Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 41: Parvaresh-Vardy List Decoder

December 5, 2007

Lecturer: Atri Rudra *Scribe: Nathan Russell*

1 Recap

We recall from the last lecture that a folded Reed-Solomon code begins with a normal RS code, which is a $[n = q - 1, k]_q$-code with codewords of the form $[f(1)], [f(\gamma)], [f(\gamma^2)], \ldots, [f(\gamma^{n-1})]$ These are then combined into groups of m symbols which each become a new symbol, so that the codeword becomes something of the form $[f(1), f(\gamma), \ldots, f(\gamma^{m-1})], [f(\gamma^m), f(\gamma^{m+1}) \ldots, f(\gamma^{2m-1})], \ldots, [f(\gamma^{n-}$ We assume for the moment that m evenly divides n, though this assumption will prove unnecessary.

Thus we have the new parameters $K = \frac{k}{m}$ and $N = \frac{n}{m}$, so that the rate remains the same. We end up with a FRS code $\text{FRS}_{K,N,\mathbb{F},\gamma}$. We will present everything for $m = 2$, but it proves to work for any m.

2 List Decoding

In defining the list decoding problem, we will take as input $(\alpha_i, y_i, z_i)|_{i=1}^{N} \in \mathbb{F}^3$ and a so-called "agreement parameter" $t \geq 0$. The output will be all degree $\leq K$ polynomials $f(X)$ such that the FRS codeword corresponding to $f(X)$ agrees with the received word in at least t places. The algorithm we will use is as follows:

1. **Step 1:** Compute a non-zero $Q(X, Y, Z)$ of $(1, K, R)$-weighted degree at most D such that it has $r \geq 0$ roots at $Q(\alpha_i, y_i, z_i)$ for some $1 \leq i \leq N$.

2. **Step 2:** Recover $f(X)$ from $Q(X, Y, Z)$ such that it has the required properties.

At this point, we need a few definitions:

Definition 2.1. *$(1, k, k)$-weighted degree of a monomial $X^i Y^{ji} Z^{jl}$ is $i + kj + kjl$. ATRI:Changed the last constant from z in my notes to l to reduce confusion -N*

Definition 2.2. *$Q(X, Y, Z)$ having r roots at $(\alpha, \beta_1, \beta_2)$ implies that $Q(X + \alpha, Y + \beta_1, Z + \beta_2$ has no monomial of degree less than r.*

In Step 1, we need that the number of coefficients is greater than the number of constraints. There are $N\binom{r+2}{3}$ constraints, and $|\{(i, j_1, j_2)|i + kj_1 + kj_2 \leq D\}| \geq \frac{D^3}{Gk^2}$ coefficients.

The range of (i, j_1, j_2) is a series of intervals $[i, i+1) \times [j_1, j_1+1) \times [j_2, j_2+1)$. The volume of this cuboid $C(i, j_1, j_2)$ is 1, since all its edges are of length 1. We define $N_3(k)$ to be the volume of the union of cuboids such that $i + kj_1 + kj_2 \leq D$ with $i, j_1, j_2 \in \mathbb{Z}^{\geq 0}$.

We note that this volume is at least the volume of of the cuboid $\{f(i, j_1, j_2) | i + (j_1 + j_2)k \leq D\}, i, j_1, j_2 \in \mathbb{R}^{\geq 0}$, which can be shown (leaving the proof as an exercise) to be $\geq \frac{D^3}{GR^2}$. The former volume can be thought of as a union of squares, each over intervals $[i, i+1) \times [j_1, j_1+1)$.

