6.895 Essential Coding Theory October 4, 2004

Lecture 8

Lecturer: Madhu Sudan *Scribe: Anindya C. Patthak*

1 Overview

In this lecture we will cover List Decoding of Reed-Solomon Codes.

2 List Decoding of Reed-Solomon Codes: Combinatorial Perspective

In the last lecture we have seen the combinatorial version of list decoding. Recall that we are given a code of distance d and we would like to correct more than $d/2$ errors. We argued that unique decoding is not possible. Therefore we decided on outputting a small list of codewords that has good agreement with the received word. We established the following combinatorial version of list decoding that ensured existence of a polynomial size list provided the agreement is suitably large.

Theorem 1 *(Combinatorial Version) Let C be an (n, k, d) error[1] correcting code over an alphabet Σ of size q. Then given any ball $B(x, r)$, where $x \in \Sigma^n$ and $r = n - \sqrt{(n-d)n}$, the set $C \cap B(x, r)$ has size at most* $\text{poly}(n)$*, more specifically n^2.*

Definition 2 *Given an $[n, k, d]_q$ code C over an alphabet Σ, we say that C is (e, ℓ)-list decodable code, if for every $x \in \Sigma^n$, $B(x, e) \cap C$ has size at most ℓ.*

The following corollary is then immediate from Theorem 1.

Corollary 3 *(***List Decoding of Reed-Solomon Codes***:Combinatorial Version) An $[n, k, n-k+1]_q$* RS *code is $(n - \sqrt{n(k-1)}, n^2)$-list decodable.*

3 List Decoding of Reed-Solomon Codes: Algorithmic Perspective

The algorithmic challenge of list decoding is the following:

Given an (e, ℓ)-list decodable code C and any received word $y = \langle y_1, \cdots, y_n \rangle$, output the set $B(y, e) \cap C$.

For an easier exposition, we give the following definition.

Definition 4 *Given $x, y \in \mathbb{F}_q^n$, we define the agreement between x and y to be*

$$\textit{agreement}(x, y) \stackrel{def}{=} |\{i | x_i = y_i\}|.$$

With this definition, we reformulate our list-decoding task the following way:

Given any (e, ℓ)-list decodable code C and a received word $y = \langle y_1, \cdots, y_n \rangle$, output the set $\{x \in C \mid \textit{ agreement}(x, y) \geq t\}$, where we set $t = n - e$.

We now describe an algorithm to list-decode RS codes from $(k+1)\sqrt{n} + 1$ agreements. With some parameter optimization, the same algorithm can be used to list-decode RS codes from agreements as low as $2\sqrt{kn} + 1$. It is possible to improve our result to correct more errors. There is an algorithm due to Guruswami and Sudan that can list-decode RS codes from agreement as small as $\sqrt{kn} + 1$. However, that requires more sophisticated arguments and therefore we skip.

[1] The bound on list size does not depend on the dimension k.

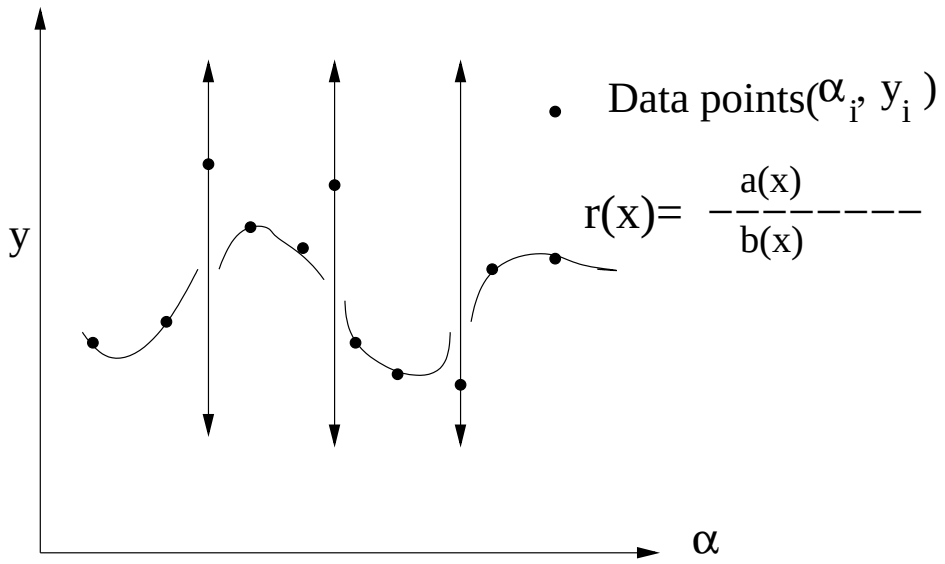

Figure 1: Interpretation of data through rational function

3.1 Problem Formulation

We quickly recall the problem we are considering.

