Exercise Sheet 10

Exercise 10.1. *[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. (Hint: Let p_i denote the probability that two distinct codewords are picked uniformly at random from R and are both adjacent to $i \in L$. Then write 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 $\sum u_i^2 \geq (\sum u_i)^2/n$.)

Exercise 10.2. 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 $A_0(\beta) = 0$. Set $\psi_0(y) = A_0(y)/(y-\beta)$.

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. In general, show that if we recursively set for $i \geq 1$

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

then $Q(x, f_0 + f_1 x + \cdots + f_i x^i) \equiv 0 \bmod x^{i+1}$. 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 $\deg(f) \leq 3$.