ICTS HDX and Codes

Coding

Lecturer: Mrinal Kumar

Abhinav

Lec - 2

28/04

$\mathbb{F}_q$, $q = n$, $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

$$\mathcal{C} = \left\{ (p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_n)) : \begin{array}{l} p \in \mathbb{F}_q[x] \\ \deg(p) \leq k \end{array} \right\}$$

$\Delta = n - k$

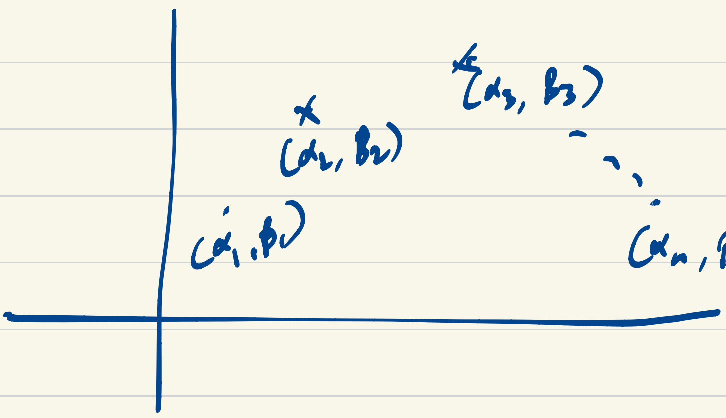
$\#$ errors $< \frac{n-k}{2}$

Berlekamp-Welch Decoder

I/P : $r = (\beta_1, \beta_2, \ldots, \beta_n)$
s.t. $\exists\, c \in RS(n,k)$ s.t. $\Delta(r, c) < \frac{n-k}{2}$

O/P: Find c/p

Noisy univariate polynomial interpolation



No errors: $Q_0(X,Y) = Y - p(X)$, $Q_0(\alpha_i, \beta_i) = 0 \;\; \forall i$

1 error: $Q_1(X,Y) = Q_0(X,Y)(X - \alpha_{17})$ error point

$$Q_2(X,Y) = Q_0(X,Y) \underbrace{\prod_{i : i \text{ is an error}} (X - \alpha_i)}^{E(X)}$$

$$Q_2 = (Y - P(x)) \cdot E(x)$$
$$= Y \cdot E(x) - P(x) \cdot E(x)$$

For eg $Q_2 = Y \cdot A(x) + B(x)$

$P = -B/A$

Insight : 1) Any 'low deg' non-zero $Q(x, y)$ that vanishes on $(\alpha_i, \beta_i)_{i=1}^{n}$ contains in its belly information about 'close enough' codewords

2) Moreover, all these codewords can be recovered efficiently.

Algorithm :

1) Interpolation step : Find a non-zero $Q(x, y) := Y \cdot A(x) + B(x)$

s.t. 1) $\forall i \; Q(\alpha_i, \beta_i) = 0$ } Linear system

2) $\deg(A) \leq \frac{n-k}{2}$

3) $\deg(B) \leq \frac{n+k}{2}$

2) Output $-B/A$

$$A(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{\frac{n-k}{2}} x^{\frac{n-k}{2}}$$

$$B(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_{\frac{n+k}{2}} x^{\frac{n+k}{2}}$$

$Q(\alpha_i, \beta_i) = 0 \equiv A(\alpha_i)\beta_i + B(\alpha_i) = 0$

$$\left(\sum_j a_j \alpha_i^j\right)\beta_i + \sum_j b_j \alpha_i^j = 0$$ Linear system

\# constraints : n

\# variables $= \frac{n-k}{2} + 1 + \frac{n+k}{2} + 1 = n+2$

Lemma: Let $Q(x,y)$ be any non-zero poly from interpolation step.
Let $p(x) \in \mathbb{F}_q[x]$, $\deg \leq k$ be st $\Delta(r, p) < \frac{n-k}{2}$

then $p = -B/A$

Proof:

$R(x) = Q(x, p(x)) = A(x) \cdot p(x) + B(x)$

$\deg(R) \leq \frac{n+k}{2}$

If $p(\alpha_i) = \beta_i$, then $R(\alpha_i) = 0$

$R(\alpha_i) = Q(\alpha_i, \beta_i) = 0$

At every point of agreement between p and r, $R(x)$ has a zero.

