Exercise Sheet 10

Exercise 10.1.

Consider the RS code defined as the image of the map

$$\begin{array}{rcl} \mathbb{F}_7[x]_{<k} & \rightarrow & \mathbb{F}_7^n \\ f(x) & \mapsto & (f(x_1), \ldots, f(x_n)), \end{array}$$

for $k = 3$, $n = 5$, and $x_i = i \in \mathbb{F}_7$.

Assume we have the guarantee that at most one error occurs during transmission. Decode the received vector $y = (5, 2, 6, 3, 5)$.

Exercise 10.2. Let $\mathcal{C} = RS(k; \gamma_0, \ldots, \gamma_{n-1})$ be a Reed-Solomon code over $\mathbb{F}_{16}$ with $n = 15$ and $k = 6$.

1. What is the minimum distance of $\mathcal{C}$? How many errors can one decode by maximum likelihood ? How many errors can one decode with the Welch–Berlekamp decoder ?
2. Let $r \in \mathbb{F}_{16}^{15}$ be a received message. Let $\mathcal{A} = \{(\gamma_0, r_0), \ldots, (\gamma_{n-1}, r_{n-1})\}$ To do list decoding, we would like to find a polynomial $p(x, y)$ of total degree δ that vanishes on $\mathcal{A}$ with multiplicity m.
   If we choose $m = 2$, how many linear equations do the coefficients of p need to satisfy ?
   What is the smallest $(1, k-1)$-degree δ that ensures that these conditions on p can always be satisfied ?
   How many errors can be corrected ?
3. Same questions with $m = 6$. (Hint : try $\delta = 53$)

Exercise 10.3. We say that a code C is (e, l)-list decodable if for any pattern of e errors, there exists a list of size l that includes the transmitted codeword, i.e., if $\forall c \in C, |\{B(c, e) \cap C\}| \leq l$, where $B(c, e)$ denotes the ball of radius e centered at c.

1. What are e and l such that any (n, M, d)-code is (e, l)-list decodable and vice-versa?
2. Recall the Johnson bound from last exercise sheet: for an $[n, k, n-k+1]$-RS code, if a vector y is received such that l codewords agree with y on at least t positions, then

   $$l \leq \frac{n(t-(k-1))}{t^2 - (k-1)n} \text{ provided that } t^2 > n(k-1).$$

   Deduce that an $[n, k, n-k+1]$-RS code is $(n - \sqrt{n(k-1)} - 1, n^2)$-list decodable.

Exercise 10.4. The purpose of this exercise is to develop an efficient algorithm for finding roots of the form $y - f(x)$, $\deg(f) < k$, of a given bivariate polynomial $Q(x, y) \in \mathbb{F}_q[x, y]$.

1. Write $Q(x, y) = A_0(y) + xA_1(y) + \cdots$. Assume that $y - f(x)$ is a factor of $Q(x, y)$ with $f(x) = f_0 + f_1 x + \cdots f_{k-1} x^{k-1}$, and suppose that $f(0) = f_0 = \beta$ in $\mathbb{F}_q$. Show that $A_0(\beta) = 0$. Hence $(y - \beta)$ is a factor of $A_0(y)$.

2. Assume now that β is a simple root of A_0. By writing

$$(y - f_0 - f_1 x - \cdots - f_{k-1}x^{k-1})(\psi_0(y) + \psi_1(y)x + \cdots) = A_0(y) + A_1(y)x + \cdots$$

show that $\psi_0(y) = A_0(y)/(y-\beta)$, and that $f_1 = -A_1(\beta)/\psi_0(\beta)$. Compute $\psi_1(y)$ from this.

3. Similarly, show the recursive formulas

$$\begin{aligned} f_i &= -\frac{A_i(\beta) + f_1\psi_{i-1}(\beta) + \cdots + f_{i-1}\psi_1(\beta)}{\psi_0(\beta)} \\ \psi_i(y) &= \frac{A_i(y) + f_i\psi_0(y) + \cdots + f_1\psi_{i-1}(y)}{y-\beta}. \end{aligned}$$

Use this to develop an algorithm for finding the factors of the form $y - f(x)$ of $Q(x, y)$.

4. Apply the algorithm you developed to the polynomial

$$\begin{aligned} Q(x,y) &= x^7 + y^3x^5 + y^3x^4 + (y^4 + y^2 + y + 1)x^3 + (y^3 + y^2 + 1)x^2 + \\ &\quad (y^2 + y)x + y^5 + y^4 + y^3 + y \end{aligned}$$

$\in \mathbb{F}_2[x, y]$ to obtain all factors of the form $y - f(x)$ of this polynomial with $\deg(f) \leq 3$.