Today
- List decoding of Reed-Solomon Codes

[Sudan 96
Guruswami-Sudan 98]

CS3.318.1
Coding Theory
Lecture 16 (2022-10-26)
Instructor: Prahladh Harsha.

Efficient List-decoding of the Reed-Solomon Code.

Problem:

Input: $\mathbb{F}$ - finite field

n - # evaluations

k - degree parameter ($\deg < k$)

t - agreement parameter ($e = n - t$ # errors)

$\alpha_1, \ldots \alpha_n$ - n distinct points in $\mathbb{F}$

$\beta_1, \ldots \beta_n$ - n field elements.

Output: Find all poly $P[x] \in \mathbb{F}_{<k}[x]$ of $\deg < k$ s.t

$$\#\{i \in [n] \mid P(\alpha_i) = \beta_i\} \geq t.$$

Question: Find efficient alg for above problems w/ as low t as possible.

Observations: $t > \frac{n+k}{2}$ - Unique-decoding Radius
Welch-Berlekamp

$t > \sqrt{nk}$ - Johnson Radius.
(combinatorially)

Today: Sudan '96 $t > \sqrt{2kn}$ $(\rho < 1-\sqrt{2R})$

Guruswami - Sudan '98 $t > \sqrt{kn}$. $(\rho < 1-\sqrt{R})$.

Recall the Welch-Berlekamp Unique-decoding Alg:

Step 1: Find all non-zero pairs of polynomial (N, E) s.t

$$\deg(N) \leq t+k-1$$
$$\deg(E) \leq t.$$
$$N(\alpha_i) = \beta_i \cdot E(\alpha_i) \quad \forall i \in [n]$$

Step 2: Output N/E

$$Q(X,Y) = N(X) - Y E(X)$$

Every P that has agreement $> \frac{n+k}{2}$ satisfies
$$Q(X, P(X)) \equiv 0$$
ie, $(Y - P(X))$ is a factor of $Q(X,Y)$

Sudan's Generalization.

Step 1: Find an "algebraic" explanation for the data points in the form of a bivariate poly $Q(X,Y)$

Step 2: Output all factors $(Y - P(X))$ of $Q(X,Y)$

— Step 2: requires efficient factorization algorithms for bivariate polynomials over finite fields

Such algorithms exist [Kaltofen, Berlekamp]

Assume as blackbox such algorithms

Sudan's Algorithm (First attempt)

Parameter – $n \geq k \geq 1$, t – agreement parameter

ℓ

Step 1: Find a non-zero polynomial $Q(X,Y)$ s.t

$\deg_X(Q) \leq \ell$

$\deg_Y(Q) \leq n/\ell$

$Q(\alpha_i, \beta_i) = 0 \quad \forall\, i \in [n]$.

Step 2: Find all poly $P(X) \in \mathbb{F}[X]$ s.t

$(Y - P(X))$ is a factor of $Q(X,Y)$

and output list of all such P s.t

(i) $\deg_X(P) < k$

(ii) $|\{i \in [n] \mid P(\alpha_i) = \beta_i\}| \geq t$.

Requirements:

(1) Can find a nonzero soln by interpolation for any input data set.

(2) Every P that has agreement at least t w/ data must appear as a factor $(Y - P(X))$ of $Q(X, Y)$.

(1) Interpolation Requirements

Non-zero Soln exists if

$$\#\text{ vars} > \#\text{ eqns}$$

$\#\text{vars} = \#$ monomial $x^i y^j$ s.t. $0 \le i \le \ell$ and $j \le \frac{n}{\ell}$

$= (\ell+1)\left(\frac{n}{\ell}+1\right)$

$\#\text{ eqns} = n$

Since $(\ell+1)\left(\frac{n}{\ell}+1\right) > n \quad \forall \ell.$

a non-zero solution exists.

Claim: If $t > \ell + (k-1)\frac{n}{\ell}$, then the following is true

$P(x)$ satisfies $\#\{i \in [n] \mid P(\alpha_i) = \beta_i\} \geq t$

$$\Downarrow$$

$$Q(x, P(x)) \equiv 0.$$

Pf: $R(x) = Q(x, P(x))$

If $P(\alpha_i) = \beta_i$ (ie point of agreement)

then $R(\alpha_i) = 0$

Hence, $\prod_{i : P(\alpha_i) = \beta_i} (X - \alpha_i)$ is a factor of $R(x)$.

$\deg(R) \leq \ell + (k-1)\frac{n}{\ell}.$

So if $t > \ell + (k-1)\frac{n}{\ell}$, $R \equiv 0$ $\boxtimes$

Set $\ell = \sqrt{n(k-1)}$; $t > 2\sqrt{n(k-1)}$

Thm: Can list-decode if # agr $> 2\sqrt{n(k-1)}$

—

Balance the imbalance in X & Y-degrees.

(a,b)-weighted degree of $X^i Y^j = ai + bj$

$D :=$ $(1, k-1)$-weighted degree of Q

If $t > D$ then $Q(X, P(X)) \equiv 0$ for every P of agreement at least t.

