Ilana Sivan
205634272
Honors Course
Homework 10

Question 1

Prove that Reed-Solomon codes are linear. That is to say, that $m_1, m_2 \in \mathbb{F}_q^k, a \in \mathbb{F}_q$
$RS(m_1) + RS(m_2) = RS(m_1 + m_2)$
$a * RS(m_1) = RS(a * m_1)$

A subspace $C \subseteq \mathbb{F}^n$ is a linear code of distance d **iff** every non-zero element of C has d non-zero coordinates.

Given a finite field $\mathbb{F}$ of size q, the messages are polynomials of degree $k-1$. There are exactly q^k such polynomials. Given a polynomial $f(x)$, the codeword that would correspond to it is the vector in $\mathbb{F}^q$. Linear combinations of two polynomials of degree $k-1$ will return another polynomial of degree $k-1$. The distance of the code is $d = q - k + 1$, where any non-zero polynomial of degree $k-1$ can have at most $k-1$ roots, and there are polynomials of degree $k-1$ that have $k-1$ roots. This means that the code matches the Singleton bound: $d + k = q + 1$.

We can show simply:
$RS(m_1)+RS(m_2) = (f_{m_1}(a_1), ...f_{m_1}(a_n))+(f_{m_2}(a_1), ...f_{m_2}(a_n)) = (f_{m_1}(a_1)+f_{m_2}(a_1), ..., f_{m_2}(a_n)+f_{m_2}(a_n) = (f_{m_1+m_2}(a_1), ..., f_{m_1+m_2}(a_n)) = RS(m_1 + m_2)$

$aRS(m_1) = a(f_{m_1}(a_1), ..., f_{m_1}(a_n)) = (af_{m_1}(a_1), ..., af_{m_1}(a_n)) = (f_{am_1}(a_1), ...f_{am_1}(a_n)) = RS(am_1)$

Question 2

Let $C_{RS} \subseteq \mathbb{F}_q^n$ be the code defined by the function $RS : \mathbb{F}_q^k \to \mathbb{F}_q^n$ a shown in class.

a. Prove that the minimal distance of C_{RS} is $n - k + 1$.

The minimum distance of a linear code C equals the minimum weight of a non-zero codeword in C. By the Singleton bound we learned previously in class, we know that $d \leq n - k + 1$. We know that two distinct polynomials $p_1, p_2 \in \mathbb{F}_q[x]$ of a degree which is less than k will agree in k points in $\mathbb{F}_q$, that is to say that there exist at most $k-1$ points $a \in \mathbb{F}_q$ such that $p_1(a) = p_2(a)$. We will prove that $d \geq n - k + 1$, if we have two distinct polynomials $p_1(a), p_2(a)$ as defined above, which agree on at most $k-1$ points of $\mathbb{F}_q$, and have a degree of at most $k-1$, they will agree on at least $n-k+1$ points on the set $\{a_1, ..., a_n\}$, so the distance of $n-k+1$ holds. Since C_{RS} is a linear code, we can show that the Hamming weight of any non-zero codeword is at least $n-k+1$. Let $m_0, m_1, ..., m_{k-1} \neq 0$. Then, the polynomial $p(x) = m_0, m_1, ..., m_{k-1}x^{k-1}$ is a non-zero polynomial with a degree of at most $k-1$. By the Singleton bound, the distance cannot exceed $n-k+1$, and therefore must equal $n-k+1$, since p has at most $k-1$ roots and that implies that $p(a_1), ...p(a_n)$ has at most k-1 zeros.

b. Show that two code words in C_{RS} which are a distance of $n-k+1$ from each other.

We know that in code C there always exists a code word 0. We know that that these two code words will differ in $n - (k-1) = n - k + 1$ exact coordinates. We can define this code word because for $k-1$ points that we select, the polynomial will have $k-1$ roots.

We can show this with a private case (at the recommendation of the Honors group):
Let $m_1(1,1), m_2(2,1)$ such that $\mathbb{F}_3 = \{0,1,2\}$ and $fm_1(x) = x+1, fm_2(x) = 2x+1$. Then, $RS(m_1) = (fm_1(0), fm_1(1), fm_1(2)) = (0,1,2)$, $RS(m_2) = (fm_2(0), fm_2(1), fm_2(2)) = (1,0,2)$, so $d = \triangle((0,1,2),(1,0,2)) = 3-2+1$ where 3 is n and 2 is k, for a final total of 2, and our case holds.

Question 3

Let $k = 2, n = 5, q = 5$ and $RS : \mathbb{F}_q^k \to \mathbb{F}_q^n$ as shown in class. Write the $RS(m) \in \mathbb{F}_q^n$ for:

a. $m = (3, 0)$

$RS(m) = (fm(0), fm(1), fm(2), fm(3), fm(4)) = (3, 3, 3, 3, 3)$

b. $m = (2, 1)$

$RS(m) = (0 + 2, 1 + 2, 2 + 2, 3 + 2, 4 + 2) = (2, 3, 4, 0, 1)$

c. $m = (1, 2)$

$RS(m) = (0 + 1, 2 + 1, 4 + 1, 6 + 1, 8 + 1) = (1, 3, 0, 2, 4)$

d. $m = (2, 2)$

$RS(m) = (0 + 2, 2 + 2, 4 + 2, 6 + 2, 8 + 2) = (2, 4, 1, 3, 0)$

e. $m = (4, 2)$

$RS(m) = (0 + 4, 2 + 4, 4 + 4, 6 + 4, 8 + 4) = (4, 1, 3, 0, 2)$

f. $m = (3, 4)$

$RS(m) = (0 + 3, 4 + 3, 8 + 3, 12 + 3, 16 + 3) = (3, 2, 1, 0, 4)$

g. $m = (4, 4)$

$RS(m) = (0 + 4, 4 + 4, 8 + 4, 12 + 4, 16 + 4) = (4, 3, 2, 1, 0)$