Lecture: Reed-Solomon Codes, BCH Codes

In this lecture, we shall take a look at one of the most important families of codes: the Reed-Solomon (RS) code family, which are maximum distance separable (MDS) codes that meet the Singleton bound with equality.

Def 1: For integers $1 \leq k \leq n$, a field $\mathbb{F}$ of size $|\mathbb{F}| \geq n$, and a set $S = \{\alpha_1, \ldots, \alpha_n\}$ of distinct elements in $\mathbb{F}$, we define the Reed-Solomon code

$$RS[n,k] = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \in \mathbb{F}^n : f \in \mathbb{F}^{\leq k-1}[x]\}.$$

In words, $RS[n,k]$ consists of the evaluation vectors of polynomials of degree at most $k-1$, on n distinct points in $\mathbb{F}$. Recall from the previous lectures that we now know to construct fields of size $\geq n$, for any n, by choosing a suitable prime power $\geq n$.

Lemma 1: $RS[n,k]$ is an $[n,k]$ linear code over $\mathbb{F}$.

Proof: Observe that a generator matrix of the code is the Vandermonde matrix

$$G_{RS} = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{K-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{K-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{K-1} \end{bmatrix}^T,$$

showing that the code is linear. Further, $\dim_{\mathbb{F}}(RS[n,K]) = K$, since there are exactly $|\mathbb{F}|^K$ distinct polynomials of degree $\leq K-1$ over $\mathbb{F}$. ▨

Lemma 2: $d_{min}(RS[n,K]) = n-K+1.$

Proof: The proof proceeds via Theorem 1 of the last lecture. Indeed, any $f(x) \in \mathbb{F}^{\leq K-1}[x]$ has at most $K-1$ zeros in $\mathbb{F}$, implying that in any codeword $\underline{c} \in RS[n,K]$, we have at most $K-1$ coordinates equalling 0.

The other direction is shown by observing that the codeword corresponding to $f(x) = \prod_{i=1}^{K-1}(x-\alpha_i)$ has exactly $K-1$ coordinates equalling 0. ▨

Remarks: ① The above argument demonstrates that the RS family is a family of MDS codes.

② Typically, one constructs RS codes by picking the set S of evaluation points to be $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$ or $\mathbb{F}$. Then, we have $n = |\mathbb{F}|-1$ or $|\mathbb{F}|$, resp.