PROBLEM: **List Decoding of Reed-Solomon codes**
INPUT: $\mathbb{F}, n, k, t$; $\alpha_1, \cdots, \alpha_n \in \mathbb{F}$, a received vector $\langle y_1, \cdots, y_n \rangle \in \mathbb{F}^n$.
GOAL: Find all polynomials p of degree $< k$ s.t. $p(\alpha_i) = y_i$ for at least t values of i.

As mentioned earlier our goal today is to find an algorithm for $t > (k+1)\sqrt{n}$.

Recall that in Welch-Berlekamp Decoder we carry out the following steps:

WELCH-BERLEKAMP DECODER

1. Find polynomials (N, E) s.t. $N(\alpha_i)/E(\alpha_i) = y_i$ holds for all $i \in [n]$ provided $E(\alpha_i) \neq 0$
2. Output $N(x)/E(x)$

Alternatively we may think of finding a rational function "to explain" the data. We will make this idea precise soon. Recall that univariate rational functions are functions that are fraction of two univariate polynomials. They have a form $f(x)/g(x)$, where $f(x)$ and $g(x)$ are univariate polynomials. They also need to satisfy the requirement that whenever $g(x) = 0$ implies $f(x) = 0$. In another words the zero set of polynomial $g(x)$ is a subset of the zero set of polynomial $f(x)$. Note if $f(x)$ and $g(x)$ are given explicitly, then it is necessary that $g(x)$ divides $f(x)$ and this does not give more power than univariate polynomials. However, the power comes if we do not know $f(x)$ and $g(x)$ explicitly, but given any x, we can compute $f(x)$ and $g(x)$. Let $r(x) = f(x)/g(x)$ be a rational function. Suppose α is in the zero set of $g(x)$. Then we know $g(\alpha) = f(\alpha) = 0$. How should we define $r(\alpha)$? A good idea is to allow $r(\alpha)$ to take any possible value. This is explained in the Figure 1.

Therefore, given a set of $\{(\alpha_i, y_i)\}_{i \in [n]}$, we relax the Welch-Berlekamp-type interpolation problem as follows:

- (WELCH-BERLEKAMP-type Goal): Find a *polynomial* $p(x)$ such that $p(\alpha_i)$ *equals* y_i *for many* i
- (Reformulation): Find a *rational function* $r(x)$ which *explains* y_i for all α_i

Thus we replace the claim in Welch-Berlekamp by the following claim.

Claim 5 *(Welch-Berlekamp) If $\exists p$ of degree $< k$ agreeing $\frac{n+k}{2}$ values of y_i then a pair of polynomials (N, E) exists with $deg(N) \leq \frac{n+k}{2}$ and $deg(E) \leq \frac{n-k}{2}$ such that $N(\alpha_i) = E(\alpha_i)p(\alpha_i)$ holds for all i.*

Claim 6 *(A slight relaxation) A pair of polynomials (N, E) exists with $deg(N) \leq \frac{n+k}{2}$ and $deg(E) \leq \frac{n-k}{2}$ such that $\frac{N}{E}(\alpha_i) = y_i$ holds whenever[2] $E(\alpha_i) \neq 0$.*

Sketch of Proof We solve the linear system $N(\alpha_i) = y_i E(\alpha_i)$ for $i = 1, \cdots, n$. This is a homogenous linear system and therefore always has a solution. Note $(N, E) \equiv (0, 0)$ is a trivial solution. We will prove that the the system has more than one solution and thus a non-trivial solution exists. The system can be reformulated as a matrix-vector equation i.e., $A \cdot X = 0$ where A is the co-efficient matrix and X is the unknown vector. Note that the rank of matrix A, say r, can be at most n. However the number of unknowns is $(n-k)/2 + 1 + (n+k)/2 + 1 = n + 2$. This system has $|\mathbb{F}|^{n+2-r}$ number of solutions including the trivial one. Since $r \leq n$, thus there exists a non-trivial solution. ■

