Class 4 Exercises

CS250/EE387, Winter 2022

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 $f(\alpha_i) = y_i$ for all $i = 0, \ldots, r$. (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.

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.
   <u>Hint:</u> 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. 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 $\vec{\alpha}$?

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...