Class 4 Exercises

CS250/EE387, Winter 2025

1. Fix $\alpha_0, \alpha_1, \ldots, \alpha_r \in \mathbb{F}_q$. Fix $y_0, y_1, \ldots, y_r \in \mathbb{F}_q$. Let

$$f(X) = \sum_{i=0}^{r} y_i \frac{L_i(X)}{L_i(\alpha_i)},$$

where

$$L_i(X) = \frac{\prod_{j=0}^{r}(X - \alpha_j)}{X - \alpha_i} = \prod_{j \neq i}(X - \alpha_j).$$

(Note that L_i depends on the definition of the α_j's).

(a) Show that $f(\alpha_\ell) = y_\ell$ for all $\ell = 0, \ldots, r$. (If you haven't seen this before, this is called *Lagrange Interpolation*.)

(b) Explain what part (a) has to do with the fact (which we saw in the lecture videos/notes) that a Reed-Solomon code is MDS (Maximum Distance Separable).

(c) In the lecture videos/notes, we defined a natural encoding map for a Reed-Solomon code $RS(\vec{\alpha}, n, k)$ by

$$(f_0, \ldots, f_{k-1}) \mapsto (f(\alpha_0), \ldots, f(\alpha_{n-1}))$$

for evaluation points $\alpha_0, \ldots, \alpha_{n-1}$. Use part (a) to give a *systematic* encoding map for $RS(\vec{\alpha}, n, k)$: that is, an encoding map of the form

$$(x_0, \ldots, x_{k-1}) \mapsto (x_0, \ldots, x_{k-1}, z_k, z_{k+1}, \ldots, z_{n-1})$$

where the message symbols appear as the first k symbols of the codeword.

(If you finish this one early, jump to Question 3 and then 4, and we'll come back together before embarking on Question 2).

2. Fix $\vec{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}^n$ and $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$ so that the λ_j's are all nonzero and the α_j's are all distinct. The **generalized** Reed-Solomon code $GRS(\vec{\lambda}; \vec{\alpha}, n, k)$ of dimension k is given by

$$GRS(\vec{\lambda}; \vec{\alpha}, n, k) = \{(\lambda_1 f(\alpha_1), \lambda_2 f(\alpha_2), \ldots, \lambda_n f(\alpha_n)) \,:\, f \in \mathbb{F}[X], \deg(f) < k\}.$$

(a) What is the generator matrix for $GRS(\vec{\lambda}; \vec{\alpha}, n, k)$? Convince yourself that generalized RS codes are MDS codes.

(b) Forget about generalized RS codes for a moment. Fix distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. Show that, for any polynomial $h(X)$ with $\deg(h) < n - 1$, we have

$$\sum_{i=1}^{n} \frac{h(\alpha_i)}{L_i(\alpha_i)} = 0,$$

where

$$L_i(X) = \prod_{j \neq i}(X - \alpha_j)$$

as in the previous problem.

Hint: Write out $h(X)$ using Lagrange interpolation with all n points $\alpha_1, \alpha_2, \ldots, \alpha_n$. What is the coefficient on X^{n-1} when you write it out this way?

(c) Back to GRS codes.

i. Show that $RS(\vec{\alpha}, n, k)^\perp = GRS(\vec{\lambda}; \vec{\alpha}, n, n-k)$ for some vector $\vec{\lambda}$. What is $\vec{\lambda}$, in terms of $\vec{\alpha}$?

ii. Find a parity-check matrix for $RS(\vec{\alpha}, n, k)$, in terms of $\vec{\alpha}$?

iii. **(Bonus)** More generally, show that $GRS(\vec{\lambda}; \vec{\alpha}, n, k)^\perp = GRS(\vec{\sigma}; \vec{\alpha}, n, n-k)$ for some $\vec{\sigma}$. What is $\vec{\sigma}$, in terms of $\vec{\lambda}$ and $\vec{\alpha}$? What is the parity-check matrix of $GRS(\vec{\lambda}; \vec{\alpha}, n, k)$?

3. **(Bonus, if time)** Let $n = q - 1$ and suppose that $f : \mathbb{F}_q \to \mathbb{F}_q$ given by $f(X) = \sum_{i=0}^{n-1} f_i X^i$ and $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(X) = \sum_{i=0}^{n-1} g_i X^i$ are polynomials that both vanish on $\gamma, \gamma^2, ..., \gamma^{n-k}$, for a primitive element γ of $\mathbb{F}_q$. Prove that the polynomial $h(X)$ given by

$$h(X) = \sum_{i=0}^{n-1} f_i g_i X^i$$

vanishes on $\gamma, \gamma^2, \ldots, \gamma^{n-2k+1}$.

