Exercise Sheet 8

Exercise 8.1. Consider the Reed Solomon code $\mathrm{RS}(k; \mathbb{F}_q^*)$ which is the image of the map

$$\begin{array}{rcl} \mathbb{F}_q[x]_{<k} & \to & (\mathbb{F}_q^*)^{q-1}, \\ f & \mapsto & (f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{q-2})), \end{array}$$

where α is a primitive element of $\mathbb{F}_q$.

Prove that this code is the cyclic code with generator polynomial

$$g(x) = \prod_{j=1}^{q-1-k} (x - \alpha^j).$$

Thus $\mathrm{RS}(k; \mathbb{F}_q^*)$ is a BCH code of length $q-1$, dimension k and minimum distance equal to the designed distance $q-k$.

Exercise 8.2. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ where the α_i are distinct elements of $\mathbb{F}_{q^m}$, and let $v = (v_1, \ldots, v_n)$ where the v_i are nonzero but not necessarily distinct elements of $\mathbb{F}_{q^m}$. Then we define the *generalized RS code*, denoted by $\mathrm{GRS}_k(\alpha, v)$, as the code consisting of all vectors

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)),$$

where $f(x)$ range over all polynomials of degree $< k$ with coefficients from $\mathbb{F}_{q^m}$. Note that this is still an $[n, k, n-k+1]$-code.

1. Show that the dual of $\mathrm{GRS}_{n-1}(\alpha, v)$ is $\mathrm{GRS}_1(\alpha, v')$ for some v'.
2. Deduce that the dual of $\mathrm{GRS}_k(\alpha, v)$ is $\mathrm{GRS}_{n-k}(\alpha, v')$ for the same v' as above.

Exercise 8.3. A linear $[n, k]_q$-code is called "zero-divisor free", or ZDF, if for any two nonzero codewords x and y their point-wise product is nonzero.

- Show that an $[n, k]_q$-ZDF code must have minimum distance at least k.
- Show that an $[n, k]_q$ Reed-Solomon code with minimum distance at least k is ZDF.