

Lecture 38: Guruswami-Sudan List Decoder

November 11, 2007

Lecturer: Atri Rudra

Scribe: Sandipan Kundu

1 General Structure of RS list decoder

Given (α_1, y_i) in \mathbb{F}_2^d

Step1: Find a non-zero $Q(X, Y)$ [with restrictions] s.t. $Q(\alpha_i, y_i) = 0, 1 \leq i \leq n$

Step2: Factorize a non-zero $Q(X, Y)$ and output $P(X, Y)$ if

- $Y - P(X)$ is a factor of $Q(X, Y)$
- $\deg(P) \leq k$
- $P(\alpha_i) = y_i$ for $\geq t$ values of i .

Recap : $\deg_x(Q) \leq \sqrt{nk}, \deg_y(Q) \leq \sqrt{\frac{n}{k}} \Rightarrow \geq 2\sqrt{nk}$

Rate $R, 1 - 2\sqrt{R}$ fraction of errors ($> \frac{1-R}{2}$ for $R < 0.07$). Still far from Johnson bound $1 - \sqrt{R}$.

1.1 Algorithm 2 (Developed Sudan'95)

For proving Step 2, $R(X) \triangleq Q(X, P(X))$

$R(X) \triangleq Q(X, P(X))$.

$\deg(R) \leq \deg_x(Q) + k\deg_y(Q)$ Problem is the maximum degree might not occur at the same time. Hence, more stricter restriction of the polynomial is being imposed.

Definition 1.1. Def: $(1, k)$ weighted degree of $X^i Y^j = i + kj$ $(1, k)$ weighted degree of $Q(X, Y) = \max(1, k)$ - degree of its monomials.

$$Q(X, Y) \triangleq \sum_{\substack{i+kj \leq D \\ i, j \geq 0}} q_{i,j} X^i Y^j$$

Restriction in Step 1 : $(1, k)$ weighted degree of $Q(X, Y) \leq D$

Step 1: Number of coefficients of $Q(X, Y) > n$.

Step 2: $R(X) \triangleq Q(X, P(X))$ Wants to show $R(X) \equiv 0$. $R(\alpha_i) = Q(\alpha_i, y_i) = 0$ if $P(\alpha_i) = y_i, 1 \leq i \leq n$,

implying t roots.

$\deg(R) \leq D$ If $t > D$ then the proof is complete as we showed more roots than degree, hence $R(X) \equiv 0$. Number of coefficients = $N = |\{(i, j) | i + kj \leq D, i, j \in \mathbb{Z}^+\}|$

To know the number of coefficients we have to know the maximum value of j .

$$\begin{aligned}
N &= \sum_{j=1}^{\lfloor \frac{D}{k} \rfloor} \sum_{i=0}^{D-kj} 1 \\
&= \sum_{j=0}^l (D - kj + 1) \\
&= \sum_{j=0}^l (D + 1) - k \sum_{j=0}^l j \\
&= (D + 1)(l + 1) - \frac{kl(l + 1)}{2} \\
&= \frac{l + 1}{2} [2D + 2 - kl] \\
&\geq \left(\frac{l + 1}{2}\right)(D + 2) \tag{1} \\
&\geq \frac{D(D + 2)}{2k} \tag{2}
\end{aligned}$$

The first inequality in (1) is obtained by using $l \leq \frac{D}{k}$ and the second inequality in (2) is obtained by using $\frac{D}{k} - 1 \leq l$.

Step 1 is done if $\frac{D(D+2)}{2k} > n$. With $D = \lceil \sqrt{2kn} \rceil$ suffices by the following argument.

$$\frac{D(D + 2)}{2k} > \frac{D^2}{2k} \geq \frac{2kn}{2k} = n \tag{3}$$

Step 2: $t > \lceil \sqrt{2kn} \rceil$, $\frac{t}{n} > 1 - \sqrt{2R} > \frac{1-R}{2}$ for $R < \frac{1}{3}$

1.2 Algorithm 3 (Developed Guruswami, Sudan'98)

The main goal of the algorithm is to correct $1 - \sqrt{R}$ fraction of errors. Idea: Add more restriction on $Q(X, Y)$ in addition to $(1, k)$ -degree $\leq D$. Change number of constraints.

- Increase in number of constraints, but the number of coefficients remains the same.
- Gain: Increase in the number of roots of $R(X)$.

Let $r \geq 1$ be a parameter. Constraint : $Q(X, Y)$ has r roots at (α_i, y_i) , $1 \leq i \leq n$.

Intuitive example:

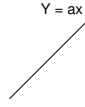


Fig 1.

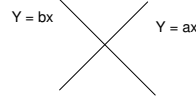


Fig 2.

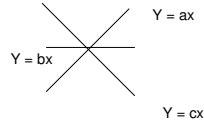


Fig 3.

For Fig.(1) $Q(X, Y) = Y - aX$. It has no term of degree 0

For Fig.(2) $Q(X, Y) = (Y - aX)(Y - bX)$. It has no term of degree ≤ 1 .

For Fig.(3) $Q(X, Y) = (Y - aX)(Y - bX)(Y - cX)$. It has no term of degree ≤ 2 .

Generalization : r line through origin, implies no monomials of degree $\leq r$

Definition 1.2. $Q(X, Y)$ has r roots at $(0, 0)$ if $Q(X, Y)$ doesn't have any monomial of degree r .

Definition 1.3. $Q(X, Y)$ has r roots at (α, β) if $Q_{\alpha, \beta}(X, Y) \triangleq Q(x + \alpha, y + \beta)$ have r roots at $(0, 0)$.

Step1: $Q(X, Y)$ has $(1, k)$ weight degree $\leq D$ and $Q(X, Y)$ has r root at (α_i, y_i) , $1 \leq i \leq n$

Lemma 1.4. Step1 implies $\binom{r+1}{2}$ for each i (over coefficient of $Q(X, Y)$)

Lemma 1.5. $R(X) \triangleq Q(X, P(X))$ r roots at every i such that $P(\alpha_i) = y_i$. $R(X)$ is divided by $(x - r_i)^r$.

Number of coefficient $\geq \frac{D(D+2)}{2k} > n \binom{r+1}{2} \frac{nr(r-1)}{2}$.

For $D = \lceil \sqrt{(knr(r-1))} \rceil$.

$$tr > D$$

$$t > \frac{D}{r} \tag{4}$$

$$= \lceil \sqrt{kn(1 - \frac{1}{r})} \rceil \tag{5}$$

tr number of roots by $R(X)$ by using (1.5). Let's pick $r = 2kn$, $\Rightarrow t > \lceil \sqrt{kn - \frac{1}{2}} \rceil > \lceil \sqrt{kn} \rceil$. The last inequality is because of t being an integer. The stated lemmas will be proved in the next lecture.