Exercise Sheet 9

Exercise 9.1. Show that the dual of any $[n, k, d]$ Generalized Reed-Solomon code with a $k \times n$ generator matrix

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

is a Generalized Reed-Solomon code with the same set of code locators (i.e., $\alpha_1, \dots, \alpha_n$).

Exercise 9.2. Let $\mathcal{C}$ be a (generalized) $[n, k, d]$ Reed-Solomon code over $\mathbb{F}_q$ with parity check matrix

$$H_{\mathcal{C}} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{d-2} & \alpha_2^{d-2} & \dots & \alpha_n^{d-2} \end{pmatrix},$$

where the α_i are distinct and nonzero.

1. Suppose that a codeword $c = (c_1, \dots, c_n)$ is sent and $y = (y_1, \dots, y_n) := c + e$ is received, where $e = (e_1, \dots, e_n)$ is the error vector of weight at most $\tau := \lfloor \frac{d-1}{2} \rfloor$. Define the *syndrome vector* $S = (S_0, S_1, \dots, S_{d-2}) := yH^\top$, and show that the knowledge of S (without knowing y) is sufficient to determine e.
2. For the rest of the exercise, we develop a *syndrome decoding* algorithm to determine the error vector e from S. First, show that $S = eH^\top$.
3. Suppose that the set of error positions (where y differs from c) is $J \subseteq \{1, \dots, n\}$. Show that, for $\ell = 0, \dots, d-2$,
$$S_\ell = \sum_{j \in J} e_j \alpha_j^\ell.$$
4. Define $S(x) := \sum_{\ell=0}^{d-2} S_\ell x^\ell$, and show that
$$S(x) \equiv \sum_{j \in J} \frac{e_j}{1 - \alpha_j x} \mod x^{d-1}.$$
5. Define the *error locator polynomial* by
$$\Lambda(x) := \prod_{j \in J} (1 - \alpha_j x)$$
and also
$$\Gamma(x) := \sum_{j \in J} e_j \prod_{m \in J \setminus \{j\}} (1 - \alpha_m x)$$
(summations and products over an empty set are treated as 0 and 1, respectively). Show that $\gcd(\Lambda(x), \Gamma(x)) = 1$, and $\deg(\Gamma) < \deg(\Lambda) \le \tau$.

6. Show that $\Lambda(x)S(x) \equiv \Gamma(x) \mod x^{d-1}$.
7. Suppose that there are polynomials $\lambda(x)$ and $\gamma(x)$ that satisfy

$$\lambda(x)S(x) \equiv \gamma(x) \mod x^{d-1}$$

and degree constaints $\deg(\gamma) < \tau$ and $\deg(\lambda) \leq \tau$. Show that $\Lambda(x) \mid \lambda(x)$.

8. Conclude that any nonzero solution to

$$\begin{pmatrix} S_\tau & S_{\tau-1} & \dots & S_0 \\ S_{\tau+1} & S_\tau & \dots & S_1 \\ \vdots & \vdots & \ddots & \vdots \\ S_{d-2} & S_{d-3} & \dots & S_{d-\tau-2} \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_\tau \end{pmatrix} = 0$$

can be used to identify the error vector e.