TMA4185 Coding Theory - Exam 2012 Sample Solutions

**Problem 1.** The first recurrence is $c_1(i) = m_i + m_{i-4}$ and the corresponding polynomial is $g_1(x) = 1 + x^4$. The second one is $c_2(i) = m_i + m_{i-1} + m_{i-2} + m_{i-3}$ with $g_2(x) = 1 + x + x^2 + x^3$. Hence a generating matrix is $G_1 = \begin{bmatrix} 1 + x^4 & 1 + x + x^2 + x^3 \end{bmatrix}$.

For encoding $m = 0101010111$, it is easier to either (i) multiply $m(x) = x + x^3 + x^5 + x^7 + x^8 + x^9$ by $G_1$ to obtain $c(x) = m(x)G_1 = \begin{bmatrix} x + x^3 + x^8 + x^{11} + x^{12} + x^{13} & x + x^2 + x^8 + x^9 + x^{10} + x^{12} \end{bmatrix}$ giving $c_1 = 01010000100111$ and $c_2 = 0110000011101$, or (ii) construct an input-state-output diagram:

| $i$ | input | state | $c_1$ | $c_2$ |
|---|---|---|---|---|
| 0 | – | 0000 | – | – |
| 1 | 0 | 0000 | 0 | 0 |
| 2 | 1 | 0000 | 1 | 1 |
| 3 | 0 | 1000 | 0 | 1 |
| 4 | 1 | 0100 | 1 | 0 |
| 5 | 0 | 1010 | 0 | 0 |
| 6 | 1 | 0101 | 0 | 0 |
| 7 | 0 | 1010 | 0 | 0 |

| $i$ | input | state | $c_1$ | $c_2$ |
|---|---|---|---|---|
| 8 | 1 | 0101 | 0 | 0 |
| 9 | 1 | 1010 | 1 | 1 |
| 10 | 1 | 1101 | 0 | 1 |
| 11 | 0 | 1110 | 0 | 1 |
| 12 | 0 | 0111 | 1 | 0 |
| 13 | 0 | 0011 | 1 | 1 |
| 14 | 0 | 0001 | 1 | 0 |
| 15 | – | 0000 | – | – |

In both cases, the interleaved output is $c = 00\ 11\ 01\ 10\ 00\ 00\ 00\ 00\ 11\ 01\ 01\ 10\ 11\ 10$. □

**Problem 2. a)** Since $\gcd(3, 8) = 1$, every distinct 3-cyclotomic coset modulo 8 corresponds to a distinct irreducible factor of $x^8 - 1$. These cosets are $C_0 = \{0\}$, $C_1 = \{1, 3\} = C_3$, $C_2 = \{2, 6\} = C_6$, $C_4 = \{4\}$, $C_5 = \{5, 7\} = C_7$. Hence there are 5 irreducible factors of $x^8 - 1$ and each of the $\sum_{k=0}^{5} \binom{5}{k} = 2^5 = 32$ possible combinations of these gives the generating polynomial of a cyclic code of the required type.

**b)** $243 = 3^5$, so we are looking for a code of dimension 5. The dimension is the length minus the degree of the generating polynomial, so we want a polynomial of degree $8 - 5 = 3$. Each element in the defining set, which is a union of cyclotomic cosets, contributes one to this degree. Hence we want a set of 3 elements, e.g. $C_0 \cup C_1 = \{0, 1, 3\}$.

**c)** A BCH code of designed distance 5 has 4 consecutive elements modulo 8 in its defining set. One choice for such a defining set is $T = C_0 \cup C_1 \cup C_2 = \{0, 1, 2, 3, 6\}$. The generating polynomial of the code is the product of the minimal polynomials corresponding to the three cosets used. To find these, we need a primitive 8th root of unity, i.e. a primitive element of $\mathbb{F}_{3^2} = \mathbb{F}_9 = \mathbb{F}_3[x]/\langle x^2 + x + 2 \rangle$ ($\mathrm{ord}_8(3) = 2$ and we are given the irreducible polynomial). We can pick $\alpha$ satisfying $\alpha^2 + \alpha + 2 = 0$ as the required primitive element, since (calculations omitted)

$$\mathbb{F}_9 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\} = \{0, 1, \alpha, 2\alpha + 1, 2\alpha + 2, 2, 2\alpha, \alpha + 2, \alpha + 1\} \ .$$