Hint: There is a short proof using something from the lecture videos/notes...

4. **(Extra Bonus, if even more time)**

(a) Over finite fields, we can define something called a *Hasse* derivative, as follows. Let $f \in \mathbb{F}_q[X]$ be a polynomial over $\mathbb{F}_q$. Then the k'th Hasse derivative of f is denoted $f^{(\ell)} \in \mathbb{F}_q[X]$, and is defined to satisfy the Taylor-like expansion:

$$f(X) = \sum_{\ell=0}^{\deg(f)} f^{(\ell)}(a)(X-a)^\ell \qquad \forall a \in \mathbb{F}_q.$$

(Note: you can define $f^{(\ell)}(X)$ directly by defining the ℓ'th Hasse derivative of X^r as $\binom{r}{\ell} X^{r-\ell}$ and extending linearly, but this isn't important for this problem).

Let $\alpha_1, \alpha_2, \ldots, \alpha_n \subseteq \mathbb{F}_q$ be n distinct evaluation points. Define a new code C (called a *derivative code* or *univariate multiplicity code*) as follows. Let $C \subseteq (\mathbb{F}_q^m)^n$ be defined by taking all codewords of the form

$$\left(\begin{bmatrix} f(\alpha_1) \\ f^{(1)}(\alpha_1) \\ \vdots \\ f^{(m-1)}(\alpha_1) \end{bmatrix}, \begin{bmatrix} f(\alpha_2) \\ f^{(1)}(\alpha_2) \\ \vdots \\ f^{(m-1)}(\alpha_2) \end{bmatrix}, \cdots, \begin{bmatrix} f(\alpha_n) \\ f^{(1)}(\alpha_n) \\ \vdots \\ f^{(m-1)}(\alpha_n) \end{bmatrix} \right) \in (\mathbb{F}_q^m)^n$$

for all polynomials f of degree at most $k-1$.

i. What is the rate of this code?

ii. What is the distance?
Hint: You may use the fact that a degree d polynomial has at most d roots *counting multiplicities*. For example, $g(X) = (X-1)^2$ has a root of multiplicity 2 at $X = 1$, which means that it can't have any more roots. Formally, the *multiplicity* of a root α is $\ell + 1$ for the largest ℓ so that $f(\alpha), f^{(1)}(\alpha), \ldots, f^{(\ell)}(\alpha)$ all vanish. For example, $g^{(1)}(X) = 2X - 2$, so $g(1) = g^{(1)}(1) = 0$; and $g^{(2)}(X) = 2$ which doesn't vanish at $X = 1$, so the multiplicity of the root at 1 is 2.

iii. What happens if $k > n$? Does it still make sense?

(b) Notice that we can write $f(\alpha)$ as "$f(X) \mod (X - \alpha)$". Thus, if we like, we can write an RS codeword as:

$$(f(X) \mod (X - \alpha), f(X) \mod (X - \alpha_2), \ldots, f(X) \mod (X - \alpha_n)).$$

For $f \in \mathbb{F}_q[X]$ of degree at most $k - 1$, consider the corresponding codeword

$$(f(X) \mod (X - \alpha_1)^m, f(X) \mod (X - \alpha_2)^m, \ldots, f(X) \mod (X - \alpha_n)^m).$$

Here, we can think of this as a polynomial of degree at most $m - 1$ (since we can view it as the remainder when we divide by a polynomial of degree m). Thus, we can also think about it as a vector in $\mathbb{F}_q^m$ (eg, the coefficients of that degree at most $m - 1$ polynomial).

Consider the code that we get when taking all such codewords (for all $f \in \mathbb{F}_q[X]$ of degree at most $k - 1$). This code lies in $(\mathbb{F}_q^m)^n$. Show that it is equivalent to the derivative code in the previous part (possibly up to taking a fixed linear transformation $L_i : \mathbb{F}_q^m \to \mathbb{F}_q^m$ in each coordinate i).

(c) (Super open-ended) Try to develop a theory of all codes that you can get by starting with a polynomial and modding out by a polynomial $E_i(X)$ in the i'th position. What do you think their rate and distance will be? What assumptions do you need on the polynomials that you mod out by? Can you think of any other examples that have a standalone interpretation?