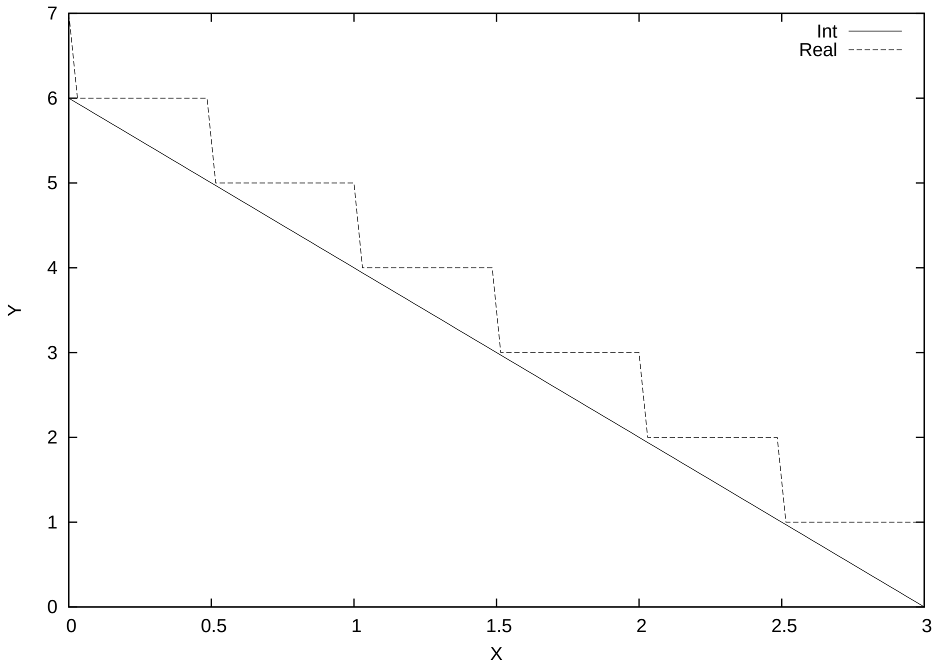

Figure 1: Real vs. integer volumes

For example, see the plot above, where the area containing the reals summing to 6 is less than that containing the integers summing to 7.

We choose D to be $\lceil \sqrt[3]{NR^2 r(r+1)(r+2)} \rceil + 1$ for $m = 2$. For general m, D is $\lceil \sqrt[m+1]{NK^m r(r+1)(r+2)} \rceil +$ 1.

At this point, we require a lemma.

Lemma 2.3. *If $tr > D$, then if $f(X)$ needs to be output then there exists a polynomial time algorithm to extract such $f(X)$'s from $Q(X, Y, Z)$.*

Assuming the above lemma, we have that $t > \sqrt[3]{K^2(i + \frac{1}{r})(1 + \frac{2}{r}) + \frac{2}{r}}$.

Since $t > \sqrt[3]{NR^2} + 1$ by suitable choice of r, we get $1 - \sqrt[3]{\frac{K^2}{N^2}} + \frac{1}{N}$.

This gives us that, since the number of errors is $N - t$, the fraction of errors is $\leq \sqrt[3]{\frac{K^2}{N^{@}}(1 + \frac{1}{r})(1 + \frac{2}{r}) + \frac{2}{r}} = 1 - (1+\delta)^3 \sqrt{\frac{R^2}{N^2}}$. By choosing a suitable r, with $r = O(\frac{1}{r})$, we end up showing that the bound on fraction of errors is $1 - (1+\delta)^3 \sqrt{4R^3}$.

We recall again that $N = \frac{n}{2}$ and so $R = \frac{K}{N} = \frac{\frac{k}{2}}{\frac{n}{2}} = \frac{k}{n}$. (ATRI: This is off to the side in my notes, ot sure where it goes -N)

For general m, we get $1 - \sqrt[m+1]{(mR)^m}$, as shown by Paravesh and Vardy in 2005.

Remarks:

1. This method is not useful for $R \geq 1$.
2. For $R \leq \frac{1}{16}$, $1 - \sqrt[3]{4R^2} > 1 - \sqrt{R}$.
3. Choosing m appropriately, we can correct $1-\varepsilon$ fraction of errors. We can get $R = O\left(\frac{\varepsilon^2}{\log\frac{1}{\varepsilon}}\right)$, recalling that at capacity $R = \Omega(\varepsilon^2)$, and Reed-Solomon codes gave us $R = \Omega(\varepsilon^2)$.

