for each integer $s \geq 4$, there exists a linear binary code of length 2s+1, dimension 2s and distance 8.

Proof. We begin by showing that the GV bound gives the existance for s=5.

$$\binom{64-1}{0} + ... + \binom{64-1}{8-2} = 75611761 < 4294967296 = 2^{64-32}$$

We get existance of $s = 4$ via application of the theorem that states if there exists a linear (n, k, δ)-code, then there exists a linear $(n-1, k-1, \delta)$-code 16 times. We will now proceed by induction with our base case being the construction of $s = 6$. We will make use of the theorem that states that if we let C_1 be a linear (n, k_1, δ_1)-code and let C_2 be a linear (n, k_2, δ_2)-code. Then there exists a linear $(2n, k_1 + k_2, d)$-code where $d = \min\{2\delta_1, \delta_2\}$. For our base case we let $C_1 = C_2 = (64, 32, 8)$, which is exactly the s=5 code and by the above theorem we get that there exists a $(2 \cdot 64, 32 + 32, \min\{2 \cdot 8, 8\}) = (128, 64, 8)$. Now we assume that it holds for m and show that it also holds for $m + 1$. By our inductive hypothesis we have that the $(2^{m+1}, 2^m, 8)$ code exists and we want to show $(2^{m+2}, 2^{m+1}, 8)$ code exists. Taking $C_1 = C_2 = (2^{m+1}, 2^m, 8)$, by the above theorem we get that $(2 \cdot 2^{m+1}, 2^m + 2^m, \min\{2 \cdot 8, 8\}) = (2^{m+2}, 2^{m+1}, 8)$ code exists. Hence by the principle of mathematical induction we have shown that there always exists codes of the form $(2^{s+1}, 2^s, 8)$ for all $s \geq 4$. $\square$

Q6

Our word is w = 10010101100111100010000. We have $\|w\| = 10$, we require $\|w*\|$ to be odd, so $w*$ = 100101011001111000100001. We now calculate the syndrome, $s = w * H = w * \begin{pmatrix} I_{12} \\ B \end{pmatrix}$ = 011010010001. Now computing the sum of s and b_j (each row of B) we get:

$s + b_j$	$\|s + b_j\|$
101101010100100000000000	7
110100011010110000000000	8
000110000110111000000000	7
100010111100111100000000	10
101011001010111110000000	11
111000100110111111000000	12
011111111110111111100000	17
010001001100111111110000	12
001100101000111111111000	13
110111100000111111111100	16
000001110010111111111110	15
100101101111111111111111	20

None of these are less than 2 so we continue. Now we comput the second syndrome, $s' = sB = 110111100100$. We have $\|s'\| = 7 > 3$ so we continue. Now computing the sum of s' and b_1 we get $s' + b_1 = 000000100001$, and as $\|s' + b_1\| = 2$ we have $e = (\theta_1 | s' + b_1) = 100000000000000000100001$. Finally decoding we get $c* = w * +e = 000101011001111000000000$. Now we remove the last bit to get that our codeword is $c = 00010101100111100000000$.

Q7

a)

We have that our recieved word is $w = 101101000010111$, $g(x) = 1 + x + x^2 + x^3 + x^6$. This generates a 3 cyclic burst error correcting linear code. We assume that a cyclic burst error pattern of burst length at most 3 has occured. From example 7.6.3 we know:

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

We now calculate the syndrome, $s = wH = 110011$. This corresponds to the polynomial $x^5 + x^4 + x + 1$ Now we calculate the shifted syndromes until burst length is ≤ 3.

$s_i = x^i \cdot s \mod g(x)$	burst length
$1 + x^3 + x^5$	6
$1 + x^2 + x^3 + x^4$	5
$x(1 + x^2 + x^3 + x^4)$	5
$1 + x + x^3 + x^4 + x^5$	6
$1 + x^3 + x^4 + x^5$	6
$1 + x^2 + x^3 + x^4 + x^5$	6
$1 + x^2 + x^4 + x^5$	6
$1 + x^2 + x^5$	6
$1 + x^2$	3

s_9 is the only shifted syndrome with burst length ≤ 3 so:

$$\begin{aligned} e(x) &\equiv x^{9-9}s_9(x) \mod 1+x^{15} \\ &= 1+x^2 \mod 1+x^{15} \\ &= 101000000000000 \end{aligned}$$

So now we get our codeword is:

$$c = w + e = 000101000010111$$

b)

Given a word $w(x)$ we encode it by performing the operation $g(x)w(x) = c(x)$. So from a) we get:

$$\begin{aligned} g(x)w(x) &= c(x) \\ \iff (1+x+x^2+x^3+x^6)w(x) &= x^3+x^5+x^10+x^12+x^13+x^14 \\ \iff w(x) &= \frac{x^3+x^5+x^10+x^12+x^13+x^14}{1+x+x^2+x^3+x^6} \\ \iff w(x) &= x^3+x^4+x^5+x^6+x^7+x^8 \\ &= 000111111000000 \end{aligned}$$