Exercise Sheet 8

Exercise 8.1. 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.

Exercise 8.2. Let $\mathcal{C}$ be any $[n,k,d]$ code over $\mathbb{F}_q$ where $d \geq 2$. Show that there is an $[n, n-1, 2]$ GRS code $\mathcal{C}'$ over $\mathbb{F}_{q^{n-k}}$ such that $\mathcal{C} = \mathcal{C}' \cap \mathbb{F}_q^n$.

Exercise 8.3. Let $\mathcal{C}$ be a GRS (Generalized Reed-Solomon) code over $\mathbb{F}_q$ with code locators $\alpha_1, \ldots, \alpha_n$ and column multipliers $v_1, \ldots, v_n \in \mathbb{F}_q$. That is, the generator matrix of $\mathcal{C}$ can be written as

$$G_{\mathcal{C}} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \begin{pmatrix} v_1 & & & 0 \\ & v_2 & & \\ & & \ddots & \\ 0 & & & v_n \end{pmatrix}.$$

Moreover, suppose that $\mathcal{C}$ is primitive, i.e., $n = q-1$ and the α_i are all nonzero. Show that the dual of $\mathcal{C}$ is a GRS code with the same set of code locators, and column multipliers $v'_j := \alpha_j / v_j$.

Exercise 8.4. Let $\mathcal{C}$ be an $[n,k]$ GRS code over $\mathbb{F}$ defined by code locators (i.e., evaluation points) $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ and column multipliers $v_1, \ldots, v_n \in \mathbb{F}$.

1. Suppose that $a, b, c \in \mathbb{F}$ where $a, c \neq 0$. Show that $\mathcal{C}$ is identical to the $[n,k]$ GRS code over $\mathbb{F}$ defined by the code locators

   $$\alpha'_j = a\alpha_j + b, \quad j = 1, \ldots, n,$$

   and column multipliers

   $$v'_j = cv_j \quad j = 1, \ldots, n.$$

2. Show that $\mathcal{C}$ is identical to an $[n,k]$ GRS code over $\mathbb{F}$ with code locators $\alpha_1^{-1}, \ldots, \alpha_n^{-1}$ and appropriately chosen column multipliers (we have assumed that the α_i are nonzero).

3. Conclude that for every $a, b, c, d \in \mathbb{F}$ where $ad \neq bc$, $\mathcal{C}$ is identical to an $[n,k]$ GRS code over $\mathbb{F}$ with code locators

   $$\alpha'_j := \frac{a\alpha_j + b}{c\alpha_j + d}, \quad j = 1, \ldots, n,$$

   and appropriately chosen column multipliers.