Solutions 7

Exercise 7.1. Note that $x^2 + x + 1$ is a divisor of $x^{15} - 1$. Let ω be such that $\omega^2 + \omega + 1 = 0$. Then x^2+x+1 has the root $\omega = \alpha^i$ for some primitive 15th root of unity α. Thus C is a BCH code with minimum distance $d \geq 2$ (note that ω^2 is also a root of $x^2 + x + 1$, but since ω and ω^2 are not successive powers of α, the BCH bound does not give us $d \geq 3$ but only $d \geq 2$). Moreover, $(x + 1)(x^2 + x + 1) = x^3 + 1$ is a codeword of weight 2, so that $d = 2$.

To show that C cannot be a Goppa code, we will show that it does not satisfy the lower bound on the minimum distance satisfied by Goppa codes. Suppose that C is a Goppa code with Goppa polynomial $g(z)$ of degree t and minimum distance d. If $t > 1$, then by Theorem 6.4 of the course notes, we must have $d \geq t + 1 > 2$, so that $g(z)$ must be of degree 1. But then by Theorem 6.7, we must have $d \geq 2t + 1 = 3$. Therefore C cannot be a Goppa code.

Exercise 7.2.

1. We have $\deg(g) = 2 =: t$, so the minimum distance of the code is at least $2\cdot2+1 = 5$ (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
$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$
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 7.3.

First note that we have implicitely assumed in the problem statement that n is odd. Indeed, there can be no primitive n-th root of unity in a field $\mathbb{F}_{2^m}$ for $n = 2n'$. To see this, consider the set of roots of $x^{2n'} - 1$ in $\mathbb{F}_{2^m}$. Since we are working over a field of characteristic 2, we have

$$(x^{2n'} - 1) = (x^{n'} - 1)^2$$

so that an n-th root of unity is also an n'-th root of unity and is thus not primitive (its order is less than n).

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 product on the left hand side is

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

   Thus

$$a(x) = \frac{1}{n}\sum_{i=0}^{n-1} A(\alpha^i)x^i = \sum_{i=0}^{n-1} A(\alpha^i)x^i.$$

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 7.4.

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.