TMA4185 Coding Theory – answers

Problem 1 (This is clearly about *binary codes*.)

a. Add the third row to the fourth row, add the fourth row from the first row, then add the first row to the third row. We get

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

The code has dimension 4 and the encoding of $(1, 1, 1, 0)$ using G' is

$$(1, 1, 1, 0, 0, 0, 0, 1).$$

b. The transpose of one parity check matrix is

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

At this point, we could notice that this is the extended $(8, 4, 4)$ Hamming code. Alternatively: From the code word we computed above, we know that the minimum distance is at most 4. Since no rows in H are equal, we know the minimum distance is at least three. By inspection, we see that among the first three rows, no choice of three sums to zero, and no choice of two sums to a vector with Hamming weight 1. Hence, no choice of three rows sums to zero, and the minimum distance must be 4.

c. We compute the syndrome

$$yH = (0, 1, 1, 1)$$

which is the first row of H, therefore the error vector is $(1, 0, 0, 0, 0, 0, 0, 0)$ and the message is $(0, 1, 0, 1)$ (easy since the generating matrix is systematic).

Problem 2

a. The cyclic codes of length 15 over $\mathbb{F}_2$ correspond to the divisors of $x^{15} + 1 \in \mathbb{F}_2[x]$. The irreducible factors of $x^{15} + 1$ are $x + 1$, $x^2 + x + 1$, $x^4 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$, and the $2^5 = 32$ products of these factors are the divisors of $x^{15} + 1$.

b. The dimension of the code is 7. We see that $g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$ and has among its zeros α, α^2, α^3 and α^4, from which minimum distance at least 5 follows. Because the generating polynomial has weight 5, the minimum distance is 5. The code's dual is generated by the reciprocal of $(x^{15} + 1)/g(x)$, $x^7 + x^3 + x + 1$.

c. We trace the algorithm's execution using the following table:

N	Δ	$C(D)$	L	m	$B(D)$
–	1	1	0	−1	1
0	$\alpha^3 + \alpha^2$	$1 + (\alpha^3 + \alpha^2)D$	1	0	1
1	0				
2	$\alpha^3 + \alpha^2 + \alpha$	$1 + (\alpha^3 + \alpha^2)D + (\alpha^2 + \alpha)D^2$	2	2	1
3	0				

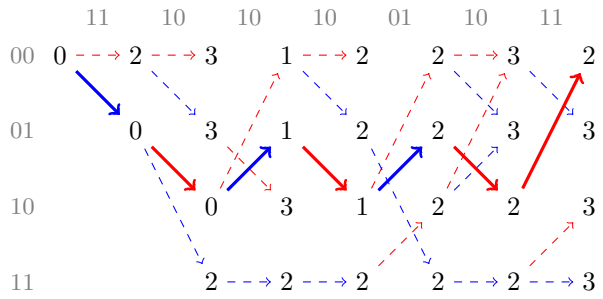
d. We compute the syndromes as $\alpha^3 + \alpha^2$, $\alpha^3 + \alpha^2 + \alpha + 1$, $\alpha^2 + \alpha$, and $\alpha^3 + \alpha$. From the previous task, we know that the error locator polynomial is $C(D) = 1 + (\alpha^3 + \alpha^2)D + (\alpha^2 + \alpha)D^2$. Rather extensive computations show that the two zeros of $C(D)$ are α^{12} and α^{13}, hence the error locations are 2 and 3, and the error vector is $e(x) = x^3 + x^2$.

We divide $y(x) + e(x)$ by $g(x)$ to get $m(x) = x^4 + x^2 + 1$.

Problem 3

a. $1 + D + D^2$ and $1 + D^2$ work. The encoding is 00 11 01 01 11.

b. The Trellis diagram below encodes 0 as red arrows and 1 as blue arrows.



Tracing back from the end state with the least errors, we get the message 10 10 10 0.