If \# agreements $\geq \frac{n+k}{2} \Rightarrow R(x) \equiv 0$

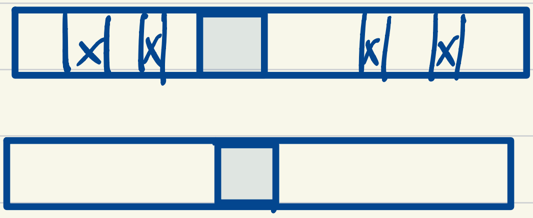
$\Rightarrow A \cdot p + B = 0$

$\Rightarrow p = \frac{-B}{A}$

Locally Decodable Codes

r :

c :



i

Find c_i.

Def: Code $\mathcal{C}$ is said to be a (t, ε) locally decodable code if there is an algorithm A that for every $r \in \Sigma^n$, $c \in \mathcal{C}$, $i \in [n]$ satisfies the following:

1) If $\Delta(r, c) < \varepsilon n$, then A outputs c_i with probability 0.9.
2) A only queries at most t locations of r.

Reed-Muller Codes

m - # variables
k - total degree
$\mathbb{F}_q$

$\Big\}\ k < 0.1q$

$$RM(m, k, q) = \{ (p(a))_{a \in \mathbb{F}_q^m} : p \in \mathbb{F}_q[x_1 \ldots x_m],\ \text{total deg} < k \}$$

Rate: $\dfrac{\binom{m+k}{k}}{q^m}$ $\left(\text{if } m = O(1),\ \approx \dfrac{k^m}{m!\, q^m} \right)$

Schwartz - Zippel lemma

zeros of a non-zero deg k, m-variate polynomial in $\mathbb{F}_q^m \le k \cdot q^{m-1}$

Distance $= (q-k)q^{m-1}$

Lec. 4

Local decoding of RM codes

$$RM(k,m) = \{ (P(a))_{a \in \mathbb{F}_q^m} \mid P \in \mathbb{F}_q[x_1 \ldots x_m], \deg(P) \le k \}$$

I/P: $f : \mathbb{F}_q^m \to \mathbb{F}_q$, $\alpha \in \mathbb{F}_q^m$

f is ε-close to $RM(k,m)$, let P be the closest codeword.

O/P: $P(\alpha)$, want the algorithm to query f on at most t-locations

Thm:

1) For $k \le q-2$, $RM(k,m)$ is $\left(q-1, \frac{1}{100q}\right)$-LDC.

2) For $k \le q/2$, $RM(k,m)$ is $\left(q-1, \frac{1}{100}\right)$-LDC.

f

x		x	$f(\alpha)$			x
			α			

P

x		'	x			
			α			

$P(x_1 \ldots x_m)$, deg k poly.

$L_{a,b} = \{ a + bt \mid t \in \mathbb{F}_q \}$ $a, b \in \mathbb{F}_q^m$

$|L_{a,b}| = q$, $P(a+bt) = P(a_1 + b_1 t, a_2 + b_2 t, \ldots, a_m + b_m t)$

$R(T) = P(a + bT) = P(a_1 + b_1 T,\ a_2 + b_2 T,\ \ldots,\ a_m + b_m T)$

$\deg(R) \leq \deg(P) = k$

$|L_{a,b}| = q > k$

Have access to q-evaluations of R.
Since $q > \deg(R)$, can reconstruct R uniquely from these evaluations.

<u>Algorithm</u>: $\qquad b \in \mathbb{F}_q^m \setminus \{0\}$

0) Pick a $b \in \mathbb{F}_q^m$ u.a.r.

1) Find the unique deg k univariate $R(T)$ s.t.
$\forall\ t \in \mathbb{F}_q^*$, $R(t) = f(\alpha + bt)$

2) Output $R(0) = P(\alpha + b \cdot 0)$

<u>Obs 1</u>: If P and f agree on all points on the line $L_{\alpha,b} \setminus \{\alpha\}$, then the algorithm correctly outputs $P(\alpha)$.

<u>Claim</u>: If f and P agree on $\left(1 - \frac{1}{10q}\right)$ fraction of points

then $\Pr_b [f, P \text{ agree on } L_{\alpha,b} \setminus \{\alpha\}] \geq 0.9$.

