CSE 190, Great ideas in algorithms: Reed-Solomon codes

1 Reed-Solomon codes

Reed-Solomon codes are an important group of error-correcting codes that were introduced by Irving Reed and Gustave Solomon in the 1960s. They have many important applications, the most prominent of which include consumer technologies such as CDs, DVDs, Blu-ray Discs, QR Codes, satellite communication and so on.

Reed-Solomon codes are defined as the evaluation of low degree polynomials over a finite field. Let $\mathbb{F}$ be a finite field. Messages are in $\mathbb{F}^k$ are treated as the coefficients of a univariate polynomial of degree $k-1$, and codewords are its evaluations on $n < |\mathbb{F}|$ points. So, Reed-Solomon codes are defined by specifying $\mathbb{F}, k$ and $n < |\mathbb{F}|$ points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$, and its codewords are

$$\mathcal{C} = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f(x) = \sum_{i=0}^{k-1} f_i x^i, f_0, \ldots, f_{k-1} \in \mathbb{F}\}.$$

We define this family of codes in general as $\mathrm{RS}_{\mathbb{F}}(n,k)$, and if needs, we can specify the evaluation points. An important special case is when $n = |\mathbb{F}|$, and we evaluate the polynomial on all field elements.

Lemma 1.1. *The minimal distance of* $\mathrm{RS}_{\mathbb{F}}(n,k)$ *is* $d = n-k+1$. *So, these are* $(n, k, n-k+1)$*-codes.*

Proof. As $\mathcal{C}$ is a linear code, it suffices to show that for any nonzero polynomial $f(x)$ of degree $\leq k-1$, $|\{x \in \mathbb{F} : f(x) = 0\}| \leq k-1$. So, $|\{i \in [n] : f(\alpha_i) = 0\}| \geq n-k+1$. Now, this follows from the fundamental theorem of algebra, that a nonzero polynomial of degree r has at most r roots. We prove it by induction on r.

If $r = 0$ then f is a nonzero constant, and so it has no roots. So, assume $r \geq 1$. Let $\alpha \in \mathbb{F}$ be such that $f(\alpha) = 0$. Lets shift the input so that the root is at zero. That is, define $g(x) = f(x+\alpha)$, so that $g(0) = 0$ and $g(x)$ is also a polynomial of degree r. Express it as

$$g(x) = \sum_{i=0}^{r} f_i (x+\alpha)^i = \sum_{i=0}^{r} g_i x^i.$$

Since $g_0 = g(0) = 0$, we get that $g(x) = xh(x)$ where $h(x) = \sum_{i=0}^{r-1} g_{i+1}x^i$ is a polynomial of degree $r-1$, and hence $f(x) = g(x-\alpha) = (x-\alpha)h(x-\alpha)$. By induction, $h(x-\alpha)$ has at most $r-1$ roots, and hence f has at most r roots. □

Recall that the Singleton bound shows that in any (n,k,d) code, $n \geq k+d-1$. Codes which achieve this bound, i.e for which $n = k+d-1$, are called MDS codes (Maximal Distance Separable). What we just showed is that Reed-Solomon codes are MDS codes. In fact, for prime fields, it is known that Reed-Solomon are the only MDS codes, and it is conjecture to be true over non-prime fields as well (except for a few exceptions in characteristic two).

2 Decoding Reed-Solomon codes from erasures

We first analyze the ability of Reed-Solomon codes to recover from erasures. Assume that we are given a Reed-Solomon codeword, with some coordinates erased. Let S denote the set of remaining coordinates. That is, for $S \subset [n]$ we know that $f(\alpha_i) = y_i$ for all $i \in S$, where $y_i \in \mathbb{F}$. The question is: for which sets S is this information enough to uniquely recover the polynomial f? Equivalently, we need to solve the following system of linear equations , where the unknowns are the coefficients of the polynomial f, denoted $f_0, \ldots, f_{k-1}$:

$$\sum_{j=0}^{k-1} f_j \alpha_i^j = y_i, \qquad \forall i \in S.$$

Equivalently, let $V = V(\{\alpha_i : i \in S\})$ be the corresponding Vandermonde matrix. That is, it is a $|S| \times k$ matrix given by $V_{i,j} = \alpha_i^j$ for $i \in S, 0 \leq j \leq k-1$. Then we want to solve

$$Vf = y,$$

where $f = (f_0, \ldots, f_{k-1}) \in \mathbb{F}^k$ and $y = (y_i : i \in S) \in \mathbb{F}^{|S|}$. Clearly, we need $|S| \geq k$ for a unique solution to exist. As we saw, whenever $|S| = k$ the matrix V is invertible, hence there is a unique solution. So, as long as $|S| \geq k$, we can restrict to k equations and uniquely solve for the coefficients of f.

