Exercise Sheet 11

(Solutions)

Exercise 11.1.

1. We have $\deg G(z) = 2 =: t$, so the minimum distance of the code is at least $2 \cdot 2 + 1 = 5$ (as the code is binary and $G(z)$ has no multiple roots, we have $d \geq 2t + 1$). The dimension of the code is at least $n - mt$ where n is the length (i.e., 8) and m is the degree of extension where L is defined (i.e., 3). Thus, the dimension is at least 2.

2. The check matrix is

$$H = \begin{pmatrix} G(0)^{-1} & G(\alpha^0)^{-1} & \dots & G(\alpha^6)^{-1} \\ 0G(0)^{-1} & \alpha^0 G(\alpha^0)^{-1} & \dots & \alpha^6 G(\alpha^6)^{-1} \end{pmatrix},$$

which is, from the given field representation,

$$\begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha^1 & \alpha^1 & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix},$$

or, in binary form,

$$\left(\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right),$$

3. We can obtain a generator matrix from H, which is

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

and from that derive the list of four codewords

$$\begin{gathered} (0,0,0,0,0,0,0,0) \\ (0,0,1,1,1,1,1,1) \\ (1,1,0,0,1,0,1,1) \\ (1,1,1,1,0,1,0,0) \end{gathered}$$

Exercise 11.2.

1. The coefficient vector of $A(z)$ can be written as

$$\begin{pmatrix} A_0 \\ A_{-1} \\ \vdots \\ A_{-(n-1)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^{-1} & \dots & \alpha^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(n-1)} & \dots & \alpha^{-(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \tag{1}$$

and then the coefficient vector of the transformation $\sum_{i=0}^{n-1} A(\alpha^i)x^i$ is defined by the product

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^1 & \dots & \alpha^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(n-1)} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} A_0 \\ A_{-1} \\ \vdots \\ A_{-(n-1)} \end{pmatrix}$$

Thus in order to show that this produces $a(x)/n$, it is sufficent to verify that

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^{-1} & \dots & \alpha^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(n-1)} & \dots & \alpha^{-(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^1 & \dots & \alpha^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(n-1)} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix} = nI_n.$$

The entry at position $(i+1, j+1)$ of the prodct on the left hand side is

$$\sum_{k=0}^{n-1} \alpha^{ik}\alpha^{-jk} = \sum_{k=0}^{n-1} \alpha^{(i-j)k} = \begin{cases} n & \text{if } i-j=0, \\ 0 & \text{otherwise.} \end{cases}$$

The claim follows.

2. This is a direct corollary of the previous part.

3. In the definition of $R_a(z)$, multiply both sides by (z^n+1) and observe that $(z^n+1) = (z+1)(z+\alpha)\cdots(z+\alpha^{n-1})$.

4. The left hand side has degree n while the right hand side has degree less than n. Thus, the equivalence holds iff

$$z^n + 1 + z\prod_{j\neq i}(z+\alpha^j) = \sum_{j=0}^{n-1} \alpha^{-ij}z^j.$$

Now we multiply both sides by $z+\alpha^i$ to obtain the equation

$$\alpha^i(z^n+1) = (z+\alpha^i)\sum_{j=0}^{n-1} \alpha^{-ij}z^j.$$

But the right hand side simplifies to

$$(z+\alpha^i)\frac{1+\alpha^{-in}z^n}{1+\alpha^{-i}z} = (z+\alpha^i)\frac{\alpha^i(1+z^n)}{\alpha^i+z} = \alpha^i(1+z^n).$$

which proves the identity.

5. By part 3 we have

$$z(z^n+1)R_a(z) = \sum_{i=0}^{n-1} a_i z\prod_{j\neq i}(z+\alpha^j),$$

which, combined with part 4, gives

$$z(z^n+1)R_a(z) \equiv \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \alpha^{-ij} z^j \pmod{z^n+1},$$

but the right hand side is $A(z)$.

6. We know that $(a_0, \ldots, a_{n-1})$ is a codeword iff $R_a(z) \equiv 0 \mod G(z)$. Since $G(z)$ does not have any α^i as a root, it is relatively prime with $z^n + 1$. Thus $(a_0, \ldots, a_{n-1})$ is a codeword iff $R_a(z)(z^n + 1) \equiv 0 \mod G(z)$. Also, $1/z \equiv z^{n-1} \mod (z^n + 1)$. This combined with the previous part shows the claim.

Exercise 11.3.

1. The coefficient vector of $A(\alpha z)$ is $(\alpha^0 A_0, \alpha^1 A_{-1}, \ldots, \alpha^{n-1} A_{-(n-1)})$, and similar to (1), this is given by the transformation

$$\begin{pmatrix} A_0 \\ \alpha A_{-1} \\ \vdots \\ \alpha^{n-1} A_{-(n-1)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha & 1 & \ldots & \alpha^{-(n-2)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{n-1} & 1 & \ldots & \alpha^{-(n-2)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

But this is the same as applying the transformation in (1) on a cyclic shift of $(a_0, \ldots, a_{n-1})$, which implies that $A'(z) = A(\alpha z)$.

2. Becuase $(a_0, \ldots, a_{n-1})$ has even weight, $A_0 = \sum_{i=0}^{n-1} a_i = 0$ and thus $A(z)$ is divisible by z, and the remainder of $A(z)/z$ by $z^n + 1$ is exactly the polynomial $A(z)/z$. Now we can use the result in the last part of the previous exercise to show that $A(z)/z \equiv 0 \mod G(z)$.

3. Suppose that Γ is cyclic and $G(z)$ has a nonzero root β. Now take an nonzero even weight codeword $(a_0, \ldots, a_{n-1})$ (which must exist for any nontrivial linear code). By the previous part, $A(z)/z$ is a multiple of $G(z)$. Because $G(\beta) = 0$, we have $A(\beta) = 0$. Now applying the same argument on the cyclic shift of the codeword and using the first part we get that $A(\alpha^i \beta) = 0$ for every $i = 0, \ldots, n-1$. This means that $A(z)$ has n distinct root, which is not possible because it is nonzero and has degree less than n. Thus Γ does not have a nonzero root and we can take it as z^r for some r.