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.

Solution

(a) We can just plug in:

$$f(\alpha_j) = \sum_{i=1}^{r} y_i \frac{L_i(\alpha_j)}{L_i(\alpha_i)} = y_j,$$

because $L_i(\alpha_j) = 0$ if $j \neq i$.

(b) Part (a) tells us how to do polynomial interpolation: given any r pairs (α_i, y_i), we can come up with a degree-r polynomial that goes through those evaluation points. One way to define an MDS code of dimension k is that any k points completely determine a codeword. Applying part (a), with $r \leftarrow k-1$, we see that any k points completely determines a degree $< k$ polynomial, and hence a Reed-Solomon codeword (which are the evaluations of that polynomial).

(c) We interpolate $f(X)$ as in part (a) so that $f(\alpha_i) = x_i$ for $i = 0, \ldots, k-1$. Then f has degree at most $k-1$. Then we set $z_j = f(\alpha_j)$ for $j \geq k$.

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.

Solution

The generator matrix is given by $D_{\vec{\lambda}} \cdot G$, where $D_{\vec{\lambda}}$ is the diagonal matrix with $\vec{\lambda}$ on the diagonal, and G is a Vandermonde matrix (the generator matrix for $RS(\vec{\alpha}, n, k)$). GRS codes are MDS since any $k \times k$ submatrix of this generator matrix is full rank; that's true because we saw in the lecture videos/notes that it was true for G, and multiplying by $D_{\vec{\lambda}}$ won't change that.

(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?

Solution

Following the hint, we can write

$$h(X) = \sum_i h(\alpha_i) \frac{L_i(X)}{L_i(\alpha_i)}.$$

In this view, the coefficient on X^{n-1} is

$$\sum_i \frac{h(\alpha_i)}{L_i(\alpha_i)} \cdot (\text{Coeff on } X^{n-1} \text{ in } L_i(X)).$$

We observe that $L_i(X) = \prod_{j \neq i}(X - \alpha_j)$ has degree exactly $n - 1$, and that the leading coefficient is 1. (That's because the only way to get X^{n-1} in this product is to take the "X" from each term $(X - \alpha_j)$). Thus, the coefficient on X^{n-1} in $h(X)$ is

$$\sum_i \frac{h(\alpha_i)}{L_i(\alpha_i)}.$$

On the other hand, the degree of $h(X)$ is at most $n - 2$ by assumption. So the coefficient on X^{n-1} is zero. This is what we wanted to show.

(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 $\vec{\alpha}$?

Solution

We can use part (b). Let $\lambda_i = \frac{1}{L_i(\alpha_i)}$. Let $f(X)$ be a degree $< k$ polynomial corresponding to a codeword c of the RS code, and let $g(X)$ be a degree $< n-k$ polynomial corresponding to a codeword c' of the GRS code with weights λ_i. Then the degree of $h(X) = f(X)g(X)$ is at most $k-1+n-k-1 = n-2 < n-1$, so we apply part (b) to $h(X)$. We get that

$$\sum_{i=1}^{n} c_i c_i' = \sum_{i=1}^{n} f(\alpha_i)\lambda_i g(\alpha_i) = \sum_i \frac{f(\alpha_i)g(\alpha_i)}{L_i(\alpha_i)} = 0.$$

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 $\vec{\alpha}$?

Solution

The same proof as above works, but we should take $\sigma_i = \frac{1}{\lambda_i L_i(\alpha_i)}$.

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...

Solution

By the dual view of RS codes, the coefficients f_i of $f(X) = \sum_{i=0}^{n-1} f_i X^i$ are evaluations of a polynomial $\tilde{f}$ of degree at most $k-1$: that is, $f_i = \tilde{f}(\alpha^i)$ for $i = 1, \ldots, n$. The same is true for g and a degree-$\leq k-1$ polynomial $\tilde{g}$. Thus, the coefficients $h_i = f_i \cdot g_i$ are given by

$$h_i = \tilde{g}(\alpha^i) \cdot \tilde{f}(\alpha^i).$$

Now, the polynomial $\tilde{h}(X) = \tilde{f}(X) \cdot \tilde{g}(X)$ has degree at most $2k-2$, and so by the duality of RS codes again, the polynomial $h(X)$ vanishes on $\alpha, \alpha^2, \ldots, \alpha^{n-2k+1}$, as desired.