Corollary 2.1. *The code* $\mathrm{RS}_{\mathbb{F}}(n,k)$ *can be uniquely decoded from* $n-k$ *erasures.*

3 Decoding Reed-Solomon codes from errors

Next, we study the harder problem of decoding from errors. Again, let $f(x) = \sum_{i=0}^{k-1} f_i x^i$ be an unknown polynomial of degree $k-1$. We know its evaluation on $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$, but with a few errors, say e. That is, we are given $y_1, \ldots, y_n \in \mathbb{F}$, such that $y_i \neq f(\alpha_i)$ for at most e errors. If we knew the locations of the errors, we would be back at the decoding from erasures scenario; however, we do not know them, and enumerating them is too long. Instead, we will learn an algebraic algorithm that can detect them efficiently, as long as the

number of errors is not too large (we will see how many errors we can correct from soon). It is called the Berlekamp-Welch algorithm.

Define a polynomial $E(x)$ as follows:

$$E(x) = \prod_{i:y_i \neq f(\alpha_i)} (x - \alpha_i).$$

The decoder doesn't know $E(x)$. However, we will still use it in the analysis. It satisfies the following equation:

$$E(\alpha_i)\,(f(\alpha_i) - y_i) = 0 \qquad \forall 1 \leq i \leq n.$$

Let $N(x) = E(x)f(x)$. Note that $\deg(E) = e$ and $\deg(N) = \deg(E) + \deg(f) = e + k - 1$. We established the following claim.

Claim 3.1. *There exists polynomials $E(x), N(x)$ of degrees $\deg(E) = e, \deg(N) = e + k - 1$ such that*

$$N(\alpha_i) - y_i E(\alpha_i) = 0$$

for all $1 \leq i \leq n$.

Proof. We have $N(\alpha_i) = E(\alpha_i)f(\alpha_i)$. This is equal to $E(\alpha_i)y_i$ as either $y_i = f(\alpha_i)$ or otherwise $E(\alpha_i) = 0$. □

The main idea is that we can find such polynomials by solving a system of linear equations.

Claim 3.2. *We can efficiently find polynomials $E'(x), N'(x)$ of degrees $\deg(E') \leq e, \deg(N') \leq e + k - 1$, not both zero, such that*

$$N'(\alpha_i) - y_i E'(\alpha_i) = 0$$

for all $1 \leq i \leq n$.

Proof. Let

$$E'(x) = \sum_{j=0}^{e} a_j x^j, \qquad N'(x) = \sum_{j=0}^{e+k-1} b_j x^j,$$

where a_j, b_j are unknown coefficients. They satisfy the following system of n linear equation:

$$\sum_{j=0}^{e} a_j (\alpha_i)^j - y_i \sum_{j=0}^{e+k-1} b_j (\alpha_i)^j = 0 \qquad \forall 1 \leq i \leq n.$$

We know that this system has a nonzero solution (since we know that E, N exist by our assumptions). So, we can find a nonzero solution by linear algebra. □

Note that it is not guaranteed that $E' = E, N' = N$, so we are not done yet. However, the next claim shows that we can still recover f from any E', N' that we find.

Claim 3.3. *If $e \leq (n-k)/2$ then $N'(x) = E'(x)f(x)$.*

Proof. Consider the polynomial $R(x) = N'(x) - E'(x)f(x)$. Note that for any i such that $f(\alpha_i) = y_i$, we have that

$$R(\alpha_i) = N'(\alpha_i) - E'(\alpha_i)f(\alpha_i) = N'(\alpha_i) - E'(\alpha_i)y_i = 0.$$

So, R has at least $n-e$ zeros. On the other hand, $\deg(R) \leq \max(\deg(N'), \deg(E')+\deg(f)) \leq e+k-1$. So, as long as $n-e > e+k-1$, it has more zeros than its degree, and hence must be the zero polynomial. □

Corollary 3.4. *The code $\mathrm{RS}_{\mathbb{F}}(n,k)$ can be uniquely decoded from $(n-k)/2$ errors.*

Note that this is the best we can do, as the minimal distance is $n-k+1$.