6.440 Essential Coding Theory March 6 2013

Lecture 9

Lecturer: Eli Ben-Sasson *Scribe: Mohamamd Bavarian*

Madhu is traveling, so we are happy to have Eli Ben-Sasson from Technion to give us a lecture today on limits of list decoding Reed Solomon codes. List Decoding is an important task is coding theory, and RS codes are probably one of the most useful codes out there, both in theory and applications. So it is important to understand the limits of this task. By the way, this work mostly addresses the phenomenon of full list decoding. It seeks to find ranges of parameter where the list becomes too large and hence even combinatorial list decoding becomes impossible. However, there are many other variant of the problem such as uniformly sampling from the list, or even producing a single element of the list where this result does not prove any limitation for. That's one frontier of research if you like these kind of topics. Most of this lecture is based on joint work with Swastik Kopparty and Jaikumar Radhakrishnan.[BSKR10]

1 Prelimineries

As mentioned previously, we will work with Reed-Solomon codes in this lecture. In RS codes, the codewords are evaluations of polynomials of degree $\leq d$ on the whole field $\mathbb{F}_N$. Notice the block length N here coincides with field size q. We will mostly be interested in parameter regime where $K = N^\delta$ for some $0 < \delta < 1$. So in our cases of interest $d = N - K + 1$ would be asymptotically close to N. Now recall that given a linear code $C = [n, k, d]_q$ and $w \in \mathbb{F}_q^n$, the decoding problem is the problem of finding a codeword $c \in C$ close to received message w. If we assume the agreement between codeword and the message, $A_g(w, c) > n - d/2$, then finding c is called the *unique decoding* problem. The list decoding question was raised by Elias and Wozencraft: How large the agreement parameter need to be so that we can at least produce decode a list candidate codewords $\exists c_1, c_2, \ldots, c_l$ Find $c_1, c_2, \ldots, c_l$ in proximity of message w. The following theorem of Johnson shows that in principle list-decoding might be possible,

Theorem 1 (Johnson) *Let α denote the agreement parameter for the list decoding radius. If $\alpha > \sqrt{N(N-d)}$ for all $w \in \mathbb{F}^N$. Then $L_\alpha(w) = \{c \in C \mid A_g(w, c) > \alpha\}$ Then,*

$$|L_\alpha(w)| < O(N^2)$$

Let's put Johnson's bound into perspective in our regime of parameters. As $d \to N$ the agreement parameter for unique decoding goes to $\frac{1+x}{2}$ and then the agreement goes to $\sqrt{x}$ in list decoding regime where x is relative rate. The algorithmic breakthrough came through by the work of Sudan, which later was improved by Gursuwami and Sudan. [Sud97, GS99]

Theorem 2 (Sudan, GS) *There exist an efficient algorithm that given $\mathbb{F}_N, K, N, A$ and a received message $w \in \mathbb{F}_N^N$ produces all the $RS(N, K)$ codewords with $Ag(c, w) > A$ as long as $A > \sqrt{NK}$.*

Our main result proves some limitation to list decoding of Reed-Solomon codes,

Theorem 3 ([BSKR10]) *Let q be a prime power and n some positive integer. Let $0 \leq u \leq v \leq m$ then there exists $P \subseteq F_{q^m}^{\leq q^u}[X]$ and $w \in \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ such that,*

1. $|P| \geq q^{(u+1)m - v^2}$
2. $\forall f \in P$ *we have* $Ag(w, f) > q^v$
3. $w(X) = X^{q^v} + \sum_{i=u+1}^{v-1} c_i X^{q^i}$

Now by setting the parameters in above theorem we get some corollaries.

Corollary 4 (Low Rate) *Let $\delta \leq \rho$ be in $(0,1)$. Then for infinitely many N there is a word $w : \mathbb{F}_N \to \mathbb{F}_N$*

$$\left|\{f \in RS[N, N^\delta] : Ag(w,f) \geq N^\rho\}\right| \geq N^{(\delta-\rho^2)\log_2 N}$$

If you compare with Johnson bound you see that when $\alpha > N^{(1+\delta)/2}$ then $|L_\alpha(w)| < O(N^2)$. However, above corollary says if $\alpha = N^{\sqrt{\delta}}$ then $|L_\alpha(w)| > N^{\Omega(\log N)}$. So we have a super polynomial lower bound on the list size..
The above separation was striking in the regime when the rate is small say going slowly to zero. Can we get something in the constant rate regime?

Corollary 5 *Let $r' \leq r \leq 2r'$ and $R = 2^{-r}$ and $A = 2^{-r'}$. Then for $RS[N, K = RN]$ and $\alpha = R'N$. (Note $\alpha > K$). We have $\exists w \in \mathbb{F}^N$ such that $|L_\alpha(w)| \geq N^{2r'-r}$*

Once more, let's compare this to the Johnson bound: If $\alpha > \sqrt{R}N \Rightarrow |L_\alpha(w)| < N^2$ But if $\alpha = R^{(1+\epsilon)/2}N \Rightarrow |L_\alpha(w)| > N^{c_R}$ we have $c_R \to \infty$. Now let's see more directly a corollary for limits of list decoding:

Corollary 6 *For all $\epsilon > 0$, there is no polynomial time algorithm that, for any N and K and received word $w : \mathbb{F}_N \to \mathbb{F}_N$, produces a list $P \in RS[N, K]$ with $Ag(w, P) > K^{1/2+\epsilon}N^{1/2-\epsilon}$.*

2 Subspace Polynomials

The main ingredient for the proof is the following class of very useful polynomials which we shall call *subspace polynomials*. Subspace polynomials are a subclass of *linearized polynomials*. These are polynomials $P : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ that satisfy $P(a\alpha + b\beta) = aP(\alpha) + bP(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^m}$ and $a, b \in \mathbb{F}_q$. Given this definition, the following lemma is obvious.

