ECE537 Topics in Coding Theory, Lecture 10 Mar 2, 2021

Lecture 10

Instructor: Prasad Krishnan *Scribe: Athreya C*

1 Today

- Recap of an efficient algorithm ("Algorithm 2") for correct list decoding for radius $1-\sqrt{2R}$.
- An efficient algorithm ("Algorithm 3") for correct list decoding for radius of $1-\sqrt{R}$.

2 Recap of Algorithm 2

1. **Interpolation:** Find $Q(X,Y)$ such that $Q(\alpha_i,y_i)=0$ for each $i=1,\cdots,n$.
2. **Factorization:** Include in the list all $\hat{M}(X)$ that satisfy -
   (a) $deg(\hat{M}(X))\leq k-1$
   (b) $(Y-\hat{M}(X))|Q(X,Y)$
   (c) $d_H((\hat{M}(\alpha_1),\cdots,\hat{M}(\alpha_n)),y)\leq e=\delta n$

The algorithm is said to be correct if the transmitted message polynomial is within the outputted list.

This is ensured by verifying that properties (a) and (c) are satisfied iff property (b) is satisfied. This is done by considering the polynomial $R(X)=Q(X,M(X))$ and checking that it is the zero polynomial for any $M(X)$ satisfying (a) and (c). If this is the case, $(Y-M(X))|Q(X,Y)$.

Definition 1. $(1,k-1)$*-degree/*$deg(R(X))=max_{i,j}\{i+j(k-1):q_{ij}$ *is a non-zero coefficient in* $Q(X,Y)\}$.

For algorithm 2, $Q(X,Y)$ is defined as $\sum_{i,j:i+j(k-1)\leq D}q_{ij}X^iY^j$. The number of roots of $R(X)$ is at least $n-e$ since whenever $M(\alpha_i)=y_i$, $Q(\alpha_i,y_i)=0$ and hence $R(\alpha_i)=0$. We want to choose D such that $e<1-\sqrt{2R}$.

Using a counting argument we got that the number of non-zero coefficients of $Q(X,Y)$ was $\geq\frac{D(D+1)}{2(k-1)}$. We also got that the number of constraints satisfied by these coefficients were exactly n. For the system of equations to have a solution, we required $\frac{D(D+1)}{2(k-1)}>n$ and hence could infer D.

3 Algorithm 3

1. **Interpolation:** Find a non-zero polynomial $Q(X,Y)$ such that its (1,k-1) degree $\leq D$, and (α_i,y_i), for $i=1,\cdots,n$, are roots of $Q(X,Y)$ each with multiplicity r.
2. **Factorization:** Include in the list all $\hat{M}(X)$ that satisfy -
   (a) $deg(\hat{M}(X))\leq k-1$
   (b) $(Y-\hat{M}(X))|Q(X,Y)$
   (c) $d_H((\hat{M}(\alpha_1),\cdots,\hat{M}(\alpha_n)),y)\leq e=\delta n$

3.1 Correctness

Now we state two claims to prove the correctness of the algorithm. The idea is the same: use a degree argument on $R(X)$. However, now due to the multiplicity, the number of constraints increases during step 1.

Claim 2. *If (α_i, y_i) is a root of multiplicity r, for each $i = 1, \cdots, n$, then the number of constraints satisfied by the coefficients of $Q(X,Y)$ if $\frac{nr(r+1)}{2}$*

Claim 3. *If $M(X)$ is a polynomial such that properties (a) and (c) hold and $Q(X,Y)$ is a polynomial obtained from step 1 of algorithm 3, then $R(X)$ has at least $n-e$ roots in $\{\alpha_1, \cdots, \alpha_n\}$, each having multiplicity r. i.e. If al_i is a root of $R(X)$ then $(X-\alpha_i)^r | R(X)$.*

Proof of correctness: In step 1, to interpolate such a polynomial, we require that the number of non-zero coefficients, $\geq \frac{D(D+1)}{2(k-1)}$, must be larger than the number of constraints on these coefficients. By claim 1, the number of constraints is $\frac{nr(r+1)}{2}$. Thus $\frac{D(D+1)}{2(k-1)} > \frac{nr(r+1)}{2}$. This gives us $D = \sqrt{nr(r+1)(k-1)}$.

By claim 2, $R(X)$ has $(n-e)r$ roots (when counted with multiplicity). To show that $R(X)$ is the zero polynomial, we want $(n-e)r > D$. Substituting the value for D, we get $e < n = \sqrt{\frac{n(r+1)(k-1)}{r}}$. Therefore, $\frac{e}{n} < 1 - \sqrt{\frac{(r+1)(k-1)}{nr}}$. Suppose we choose $r = k-1$ we get our required $\frac{e}{n} < 1 - \sqrt{R}$. □

3.2 Multiplicity of Roots

Definition 4. *$f(x)$ has a root at 0, with multiplicity r, if $X^r | f(X)$ (OR) $f(x)$ does not have monomials of degree $< r$.*

Definition 5. *$f(x)$ has a root at α, with multiplicity r, if $(X-\alpha)^r | f(X)$.*

Remark $f(x)$ has root α with multiplicity r iff $f(X+\alpha)$ has root 0 with multiplicity r.