<u>Obs</u>: For any fixed $t \in \mathbb{F}_q^*$

$$\Pr_b [f(\alpha + bt) \neq P(\alpha + bt)] = \frac{1}{10q}$$

Obs: $\Pr_b\left[\exists\, t \in \mathbb{F}_q^+ \text{ st } f(x+bt) \neq P(x+bt)\right] \leq (q-1)\frac{1}{100q} \leq \frac{1}{100}$

For 2):

Use Berlekamp-Welch for step 1) of the algorithm

Local Testing of RM codes

We want an algorithm that distinguishes if a given $f: \mathbb{F}_q^m \to \mathbb{F}_q$ is a Reed-Muller codeword OR it is far from all the codewords.

$m = 3$

Test:

1) Pick a plane π in $\mathbb{F}_q^3$ u.a.r

2) If $f|_\pi$ is a deg k bivariate, then accept
else reject.

Theorem [Raz-Safra baby version]

For all small enough constants ϵ, finite field $\mathbb{F}_q$. If $k < \epsilon q$ and the test passes with prob $1-\epsilon$, then $\exists$ degree k trivariate $P(x,y,z)$ st.

$$\text{Agree}(f, P) \geq 1 - 10\epsilon$$

g_π : bivariate deg k poly equal to $f|_\pi$

Consistency of two planes:

Planes π, σ are consistent if g_π, g_σ agree on $\pi \cap \sigma$.

$$\Pr_{\pi,\sigma}[\pi \text{ and } \sigma \text{ are consistent}] \approx 1 - 2\varepsilon$$

1) There is a large $(1-10\varepsilon)$ subset $\mathcal{U}$ of planes that are all consistent with each other.

2) There is a deg k trivariate P s.t $\forall \pi \in \mathcal{U}$, $g_\pi = P|_\pi$.

Obs: P agrees with f on $(1-100\varepsilon)$ fraction of all points in $\mathbb{F}_q^n$.

$G(V,E)$

$V \rightarrow$ set of all planes in $\mathbb{F}_q^3$ $\qquad |V| \sim q^3$

$E \rightarrow \{(\pi,\sigma) \mid \pi \text{ and } \sigma \text{ are consistent}\}$

$$\Pr_{\pi,\sigma\in V}[(\pi,\sigma)\in E] = \Pr_{\pi,\sigma}[\pi \text{ and } \sigma \text{ are consistent}] = 1-10\varepsilon$$

Lemma 1: If $(\pi,\sigma) \notin E$, then at least one of π or σ must be inconsistent with at least $\frac{1}{2}(1-\frac{k}{q})$ fraction of all planes.

<u>Obs 2</u>: $\mathcal{U} = \{ \pi \mid \deg(\pi) > \frac{1}{2}(1 + \frac{k}{q}) \}$. Then $\mathcal{U}$ forms a clique in G_2

<u>Obs 3</u>: $|\mathcal{U}| \geq (1 - 10\varepsilon)|V|$

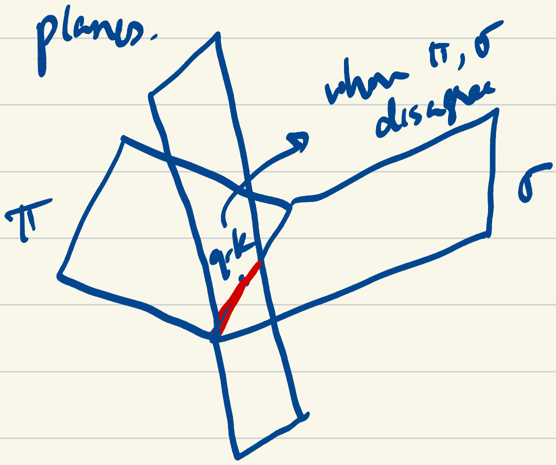
Lec-6

30/04

Lemma 1: G contains a clique of size $\geq (1 - 10\epsilon)|V|$

Claim: If π, σ are inconsistent, then at least one of them is inconsistent with $\frac{1}{2}(1 - \frac{k}{q} - o(1))|V|$ planes.

Proof:



No. of planes intersecting in those points

$\frac{q-k}{q}$

$U \subseteq V$, U forms a clique

$|U| \geq (1 - 10\epsilon)|V|$

Planes in General Position:

$\Pi_1, \Pi_2, \ldots, \Pi_t$ are said to be in general position if

1) Every pair intersects at a line
2) Every triplet intersects at a point
3) No four of them intersect.