3.2 Nice Algebraic Interpretations of Data

Earlier we have argued that univariate rational functions are generalizations of univariate polynomial functions. It turns out that there are even richer class of functions that fits our purpose better. Given a set of pairs $\{(\alpha_i, y_i)\}_{i \in [n]}$ we would fit them in an algebraic curve in the plane, that is, we would construct a bi-variate polynomial $Q(x, y)$ s.t. $Q(\alpha_i, y_i) = 0$ for all $i \in [n]$. We make the following claim.

Claim 7 *(Bi-variate Interpolation Claim) For every set of pairs $\{(\alpha_i, y_i)\}$ of size n, there exists a bivariate polynomial $Q(x, y)$ with $deg_x(Q), deg_y(Q) \leq \sqrt{n}$ such that*

$$Q(\alpha_i, y_i) = 0 \text{ for all } i \in [n] \text{ and } Q(x, y) \neq 0$$

Sketch of Proof We will set up a linear system with the coefficients of $Q(x, y)$ being unknowns. Note from the degree bound, the number of unknown variables is $(\sqrt{n} + 1)^2$. However the number of constraints is n. This is an under-constrained system. Therefore the system has more than one solution including the trivial one (i.e., identically zero polynomial). Thus non-trivial solutions exists. ■

Consider the algebraic curve in Figure 2. An inspection reveals that the curve is given by the equation $Q(x, y) = (x^4 - y^4 - x^2 + y^2)$. Note however that there are many points which fits nicely on simpler curves $(x + y)$, $x - y)$ and $(x^2 + y^2 - 1)$. Thus to solve the list decoding problems, we can think of getting an algebraic curves that fits the data nicely. Then we can hope that the curve may be factored into several factors and each factor will have good agreement with the data. We now show that *this intuition works.*

3.3 List Decoding of Reed-Solomon Codes

We describe the list decoding algorithm.

[2]Note thus we are essentially looking for a rational function in x.

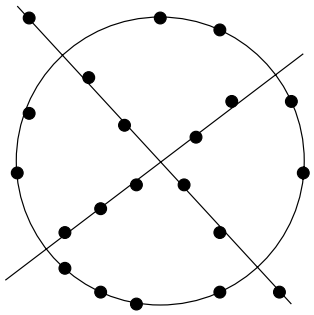

Figure 2: An algebraic curve that fits many points

LIST DECODING OF RS CODE
INPUT: $\{(\alpha_i, y_i)\}_{i\in[n]}, t > (k+1)\sqrt{n}$
OUTPUT: A list of univariate polynomials p_j of degree $\leq k$ such that $p_j(\alpha_i) = y_i$ for at least t values of i

1. Find $Q(x,y) \neq 0$ where $\deg_x(Q), \deg_y(Q) \leq \sqrt{n}$ such that $Q(\alpha_i, y_i) = 0$ for all i
2. Factor $Q(x,y)$ into irreducible polynomials i.e., let $Q(x,y) = Q_1(x,y)\cdots Q_s(x,y)$
3. Output all polynomials $p_1, \cdots p_j$ of degree $\leq k$ if $(y - p_j(x)) \equiv Q_j(x,y)$ and $p_j(\alpha_i) = y_i$ for at least t values of i

Claim 8 *Algorithm* LIST DECODING OF RS CODE *runs in poly time and outputs all polynomial $p(x)$ such that $p(\alpha_i) = y_i$ for at least t values of i.*

Sketch of Proof Step 1 and 3 can clearly be done in polynomial time. Moreover there are efficient algorithms to solve the multivariate polynomial factorization problem over finite fields (in fact over almost all fields). Deterministic versions of these algorithms takes $poly(\log|\mathbb{F}|, n)$ steps over most fields and $poly(|\mathbb{F}|, n)$ steps over few fields[3]. However efficient randomized versions are known that runs in $poly(\log|\mathbb{F}|, n)$ time for all fields. This ensures that the algorithm is efficient i.e., runs in polynomial time.