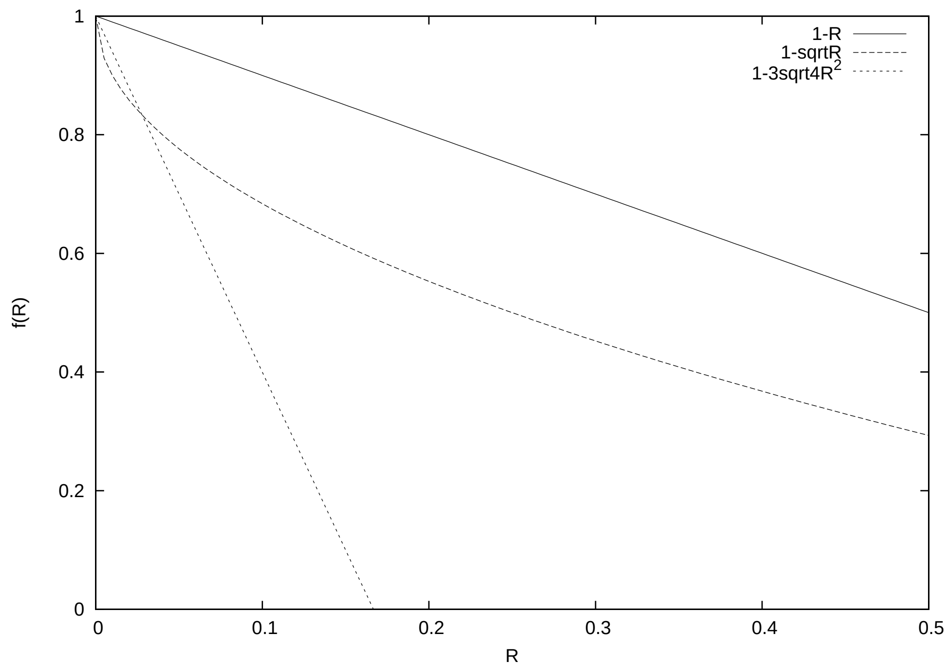

Figure 2: The values in point 2 plotted against each other

GRAPH GOES HERE

To show Lemma 2.3, we need another lemma:

Lemma 2.4. *There exists an irreducible polynomial $E(X)$ of degree $q-1$ such that $f(X)^q mod E(X) \equiv f(\gamma X)$ for any f of degree $< q-1$.*

We will show this second lemma in the next lecture.

Proof of Lemma 2.3: Let $Q_0(X, Y, Z)$ be such that $Q(X, Y, Z) = E(X)^b Q_0(X, Y, Z)$ for the largest possible integer b. That is, $E(X)$ doesn't divide Q_0 because not all coefficients are divisible by it.

We can consider $Q_0(X,Y,Z) = T_0(X,Y,Z)$, thinking of the coefficients as being chosen from $\mathbb{F}_q(X)$.

As an example of this sort of factorizatin, we can consider starting with something like $X^2Y + XY+Y^2Z$ and factor out the biggest polynomial over X, getting $Y(X^2+X)+Y^2Z$. We know that, since $E(X)$ is irreducible, $\mathbb{F}_q[X]/E(X) \equiv \mathbb{F}_{q^{a-1}}$. This means that $T(Y,Z) \triangleq T_0(Y,Z) mod E(X)$. We note that $T(Y,Z) \not\equiv 0$ as $E(X)$ doesn't divide $Q_0(X,Y,Z)$. Also, $Q(\alpha_i, y_i, z_i) = 0 \Leftrightarrow Q_0(\alpha_i, y_i, z_i) = 0$. Finally, $R(X) = Q_0(X, f(X), f(\gamma X)) = g(X)$.

Consider $T(f(X), f(\gamma X))$. If we compute $f(X)$ from this, then $f(X) \in \mathbb{F}_{q^{a-1}}$ and $f(\gamma X) = f(X)^a \mod E(X)$. We want all $Y \in \mathbb{F}_{q^{a-1}}$ such that $T(Y, Y^a) = 0$ and $R(Y) \triangleq T(Y, Y^a)$. We will show later the reason for the former restriction on Y.

We will additionally show that, if $f(X)$ needs to be output, then $T(f(X), f(\gamma X)) = 0 \equiv T(f(X), f(X)^a) = 0$.

Note that we need to find all roots of $R(Y)$ over $\mathbb{F}_{q^{a-1}}$. This can be done in polynomial time, as shown by Berlekamp.