SOLUTIONS FOR EXAM IN SIF5032, KODETEORI, MAY 2003

Problem 1

(a) The code C has generator matrix

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

and the cosets are as follows:

$$C = \{000000, 100110, 010111, 001010, 110001, 101100, 011101, 111011\}$$
$$C{+}000001 = \{000001, 100111, 010110, 001011, 110000, 101101, 011100, 111010\}$$
$$C{+}000010 = \{000010, 100100, 010101, 001000, 110011, 101110, 011111, 111001\}$$
$$C{+}000100 = \{000100, 100010, 010011, 001110, 110101, 101000, 011001, 111111\}$$
$$C{+}010000 = \{010000, 110110, 000111, 011010, 100001, 111100, 001101, 101011\}$$
$$C{+}100000 = \{100000, 000110, 110111, 101010, 010001, 001100, 111101, 011011\}$$
$$C{+}000011 = \{000011, 100101, 010100, 001001, 110010, 101111, 011110, 111000\}$$
$$C{+}000101 = \{000101, 100011, 010010, 001111, 110100, 101001, 011000, 111110\}$$

(b) The coset leader in a coset is the unique element with smallest weight (if it exists). We get the following SDA.

Coset leader u	Syndrome uH
000000	000
000001	001
–	010
000100	100
–	011
100000	110
–	101
010000	111

For the received word $w_1 = 011100$ the syndrome is $w_1H = 001$. The coset leader for that syndrome is 000001. The most likely codeword sent is therefore $c_1 = 011100{+}000001 = 011101$.

For the received word $w_2 = 111100$ the syndrome is $w_2H = 111$. The coset leader for that syndrome is 010000. The most likely codeword sent is therefore $c_2 = 111100+010000 = 101100$.

Problem 2

Hamming bound: If C is a (binary) code of length n and distance $d = 2t + 1$ or $d = 2t + 2$ then

$$|C| \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}}.$$

In our case we get

$$|C| \leq \frac{2^{12}}{\binom{12}{0} + \binom{12}{1}} \approx 315.08$$

Since $|C| = 2^k$ (a power of 2), and

$$2^8 = 256 < 315.08 < 512 = 2^9,$$

the bound we get from the Hamming bound is $k \leq 8$.

Gilbert-Varshamov bound: There exists a linear code of length n, dimension k and distance d if

$$2^k < \frac{2^n}{\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2}}.$$

In our case we have

$$\frac{2^n}{\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2}} = \frac{2^{12}}{\binom{11}{0} + \binom{11}{1} + \binom{11}{2}} \approx 61.13$$

The largest value of k for which the Gilbert-Varshamov bound says there exists a $(12, k, 4)$ code is 5 since

$$2^5 = 32 < 61.13 < 64 = 2^6.$$

Problem 3

(a) The polynomial corresponding to the word 0101100 is $v(x) = x + x^3 + x^4$, and this is a generator for the code. To find the generator polynomial $g(x)$ (non-zero codeword of smallest degree), we can use Corollary 4.2.18 in the book which says that $g(x) = \gcd(v(x), 1 + x^n)$, where n is the word length.

In our case we have $g(x) = \gcd(x+x^3+x^4, 1+x^7)$. This can be computed for instance using the Euclidean Algorithm:

$$1 + x^7 = (x + x^2 + x^3)(x + x^3 + x^4) + (1 + x^2 + x^3)$$
$$(x + x^3 + x^4) = x(1 + x^2 + x^3)$$

So the genrator polynomial is

$$g(x) = \gcd(x + x^3 + x^4, 1 + x^7) = 1 + x^2 + x^3.$$

A generator matrix for C is for instance

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

(b) Theorem 4.5.2 in the book says that if C is a linear cyclic code of length n and dimension k with generator polynomial $g(x)$, and if $1 + x^n = g(x)h(x)$, then $C^\perp$ is a cyclic code of dimension $n - k$ with generator polynomial $g^\perp(x) = x^k h(x^{-1})$.

Here we have

$$h(x) = (1 + x^7)/g(x) = (1 + x^7)/(1 + x^2 + x^3) = 1 + x^2 + x^3 + x^4$$

and

$$g^\perp(x) = x^4 h(x^{-1}) = 1 + x + x^2 + x^4.$$

To find the distances of C and $C^\perp$, one can for instance have a look at their parity check matrices.

Since

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

(Here $\sim$ denotes row equivalence.), we have the following parity check matrix for C.

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

This can be recognised as a parity check matrix of a Hamming code. In any case it is easy to argue that the distance of the code is 3, since any set of 2 rows are linearly independent (they are different!), while there are sets of 3 rows which are linearly dependent.

To get a parity check matrix for $C^\perp$, we can take the transpose of a generator matrix for C.