Sudan's Algorithm (Second attempt)

Parameter - $n \geq k \geq 1$, t - agreement parameter

D

Step 1: Find a non-zero polynomial $Q(X,Y)$ s.t

$(1, k-1)$-weighted deg of $Q \leq D$

$Q(\alpha_i, \beta_i) = 0 \quad \forall i \in [n]$

Step 2: Find all poly $P(X) \in \mathbb{F}[X]$ s.t

$(Y - P(X))$ is a factor of $Q(X,Y)$ and output list of all such P s.t.

(i) $\deg_X(P) < k$

(ii) $|\{i \in [n] \mid P(\alpha_i) = \beta_i\}| \geq t$.

Step 2 Requirements: $D > t$

Step 1 (interpolation) Requirements:

$$\#\text{eqns} = n.$$

$$\#\text{vars} = |\{(i,j) \mid 0 \leq i,j,\ i + (k-1)j \leq D\}|$$

$$= \sum_{j=0}^{\ell} \sum_{i=0}^{D-(k-1)j} 1 \qquad \ell = \left\lfloor \frac{D}{k-1} \right\rfloor$$

$$= \sum_{j=0}^{\ell} [D + 1 - (k-1)j]$$

$$= (D+1)(\ell+1) - (k-1)\sum_{j=0}^{\ell} j$$

$$= (D+1)(\ell+1) - (k-1)\frac{\ell(\ell+1)}{2}$$

$$= \frac{(\ell+1)}{2}\left[2D + 2 - (k-1)\ell\right]$$

$$\geq \frac{\ell+1}{2}(D+2) \qquad \left(\text{since } \ell \leq \frac{D}{k-1}\right)$$

$$\geq \frac{D(D+2)}{2(k-1)} \qquad \left(\text{since } \ell \geq \frac{D}{k-1} - 1\right)$$

If we choose D s.t $\frac{D(D+2)}{2(k-1)} > n$ then

Interpolation conditions are met

Set $D = \lceil \sqrt{2(k-1)n} \rceil$

$t = \lceil \sqrt{2(k-1)n}. \rceil$

Thm [Sudan] Can efficiently list-decode RS code w/ # agreements $\geq \lceil \sqrt{2(k-1)n} \rceil$

(ie, $\rho > 1 - \sqrt{2R}$)

Guruswami - Sudan Improvement:

Idea: Incorporate multiplicities.

① Step 1: Adding more restrictions

ie, $Q(X,Y)$ has "r roots" at (α_i, β_i)

eqns are increasing $\Rightarrow$ D must be larger

② Every pt of agreement given "r roots" of $R(X) = Q(X, P(X))$.

$rt > D$

Defn. (1) $Q(X,Y)$ has r roots at $(0,0)$ if coeffts of $X^i Y^j$ for any (i,j) satisfying $i+j < r$ is zero.

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

Guruswami - Sudan Algorithm.

Parameter - $n \geq k \geq 1$, t - agreement parameter
D , r

Step 1: Find a non-zero polynomial $Q(X,Y)$ s.t
$(1, k-1)$-weighted degree of $Q \leq D$
$Q(X,Y)$ has r roots at (α_i, β_i), $\forall i \in [n]$

Step 2: Find all poly $P(x) \in \mathbb{F}[X]$ s.t
$(Y - P(X))$ is a factor of $Q(X,Y)$
and output list of all such P s.t
(i) $\deg_X(P) < k$
(ii) $|\{i \in [n] \mid P(\alpha_i) = \beta_i\}| \geq t$.

Step 1 Requirements: $\#\text{vars} > \dfrac{D(D+2)}{2(k-1)}$

$\#\text{eqns} = n \cdot \#\{(i,j) \mid 0 \leq i,j, \ i+j < r\}$
$= n \cdot \binom{r+1}{2}$.

$$\frac{D(D+2)}{2(k-1)} > n\binom{r+1}{2}$$

Set $D = \left\lceil \sqrt{(k-1)\, n\, r(r-1)} \right\rceil$ to satisfy interpolation requirements

Claim: If $D < tr$, and P has $\geq t$ agreements w/ data, then $R(x) = Q(x, P(x)) \equiv 0$.

$t > \frac{D}{r}$; $D = \left\lceil \sqrt{(k-1)\, n\, r\, (r-1)} \right\rceil$

$t = \left\lceil \sqrt{(k-1)\, n \left(1 - \frac{1}{r}\right)} \right\rceil$

Set $r = 2(k-1)n$, $t > \left\lceil \sqrt{(k-1)n - \frac{1}{2}} \right\rceil > \sqrt{(k-1)n}$

Thm [Guruswami-Sudan] Can list-decode RS codes if # agreements $\geq \sqrt{(k-1)n}$ (i.e. $\rho \geq 1 - \sqrt{R}$)

Proof of Claim:

Suppose we show

For every point of agreement (i.e., $P(\alpha) = \beta$) we have $(x-\alpha)^r$ is a factor of $R(x) = Q(x, P(x))$.

then we are done.

Special case when $(\alpha, \beta) = (0, 0)$

Since $P(\alpha) = \beta$; constant term of $P(x)$ is 0.

$$R(x) = Q(x, P(x)) = Q(x, ax + \dots)$$

least deg term in $R \geq r$.

ie, $x^r / R(x)$ in this case.

General (α, β), $(x-\alpha)^r / R(x)$. $\boxtimes$.