Lemma 7 *The zero set of linearized polynomials is a vector space over $\mathbb{F}_q$.*

Now let's define subspace polynomials.

Definition 8 *Let $K = \mathbb{F}_{q^m}$ be the degree m field extension of $\mathbb{F}_q$. K can be seen naturally as vectors space of dimension m over $\mathbb{F}_q$. Let $V \subseteq K$ be d dimensional space over $\mathbb{F}_q$. Consider*

$$P_V(X) = \prod_{v \in V} (X - v)$$

This is the polynomial corresponding the subspace V.

Theorem 9 (Ore) *Let P_V be the subspace polynomial corresponding to a d dimensional subspace $V \subseteq K$, where K is a finite field of characteristic q. For some coefficient $c_i \in K$,*

$$P_V(X) = X^{q^d} + \sum_{i=0}^{d-1} c_i X^{q^i}$$

Notice that because $(a\alpha + b\beta)^{q^s} = a\alpha^{q^s} + b\beta^{q^s}$ it follows that any polynomial of above form is indeed a linearized polynomial.
Proof Let $\{v_1, v_2, v_3, \ldots, v_d\}$ be a basis for V. Consider the $d \times (d+1)$ matrix A as follows,

$$A = \begin{bmatrix} 1 & v_1^q & v_1^{q^2} & \ldots & v_1^{q^d} \\ 1 & v_2^q & v_2^{q^2} & \ldots & v_2^{q^d} \\ \vdots & \vdots & \vdots & \ddots & \ldots \\ 1 & v_d^q & v_d^{q^2} & \ldots & v_d^{q^d} \end{bmatrix}$$

Since the number of columns is more than rows $Ax = 0$ has a non-trivial solution. This corresponds to a non-zero polynomials of degree at most q^d where $\{v_i\}$ all are roots. Now since the only non-zero coefficients of this polynomial is at powers of q we see that this is a linearized polynomial and hence vanishes on whole V. Since this means the polynomial has q^d roots we see that it has be degree at least q^d which proves that V is the only zero points of the polynomial. Dividing by the coefficient of q^d which we know is non-zero finishes the proof. ■

Subspace polynomials are important mostly because two properties: Their sparsity and their abundance of zeroes. They have applications in following areas:

1. Limits to Reed Solomon List decoding which is our present concern.
2. Super-efficient verification of computation. [Ben Sasson with Sudan, Sudan Vadhan et al, and with Chiesa et al]
3. Analyzing affine extractor. [Ben Sasson and Kopparty]

While we are at it let's mention a few more simple facts about subspace polynomials which we won't need but they are amusing so you must learn them: As they are linear their image is also a subspace. Let U be the subspace $P_V(K)$. The dimension U is $m - d$ since V the kernel of the linear map. By composing the linear maps, it follows that

$$P_U(P_V(X)) = P_V(P_U(X)) = X^{q^m} - X$$

The above relationship is a notion of *duality*.

3 Proof of The Main Theorem

Theorem 10 ([BSKR10]) *Let q be a prime power and n some positive integer. Let $0 \leq u \leq v \leq m$ then there exists $P \subseteq F_{q^m}^{\leq q^u}[X]$ and $w \in \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ such that,*

1. $|P| \geq q^{(u+1)m-v^2}$
2. $\forall f \in P$ *we have* $Ag(w, f) > q^v$
3. $w(X) = X^{q^v} + \sum_{i=u+1}^{v-1} c_i X^{q^i}$

Proof Consider all subspace V's of dimension v of K. By counting the number of bases and dividing by the number of all the elements of $GL(\mathbb{F}_{q^m})$ we see that the number of such subspaces is as follows,

$$\frac{(q^m - 1)(q^m - q)\dots(q^m - q^{v-1})}{(q^v - 1)(q^v - q)\dots(q^v - q^{v-1})} \geq q^{v(m-v)}$$

There exist $q^{-m(v-u-1)}$ fraction of such subspaces whose subspace polynomials have the coefficients the same α_i's for degree $q^v, q^{v-1}, \dots q^{u+1}$. So take this set of $q^{v(m-v)} \times q^{-m(v-u-1)} = q^{(u+1)m-v}$ and let P to be the union of the subspace polynomials for them. Consider the word $w : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ given by

$$w(X) = X^{q^v} + \sum_{i=u+1}^{v} \alpha_i X^{q^i}$$

Now consider $q(X) = w(X) - f(X)$ for any $f \in P$. It is clear that any such q is a polynomial of degree at most q^u and it agrees with w in number of roots of f which is q^v. Since $|P| \geq q^{(u+1)m-v}$ this finishes the proof. ■

References

[BSKR10] Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace polynomials and limits to list decoding of reed-solomon codes. *IEEE Trans. Inf. Theor.*, 56(1):113–120, January 2010.

[GS99] Venkatesan Guruswami and Madhu Sudan. Improved decoding of reed-solomon and algebraic-geometric codes. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 181–190, 1999.

[Sud97] Madhu Sudan. Decoding of reed solomon codes beyond the error-correction bound. *J. Complex.*, 13(1):180–193, March 1997.