We can for instance get the following matrix.

$$H_{C^\perp} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Here one sees that any set of 3 rows are linearly independent. One way to argue is to show that the sum of any two rows always has even weight, while the rows themselves have odd weight. This makes it impossible for 3 rows to sum to 0000. (Also 2 rows cannot sum to 0000 since the rows are different.) Since there are codewords of weight 4, the distance must be 4.

The conclusion is $d(C) = 3 < 4 = d(C^\perp)$.

Problem 4

The following table is useful for computations in $GF(2^3)$.

word	power of β
000	0
100	1
010	β
001	β^2
110	β^3
011	β^4
111	β^5
101	β^6

(a) Since the distance of C is $\delta = 5$, the code can correct $t = \lfloor \frac{5-1}{2} \rfloor = 2$ errors.

The word we are asked to decode is $w = (1, 0, 1, 0, 0, 0, \beta)$. The corresponding polynomial is $w(x) = 1 + x^2 + \beta x^6$. We use the decoding algorithm for Reed-Solomon codes (Algorithm 6.3.2 in the book).

Step 1. Calculate the syndromes.

$$s_1 = w(\beta) = 1 + \beta^2 + 1 = \beta^2$$
$$s_2 = w(\beta^2) = 1 + \beta^4 + \beta^6 = \beta$$
$$s_3 = w(\beta^3) = 1 + \beta^6 + \beta^5 = \beta^3$$
$$s_4 = w(\beta^4) = 1 + \beta + \beta^4 = \beta^6$$

Step 2. Find the rank of M'.

$$M' = \begin{bmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{bmatrix} = \begin{bmatrix} \beta^2 & \beta & \beta^3 \\ \beta & \beta^3 & \beta^6 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \beta^6 \\ 0 & 1 & \beta^6 \end{bmatrix}$$

We get $\text{rank}(M') = 2$. This is the number of errors (but see Step 6).

Step 3. Solve the linear system

$$\begin{bmatrix} s_1 & s_2 \\ s_2 & s_3 \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} s_2 \\ s_3 \end{bmatrix}$$

This gives the coefficients in the error locator polynomial. From the row reduction in Step 2 we see that $\sigma_0 = \beta^6$ and $\sigma_1 = \beta^6$.
Therefore the error locator polynomial is

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + x^2 = \beta^6 + \beta^6 x + x^2.$$

Step 4. Solve $\sigma_A(x) = 0$. This will give the error location numbers. For solving quadratic equations the following table is useful.

α	$\alpha + 1$	$\alpha(\alpha + 1)$
0	1	0
β	β^3	β^4
β^2	β^6	β
β^4	β^5	β^2

The equation is

$$x^2 + \beta^6 x + \beta^6 = 0.$$

We make a subtitution of variables

$$x = \beta^6 y.$$

The equation becomes

$$\begin{aligned}\beta^5 y^2 + \beta^5 y + \beta^6 &= 0\\ y^2 + y + \beta &= 0\\ y(y+1) &= \beta\end{aligned}$$

From the table we see that the two solutions are $y = \beta^2$ and $y = \beta^6$. The corresponding values for x are $x = \beta$ and $x = \beta^5$. Therefore we have error location numbers $a_1 = \beta$ and $a_2 = \beta^5$.

Step 5. Solve the system

$$\begin{bmatrix} a_1 & a_2 \\ {a_1}^2 & {a_2}^2 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$$

This will give the error magnitudes.

$$\begin{bmatrix} \beta & \beta^5 \\ \beta^2 & \beta^3 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} \beta^2 \\ \beta \end{bmatrix}$$

$$\begin{bmatrix} \beta & \beta^5 & \beta^2 \\ \beta^2 & \beta^3 & \beta \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \beta^3 \\ 0 & 1 & \beta^3 \end{bmatrix}$$

We see that the error magnitudes are $b_1 = \beta^3$ and $b_2 = \beta^3$. So the most likely error pattern is $e = (0, \beta^3, 0, 0, 0, \beta^3, 0)$ and the most likely codeword sent is $c = (1, \beta^3, 1, 0, 0, \beta^3, \beta)$.

(Step 6.) Check if the answer is a codeword.

This step is not part of the algorithm in the book, but it is a good idea to add this. The reason is that sometimes the algoritm goes through, even if the distance from the received word to the nearest codeword is larger than the number of errors we are able to correct. In this case the answer we get in the end will not be a codeword.

One way to check whether c is a codeword is to see if $c(x)$ is divible by $g(x)$. (Alternatively one can look at the syndromes for $c(x)$.) Here we have

$$\begin{aligned}c(x) &= 1 + \beta^3 x + x^2 + \beta^3 x^5 + \beta x^6\\ &= (\beta^3 + \beta x + x^2 + \beta^3 x^3 + x^4)(\beta^4 + \beta^6 x + \beta x^2)\\ &= g(x)(\beta^4 + \beta^6 x + \beta x^2),\end{aligned}$$

so c is a codeword.

