Solutions 9

Exercise 9.1. First a sanity check: the dimension is k in both cases. Moreover, the minimum distance of the RS code is $q-k$, and the minimum distance of the code viewed as a BCH code is at least $q-k$ by the BCH bound.

Let $f(x) = \sum_{l=0}^{k-1} f_l x^l$ be a message. The corresponding codeword is

$$c = (f(\alpha^0), \ldots, f(\alpha^{q-2})).$$

Another way to view c is as a polynomial $c(x) = \sum_{i=0}^{q-2} f(\alpha^i)x^i$. It is enough to prove that any such codeword is a multiple of $g(x)$, i.e., that

$$c(\alpha^j) = 0, \ j = 1, \ldots, q-1-k.$$

Now

$$\begin{aligned} c(\alpha^j) &= \sum_{i=1}^{q-2} f(\alpha^i)(\alpha^j)^i \\ &= \sum_{i=0}^{q-2} \sum_{l=0}^{k-1} f_l (\alpha^i)^l (\alpha^j)^i \\ &= \sum_l f_l \sum_i (\alpha^{j+l})^i. \end{aligned}$$

Note that j ranges over $1, \ldots, q-1-k$ and l ranges over $1, \ldots, k-1$, so that $0 < j+l < q-1$ and thus $\alpha^{j+l} \neq 1$ for all values of j and l. Moreover, for fixed j and l, $(\alpha^{j+l})^{q-1} = 1$, or in other words,

$$(\alpha^{j+l} - 1) \sum_{i=0}^{q-2} (\alpha^{j+l})^i = 0.$$

But since $\alpha^{j+l} \neq 1$, we have that

$$\sum_{i=0}^{q-2} (\alpha^{j+l})^i = 0$$

and thus $c(\alpha^j) = 0$.

Exercise 9.2.

1. Let D be the dual code of $\mathrm{GRS}_{n-1}(\alpha, v)$. D has dimension 1 and thus consists of all scalar multiples of some fixed vector $v' = (v'_1, \ldots, v'_n)$. We must show that all v'_i are nonzero. Now by the dual code property, and taking a basis for $\mathrm{GRS}_{n-1}(\alpha, v)$ corresponding to the basis of polynomials $\{1, x, \ldots, x^{k-1}\}$, we know that v' satisfies

$$\begin{aligned} v_1 v'_1 + \cdots + v_n v'_n &= 0 \\ \alpha_1 v_1 v'_1 + \cdots + \alpha_n v_n v'_n &= 0 \\ &\vdots \\ \alpha_1^{n-2} v_1 v'_1 + \cdots + \alpha_n^{n-2} v_n v'_n &= 0. \end{aligned}$$

This is equivalent to saying that

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ & \vdots & & \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \dots & \alpha_n^{n-2} \end{pmatrix} \begin{pmatrix} v_1 v_1' \\ v_2 v_2' \\ \vdots \\ v_n v_n' \end{pmatrix} = 0. \quad (1)$$

If any v_i' was equal to 0, then equation (1) gives a set of simultaneous equations for the other $v_i v_i'$ whose coefficient matrix is Vandermonde. But then all $v_i v_i'$ must be 0 and hence all v_i' must be 0, which is impossible since the space generated by v' is of dimension 1. Hence D is indeed $\text{GRS}_1(\alpha, v')$.

2. A basis for $\text{GRS}_k(\alpha, v)$ is

$$\{(\alpha_1^s v_1, \alpha_2^s v_2, \dots, \alpha_n^s v_n)\}_{s \le k-1},$$

and a basis for $\text{GRS}_{n-k}(\alpha, v')$ is

$$\{(\alpha_1^t v_1', \alpha_2^t v_2', \dots, \alpha_n^t v_n')\}_{t \le n-k-1}.$$

A necessary and sufficient condition for duality is to have

$$\sum_{i=1}^{n} (\alpha_i^s v_i)(\alpha_i^t v_i') = 0$$

for all s, t as specified above. But

$$\sum_{i=1}^{n} (\alpha_i^s v_i)(\alpha_i^t v_i') = \sum_{i=1}^{n} \alpha_i^{s+t} v_i v_i' = 0$$

for $s + t \le n - 2$, by equation (1).

Thus we see that in particular, the dual of a RS code is a GRS code.

Exercise 9.3.

1. Suppose that there is a codeword c of weight less than k. Project the code to the subset of the coordinates determined by the nonzero positions of c. No two codewords can have the same projections, since otherwise, their difference will be all zeros at the nonzero positions of c and this will violate the ZDF property of the code. But this gives a contradiction as there are q^k codewords and their projection to less than k coordinates cannot be injective. Thus the minimum distance of the code is at least k.

2. As the code is MDS the distance d of the code is equal to $n - k + 1$. Morevoer we know that $d \ge k$, which means $k \le (n+1)/2$. Thus $d \ge n - (n+1)/2 + 1 = (n+1)/2 > n/2$, and the weight of all nonzero codewords is larger than half the code length. Therefore, the code is ZDF as for every pair of codewords there has to be a position where both words are nonzero.