By Claim 7 we know step 1 always finds a non-trivial Q. Therefore all that remains to show is the following: If p has degree $\leq k$ and satisfies $p(\alpha_i) = y_i$ for at least t values of i and if $Q(x,y)$ is an output of step 1, then $(y - p(x))|Q(x,y)$ provided $t > (k+1)\sqrt{n} + 1$. Assume $p(x)$ is such a polynomial.

How could one hope to prove such divisibility results? In general this may be addressed using age-old Bezout's theorem.

Theorem 9 *(Bezout's Theorem in the plane) Let $Q_1(x,y)$ and $Q_2(x,y)$ be bivariate polynomials of degree at most D_1 and D_2, respectively over a field F. If $Q_1(x,y)$ and $Q_2(x,y)$ have more than $D_1 \cdot D_2$ common zeros, then they share a non-trivial factor.*

Thus if one of the polynomials is irreducible, then this gives a divisibility criteria. It turns out that we can argue even simpler. We recall the following innocent lemma.

Lemma 10 *(Remainder Theorem) Let $g(y)$ be an univariate polynomial over a field F. Then for any $\gamma \in \mathbb{F}$, $(y - \gamma)|g(y)$ if and only if $g(\gamma) = 0$.*

We mention that the above theorem holds over UFD (Unique Factorization Domain). We also mention that $\mathbb{F}[x], \mathbb{F}[x_1, \cdots, x_n]$ i.e., the ring of univariate and multivariate polynomials over a field, are in fact UFD. We will apply the above lemma over $\mathbb{F}[x]$.

[3]For example, over a large prime field $\mathbb{F}_p$

Recall we want to show that $(y - p(x))|Q(x, y)$. By Lemma 10, it is therefore enough to show that $Q(x, p(x))$ is identically zero polynomial. Define

$$h(x) \stackrel{def}{=} Q(x, p(x)).$$

The following claim can easily be verified by replacing y by $h(x)$.

Claim 11 *$deg(h(x)) \leq (1 + k)\sqrt{n}$.*

By hypothesis we have that $p(\alpha_i) = y_i$ for at least t values of i. Note whenever it holds that $p(\alpha_i) = y_i$, we have $h(\alpha_i) = Q(\alpha_i, p(\alpha_i)) = Q(\alpha_i, y_i) = 0$. This implies the following claim.

Claim 12 *$h(x)$ has at least t zeros.*

Since a univariate polynomial of degree d can have at most d zeros, from Claims 11 and 12 and the fact that $t > (1 + k)\sqrt{n}$ we conclude that $h(x)$ must be identically zero polynomial. This concludes the analysis. ■

Remark Note that the $\deg_y(Q) \leq \sqrt{n}$ and therefore it can have at most $\sqrt{n}$ factors of the form $(y - p(x))$. However this does not improve upon the combinatorial version of the list decoding. The agreement assumed here is much larger than the one assumed in the combinatorial version.

We now modify the interpolation lemma slightly. We now try to find a bivariate poly $Q(x, y)$ with $\deg_x(Q) \leq \sqrt{kn}$ and $\deg_y(Q) \leq \sqrt{n/k}$. With this setting the same algorithm can be used to recover codewords from agreement $t > 2\sqrt{kn}$ (can be proved in an analogous fashion).

Theorem 13 *Interpolating with a bivariate polynomial $Q(x, y)$ with $deg_x(Q) \leq \sqrt{nk}$ and $deg_y(Q) \leq \sqrt{n/k}$, the algorithm* List Decoding of RS code *solves the* RS *list decoding problem with agreements $> 2\sqrt{kn}$ in polynomial time.*

(**Notes**)

1. As mentioned previously the best known list decoding algorithm can correct from agreements as low as $\sqrt{kn}$. Moreover the algorithm does not necessarily require that all α_i's are distinct. Though it assumes a bound on the number that a distinct α_i can appear. We leave the details.

2. Can we do better? A recent result of Guruswami and Rudra suggest that in order to improve the algorithm we have to exploit the fact that many α_i's are distinct.

3. At this moment all the combinatorial results involving Reed-Solomon codes have their algorithmic counterparts. We mention that Guruswami and Vardy have recently shown that the Maximum-Likelihood Decoding of Reed-Solomon Code is NP-complete.