Definition 6. *$Q(X,Y)$ has a root at $(0,0)$ with multiplicity r if $Q(X,Y)$ contains no monomial of total degree $< r$. i.e. $\sum_{i,j} q_{ij} X^i Y^j$ such that $q_{ij} = 0$ for $0 \leq i+j \leq r-1$.*

Remark $Q(X,Y)$ has a root at (α_i, y_i) with multiplicity r, if $Q(X+\alpha_i, Y+y_i)$ has root $(0,0)$ with multiplicity r.

3.3 Proof of Claim 2

Let (α, y) be a roots of multiplicity r, for each $i = 1, \cdots, n$. This means that $Q(X+\alpha, Y+y)$ has a root at $(0,0)$ with multiplicity r.

Suppose $Q(X+\alpha, Y+y) = \sum_{i,j} q_{ij}(X+\alpha)^i (Y+y)^j = \sum_{i',j'} \tilde{q}_{i'j'} X^{i'} Y^{j'}$. By multiplicity, we have $\tilde{q}_{i,j} = 0$ for all $i+j \leq r-1$. Therefore total number of zero coefficients for a fixed (α, y) is $\sum_{j=0}^{r-1}(r-j) = \frac{r(r+1)}{2}$. Thus for all (α_i, y_i), number of zero coefficients is $\frac{nr(r+1)}{2}$. Each of these behave as a constraint and hence there are $\frac{nr(r+1)}{2}$ many constraints. □

Remark We can show the relation between q_{ij} and $\tilde{q}_{ij}$. $\sum_{i,j} q_{ij}(X+\alpha)^i (Y+y)^j = \sum_{i',j'} \tilde{q}_{i'j'} X^{i'} Y^{j'}$. Consider the LHS. Expanding the inner terms using binomial expansion we have,

$$\sum_{i,j} q_{ij} [\sum_{i'=0}^{i} \binom{i}{i'} X^{i'} \alpha^{i-i'}][\sum_{j'=0}^{j} \binom{j}{j'} Y^{j'} y^{j-j'}]$$

.

Reversing the order of summations we get,

$$\sum_{i',j'}[\sum_{i\geq i',j\geq j'} q_{ij}\binom{i}{i'}\alpha^{i-i'}\binom{j}{j'}y^{j-j'}]X^{i'}Y^{j'}$$

Hence,

$$\tilde{q}_{i'j'} = [\sum_{i\geq i',j\geq j'} q_{ij}\binom{i}{i'}\alpha^{i-i'}\binom{j}{j'}y^{j-j'}]$$

3.4 Proof of Claim 3

As stated before, the number of roots of $R(X)$ is at least $n-e$ since whenever $M(\alpha_i) = y_i$, $Q(\alpha_i, y_i) = 0$ and hence $R(\alpha_i) = 0$. Let (α, y) be at one such position. We want to show that $R(X)$ has a root at α with multiplicity r.

Equivalently, we want to show that $R(X+\alpha)$ is divisible by X^r.

Now, $R(X+\alpha) = Q(X+\alpha, M(X+\alpha))$. Adding and subtracting y, $R(X+\alpha) = Q(X+\alpha, M(X+\alpha+y-y))$. Let $\tilde{M}(X+\alpha) = M(X+\alpha) - y$. Thus, $R(X+\alpha) = Q(X+\alpha, \tilde{M}(X+\alpha)+y)$.

Note that for $TildeM(X+\alpha) = M(X+\alpha) - y$, we have $\tilde{M}(0+\alpha) = M(0+\alpha) - y$. By our choice of (α, y), $M(\alpha) - y = 0$. Hence, $X|\tilde{M}(x+\alpha)$, or, $\tilde{M}(X+\alpha) = Xg(X)$ for some polynomial $g(X)$.

Looking at $R(X+\alpha)$,

$$R(X+\alpha) = Q(X+\alpha, \tilde{M}(X+\alpha)+y)$$

We know that $Q(X+\alpha, Y+y)$ does not have a monomial of degree $< r$. Expanding,

$$= \sum_{ij:i+j\geq r} \tilde{q}_{ij}X^i\tilde{M}(X+\alpha)^j$$

Substituting $\tilde{M}(X+\alpha) = Xg(X)$,

$$= \sum_{ij:i+j\geq r} \tilde{q}_{ij}X^iX^jg(X)^j$$

$$= \sum_{ij:i+j\geq r} \tilde{q}_{ij}X^{i+j}g(X)^j$$

Since $i+j \geq r$, each monomial is divisible by X^r. Hence $X^r|R(X+\alpha)$. □