STIR (blueprint)

LeastAuthority

April 8, 2025

Chapter 1

The Reed-Solomon Code

Definition 1.1 (Error-Correcting Code)**.** *An* error-correcting code *of length n over an alphabet Σ is a subset $\mathcal{C} \subseteq \Sigma^n$. The code $\mathcal{C}$ is called a* linear code *if $\Sigma = \mathbb{F}$ is a finite field and $\mathcal{C}$ is a subspace of $\mathbb{F}^n$.*

Definition 1.2 (Reed-Solomon Code)**.** *The* Reed-Solomon code *over finite field $\mathbb{F}$, evaluation domain $\mathcal{L} \subseteq \mathbb{F}$ and degree $d \in \mathbb{N}$ is the set of evaluations (over $\mathcal{L}$) of univariate polynomials (over $\mathbb{F}$) of degree less than d:*

$$\mathrm{RS}[\mathbb{F}, \mathcal{L}, d] := \left\{ f : \mathcal{L} \to \mathbb{F} \;\middle|\; \exists\, \hat{f} \in \mathbb{F}^{<d}[X] \text{ such that } \forall x \in \mathcal{L},\; f(x) = \hat{f}(x) \right\}.$$

The rate of $\mathrm{RS}[\mathbb{F}, \mathcal{L}, d]$ *is* $\rho := \frac{d}{|\mathcal{L}|}$.

Given a code $\mathcal{C} := \mathrm{RS}[\mathbb{F}, \mathcal{L}, d]$ and a function $f : \mathcal{L} \to \mathbb{F}$, we sometimes use $\hat{f} \in \mathbb{F}^{<d}[X]$ to denote a nearest polynomial to f on $\mathcal{L}$ (breaking ties arbitrarily).

Remark 1.3. *Note that the evaluation domain $\mathcal{L} \subseteq \mathbb{F}$ is a non-empty set.*

Definition 1.4. *For a Reed-Solomon code $\mathcal{C} := \mathrm{RS}[\mathbb{F}, \mathcal{L}, d]$, parameter $\delta \in [0, 1]$, and a function $f : \mathcal{L} \to \mathbb{F}$, let $\mathsf{List}(f, d, \delta)$ denote the list of codewords in $\mathcal{C}$ whose relative Hamming distance from f is at most δ. We say that $\mathcal{C}$ is* (δ, d)-list decodable *if*

$$\left|\mathsf{List}(f, d, \delta)\right| < |L| \quad \text{for every function } f.$$

The Johnson bound provides an upper bound on the list size of this Reed-Solomon code:

Theorem 1.5 (Johnson bound)**.** *The Reed-Solomon code* $\mathrm{RS}[\mathbb{F}, \mathcal{L}, d]$ *is* $(1 - \sqrt{\rho} - \eta, \frac{1}{2\eta\rho})$*-list-decodable for every $\eta \in (0, 1 - \sqrt{\rho})$, where $\rho := \frac{d}{|\mathcal{L}|}$ is the rate of the code.*