Exercise Sheet 8

Exercise 8.1. 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 $\tau := \left\lfloor \frac{d-1}{2} \right\rfloor$. 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
$$S(x) \equiv \sum_{j \in J} \frac{e_j}{1 - \alpha_j x} \mod x^{d-1}.$$
(Hint: what is the multiplicative inverse of $1 - \alpha_j x$ modulo 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 $\deg(\Gamma) < \deg(\Lambda) \leq \tau$. Show that $\gcd(\Lambda(x), \Gamma(x)) = 1$.
(Hint: for the second part, it is enough to show that $\Lambda(x)$ and $\Gamma(x)$ have no common roots. Why?)

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 constraints $\deg(\gamma) < \tau$ and $\deg(\lambda) \leq \tau$. Show that $\Lambda(x) \mid \lambda(x)$.
(Hint: prove and use the fact that $\Lambda(x)$ has a multiplicative inverse in the ring $\mathbb{F}_q[x]/x^{d-1}$).

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.

Exercise 8.2. [Some properties of MDS codes] Let C be an $[n, k, d]_q$-code. Let G and H be a generator and a check matrix for C, respectively. Prove the following statements.

1. C is MDS if and only if every $n - k$ columns of H are linearly independent.
2. C is MDS if and only if its dual $C^\perp$ is MDS.
3. C is MDS if and only if C has a minimum weight codeword in any d coordinates.

Exercise 8.3. [Johnson Bound for MDS Codes] Consider encoding using a Reed-Solomon code of length n and dimension k. Given a received vector y, construct a bipartite graph with n left nodes L, one corresponding to each symbol of the y, and ℓ right nodes R, corresponding to ℓ codewords of the RS code that agree with at least t positions with the received y.

1. Connect with an edge $i \in L$ with $j \in R$ iff $y_i = (c_j)_i$, i.e., if the received vector agrees with codeword c_j at the ith coordinate. Show that the bipartite graph cannot have as subgraph a complete bipartite graph $\mathcal{K}_{k,2}$ (i.e., a bipartite graph with k vertices on the left and 2 vertices on the right).
2. Note that each codeword has at least t coordinates that agree with y. Remove some edges in the graph so that the right vertices have degree exactly t. Show that then $\ell t = \sum_i u_i$, where u_i is the degree of $i \in L$.
3. Calculate the average number of common neighbors C that two distinct codewords have, in terms of l, t, and the u_i.
(Hint: Let p_i denote the probability that two distinct codewords picked uniformly at random from R are both adjacent to $i \in L$. Then start by writing C in terms of the p_i).
4. Observe that we can upper bound C as $C \leq k - 1$. Show that
$$\ell \leq \frac{n(t - (k-1))}{t^2 - (k-1)n} \quad \text{provided that } t^2 > n(k-1).$$
(Hint: from the Cauchy-Schwarz inequality it holds that $\sum u_i^2 \geq (\sum u_i)^2/n$.)