③ RS codes and secret sharing: Recall the problem statement for sharing a secret, from Lecture 1. Suppose that the secret is an element $\alpha \in \mathbb{F}$.

Now, one can consider sharing this secret as follows: let

$$\mathcal{F}_\alpha = \{f(x) \in \mathbb{F}^{\leq t-1}[x] : f(x) = a_0 + a_1 x + \dots + a_{t-1} x^{t-1}, \text{ with } a_0 = \alpha\}$$

and pick $f \underset{\text{unif}}{\sim} \mathcal{F}_\alpha$. Encode f using RS$[n,k]$ with $S = \mathbb{F}^*$ to yield a codeword $c = (c_0, \dots, c_{n-1})$ and distribute c_i, $0 \leq i \leq n-1$, to the n different parties.

Via a property of the Vandermonde matrix, it follows that every collection of t coordinates is an information set, allowing for the polynomial f to be reconstructed exactly (and $\alpha = a_0$ to be recovered) when $\geq t$ parties get together. Moreover, the property that any collection of $\leq t-1$ parties can also make a uniformly random guess about α also holds.

Parity-check matrix of RS$[n,k]$

To obtain a parity-check matrix of RS$[n,k]$, the following lemmas will be useful. Let $|\mathbb{F}| = q$, and $S = \mathbb{F}$.

Lemma 3: For any i, j such that $0 \le i+j \le q-2$, we have

$$\sum_{\alpha \in \mathbb{F}} \alpha^i \alpha^j = 0$$

Proof: Note that $\sum_{\alpha \in \mathbb{F}} \alpha^i \alpha^j = \sum_{\alpha \in \mathbb{F}} \alpha^{i+j} = \frac{(\beta^{i+j})^{q-1} - 1}{\beta^{i+j} - 1} = 0,$

for β primitive. Since $\gamma^{q-1} = 1$, for all $\gamma \in \mathbb{F}$, the last equality above holds. ☒

As an immediate corollary of Lemma 3, we obtain the following claim.

Corollary 1: For all $f(x), g(x) \in \mathbb{F}[x]$ s.t. $\deg(f(x)) + \deg(g(x)) \le q-2$, we have

$$\sum_{\alpha \in \mathbb{F}} f(\alpha) \cdot g(\alpha) = 0$$

Proof: Follows by linearity. ▨

Equivalently, we have that $(RS[n,k])^{\perp} \supseteq RS[n, q-k] = RS[n, n-k]$.
However, $\dim((RS[n,k])^{\perp}) = \dim(RS[n, n-k])$, giving rise to the following theorem.

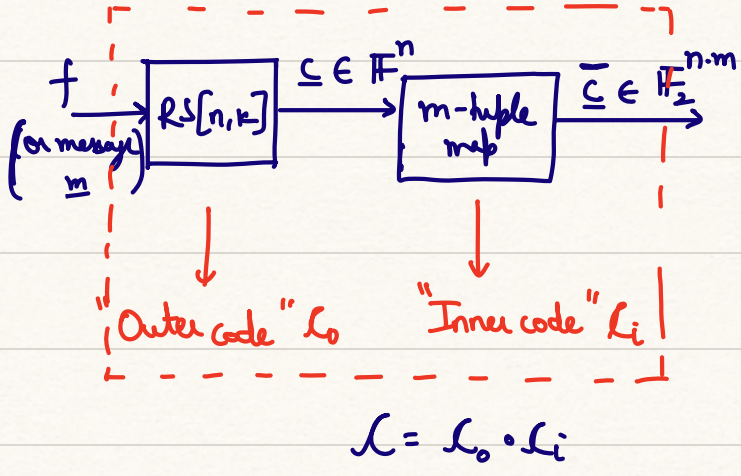
Theorem 1: $(RS[n,k])^{\perp} = RS[n, n-k]$.

Hence, a parity-check matrix of $RS[n,k]$ is simply the Vandermonde generator matrix of $RS[n, n-k]$.

Codes of good distance via concatenation

Although RS codes have excellent error correction property [highest minimum distance possible!], they suffer from the drawback that the field size necessary to construct such codes grows with the blocklength n. In what follows, let $\mathbb{F} = \mathbb{F}_{2^m}$ and $S = \mathbb{F}^*$.

An immediate resolution to this issue is via code concatenation: concatenate a RS $[n, K]$ code with the simple map that takes $\alpha \in \mathbb{F}^*$ to its m-tuple representation. Clearly, the distance of the resultant code is at least $n-K+1$ [Why?], and its dimension (over $\mathbb{F}_2$) is $K \cdot m$. (see the picture below):



$$C = C_o \circ C_i$$

The (linear) concatenated code C is an $[nm, Km, \geq n-K+1]_2$ code.