Then, the required minimal polynomials are $M_{\alpha^0}(x) = M_1(x) = x - 1 = x + 2$,
$M_\alpha(x) = (x - \alpha)(x - \alpha^3) = x^2 - (\alpha^3 + \alpha)x + \alpha^4 = x^2 + x + 2$ and

$M_{\alpha^2}(x) = (x-\alpha^2)(x-\alpha^6) = x^2 - (\alpha^6+\alpha^2)x + \alpha^8 = x^2+1$.
Hence the required generating polynomial is their product i.e. $x^5+2x^3+x^2+x+1$. □

**Problem 3. a)** A parity check matrix is $H_2 = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{bmatrix}$. By Gaussian elimination, this reduces to $G_2$ (e.g. first $r_2 \leftarrow r_1 - r_2$ and then $r_1 \leftarrow 2r_1 - r_2$). Hence the code is self dual.

To see that the minimum distance $d(\mathcal{C}_2) = 3$, we either (i) notice that the 1st, 3rd and 4th columns of $H_2$ are dependent and all columns are distinct, or (ii) we compute all of the $3^2 = 9$ codewords of

$$\mathcal{C}_2 = \{0000, 1011, 2022, 0112, 0221, 1120, 1202, 2101, 2210\}$$

and by direct inspection see that all codewords have weight 3.

**b)** Since the syndrome of the received vector was non-zero, there was an error. The code is single error correcting (as it has distance 3) and possible error vectors are coset leaders, i.e. vectors of weight one (by nearest neighbor decoding). So we are looking for the (weight 1) coset leader $w$ for which $H_2 \cdot w^T = [1,\ 2]^T$. This means that by finding the column of $H_2$ that the syndrome $[1,\ 2]^T$ is a multiple of, we can find the required coset leader $w$, which in this case turns out to be $[0\ 2\ 0\ 0]$. The error-vector is unique since each coset leader is unique (there are $3^{4-2} = 9$ cosets and $\binom{4}{0} + \binom{4}{1} \cdot 2 = 9$ coset leaders).

**c)** Either by (i) the sphere packing bound ($A_3(4,3) \leq \frac{3^4}{1 \cdot 1 + 4 \cdot 2} = 3^2$), or (ii) the Singleton bound ($A_3(4,3) \leq 3^{4-3+1} = 3^2$), we deduce that $A_3(4,3) = |\mathcal{C}_2| = 3^2$ (the code is both perfect and MDS).

**d)** One way is to first puncture the code in any of the 4 positions which will result in a code of length 3 and distance $d = 2$. Extending this by appending a parity check column to its generating matrix we get a code of length 4 with distance either 2 or 3 (have to show the details). □

**Problem 3.** The code is non-linear as when taking the sum of two codewords, the first nine digits are added modulo 10 whereas the last digits modulo 11. For example, $c_1 = (5000000005)$ is a valid codeword (as $5 + 10 \cdot 5 \equiv 0 \mod 11$) but $2c_1 = (000000000X)$ is not (as $10 \cdot 10 \equiv 1 \mod 11$).

A single error in position $i$ (i.e. typing $c_i'$ instead of $c_i$) is detected since it will cause the condition to fail: going undetected means $ic_i \equiv ic_i' \mod 11$ implying $i(c_i - c_i') \equiv 0 \mod 11$, which is impossible as there are no zero divisors in $\mathbb{F}_{11}$. (However, Random double errors might not be detected.)

Now suppose that in the received number $(a_1 \ldots a_{10})$ a transposition of distinct adjacent digits occurs, say of $c_i$ and $c_{i+1}$. The error is detected since trying to check the condition will give us

$$\sum_{i=1}^{10} ia_i \equiv -ic_i - (i+1)c_{i+1} + ic_{i+1} + (i+1)c_i \equiv c_i - c_{i+1} \not\equiv 0 \mod 11\ .$$

(In fact this holds also for transpositions of distinct non-adjacent digits, say $c_i$ and $c_j$. In this case,

$$\sum_{i=1}^{10} ia_i \equiv (j-i)(c_i - c_j) \not\equiv 0 \mod 11\ ,$$

again since in $\mathbb{F}_{11}$ there are no zero divisors.) □