(b) If w is a word with ϵ erasures and e errors which are not erasures, then w can be decoded correctly if $2e + \epsilon \leq \delta + 1$.

In our case $\epsilon = 1$, so the code can correct

$$e = \lfloor \frac{\delta - 1 - \epsilon}{2} \rfloor = \lfloor \frac{5 - 1 - 2}{2} \rfloor = 1$$

additional error.

The recieved word is $w = (1, *, *, 1, 0, 0, 0)$

To find the additional error we use the algorithm for decoding with erasures in Reed-Solomon codes.

The erasure locator polynomial for the word w is $\sigma_B = (\beta + x)(\beta^2 + x) = \beta^3 + \beta^4 x + x^2 = B_0 + B_1 x + x^2$. So $B_0 = \beta^3$ and $B_1 = \beta^4$.

We make the polynomial $w(x) = 1 + x^3$.

Step 1. Calculate the syndromes.

$$\begin{aligned} s_1 &= w(\beta) = 1 + \beta^3 = \beta \\ s_2 &= w(\beta^2) = 1 + \beta^6 = \beta^2 \\ s_3 &= w(\beta^3) = 1 + \beta^2 = \beta^6 \\ s_4 &= w(\beta^4) = 1 + \beta^5 = \beta^4 \end{aligned}$$

Step 1*. Calculate the modified syndromes.

$$\begin{aligned} s_1^* &= B_0 s_1 + B_1 s_2 + s_3 = \beta^4 + \beta^6 + \beta^6 = \beta^4 \\ s_2^* &= B_0 s_2 + B_1 s_3 + s_4 = \beta^5 + \beta^3 + \beta^4 = \beta \end{aligned}$$

Step 2. Find the rank of M'.

$$M' = \begin{bmatrix} s_1^* & s_2^* \end{bmatrix} = \begin{bmatrix} \beta^4 & \beta \end{bmatrix}$$

We have $\text{rank}(M') = 1$.

Step 3. Solve

$$\begin{bmatrix} s_1^* \end{bmatrix} \begin{bmatrix} A_0 \end{bmatrix} = \begin{bmatrix} s_2^* \end{bmatrix}$$

$$\beta^4 A_0 = \beta$$

The solution is $A_0 = \beta^4$.

Therefore $\sigma_{A-B}(x) = A_0 + x = \beta^4 + x$.

(The error locator polynomial is $\sigma_A(x) = \sigma_B(x)\sigma_{A-B}(x)$.)

Step 4. Solve $\sigma_{A-B} = 0$. This will give the location numbers of the errors which are not erasures.

The equation $\sigma_{A-B}(x) = \beta^4 + x = 0$ has one solution $a_3 = \beta^4$.

We conclude that the error which is not an erasure is in located in position 4 (we start counting with 0).

(The error magnitudes can be found by finishing the algorithm, but this was not part of the question.)

Problem 5

Suppose u and v are two words in $C_1 \cap C_2$. Then $u, v \in C_1$, so $u+v \in C_1$ since C_1 is linear. Similarly $u+v \in C_2$. Therefore $u+v \in C_1 \cap C_2$. We conclude that $C_1 \cap C_2$ is a linear code. (One does not need to check closure under scalar multiplication for binary codes.)

Suppose v is a word in $C_1 \cap C_2$. Let $\pi(v)$ denote the cyclic shift of v. Since $v \in C_1$ and C_1 is cyclic, we have $\pi(v) \in C_1$. Similarly $\pi(v) \in C_2$. So $\pi(v) \in C_1 \cap C_2$. We conclude that $C_1 \cap C_2$ is a cyclic code, since it is closed under cyclic shift.

We decompose the generator polynomials for C_1 and C_2 into irreducible factors.

$$g_1(x) = 1 + x^3 = (1+x)(1+x+x^2)$$
$$g_2(x) = 1 + x + x^2 + x^4 = (1+x)(1+x^2+x^3)$$

A polynomial $v(x)$ is in $C_1 \cap C_2$ if and only if $v(x)$ is a multiple of both $g_1(x)$ and $g_2(x)$. Among such common multiples, the nonzero one with smallest degree is the generator polynomial of $C_1 \cap C_2$. (In other words the generator polynomial is the least common multiple of $g_1(x)$ and $g_2(x)$.) The polynomial of smallest degree having both g_1 and g_2 as factors is

$$(1+x)(1+x+x^2)(1+x^2+x^3) = 1 + x^2 + x^5 + x^6.$$

Therefore this polynomial is the generator polynomial of $C_1 \cap C_2$.