Lemma 2: There exist $10\epsilon q$ planes in general position in U.

$\hat{U} \subseteq U$ in gen position $|\hat{U}| = 10\epsilon q$

Let U_0 be a subset of $\hat{U}$ s.t $|U_0| = k+3$

Lemma 3: $S = \{ \pi_i \cap \pi_j \cap \pi_\ell \mid \underbrace{\pi_i, \pi_j, \pi_\ell}_{\text{distinct}} \in U_0 \}$

Then, S is an interpolating set of 3-variate deg ℓ polynomials.

Equiv: for every $h : S \to \mathbb{F}$, $\overset{\text{unique}}{\exists}$ poly $P(x,y,z)$, deg k s.t $h(\alpha) = P(\alpha)$ $\forall \alpha \in S$

$$\underset{k+3}{U_0} \subseteq \underset{10\epsilon q}{\hat{U}} \subseteq \underset{(1-10\epsilon)q^3}{U}$$

Claim 1: $\forall \pi \in U_0$, $g_\pi = P|_\pi$

Proof: Consider $\{ \pi_i \cap \pi \mid \pi_i \in U_0 \setminus \{\pi\} \}$

- All these lines are in general position. - $k+2$ lines in G.P.

interpolating set for deg-k bivariate

- T = set of intersection of these lines

$|T| = \binom{k+2}{2}$ $\forall \alpha \in T$, $P(\alpha) = g_\pi(\alpha) = P|_\pi(\alpha)$

$$\Rightarrow g_\pi = P|_\pi$$

Claim 2: $\forall \pi \in \hat{U}$, $g_\pi = P|_\pi$ Same argument as above with more degrees of freedom

Claim 3: $\forall \pi \in U$, $g_\pi = P|_\pi$

Proof: Consider $\pi \in U$

Consider $L_\pi = \{ \pi \cap \pi_i \mid \pi_i \in \hat{U} \}$

$M_\pi =$ set of points on lines $\ell \in L_\pi$

<u>Obs</u>: $\forall \alpha \in M_\pi, \quad P|_\pi(\alpha) = g_\pi(\alpha)$

$$|L_\pi| \geq \frac{|\hat{U}|}{2} = 5\epsilon q$$

$$|M_\pi| \geq (5\epsilon q)q - \binom{5\epsilon q}{2} \cdot 1$$

$$= 5\epsilon q^2 - \frac{25}{2}\epsilon^2 q^2 \geq 4\epsilon q^2$$

By the SZ lemma,

if $P|_\pi$ and g_π are distinct, then

$\#$ pts of agreement $\leq kq \leq \epsilon q^2$

$\Rightarrow \quad g_\pi = P|_\pi$

<u>Lemma</u>: $\exists$ $10\epsilon q$ planes in gen. pos. in U,

1) Take a nice construction of such planes

2) Do a random rotation.

$$\Pi_{v,d} = \{ (a,b,c) \in \mathbb{F}_q^3 : av_1 + bv_2 + cv_3 = d \}$$

normal vector

$$v(\alpha) = (1, \alpha, \alpha^2) \quad d(\alpha) = \alpha^3$$

$$H(p) = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{(1-p)}$$

List Decoding

A code $C \subseteq \Sigma^n$ is (p,L)-list-decodable if $\forall\, a \in \Sigma^n$

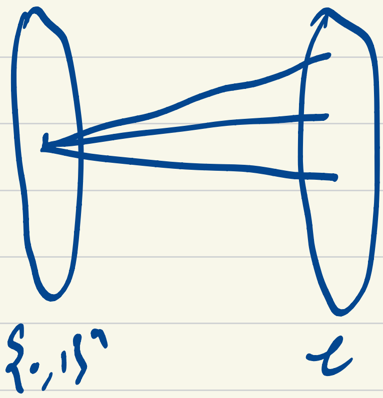
$$|B(a, pn) \cap C| \le L.$$

Thm: If $C \subseteq \{0,1\}^n$ is (p,L)-list-decodable, then

$$\text{Rate}(C) = 1 - H(p) + \frac{\log L}{n}$$

Thm: There exist (p,L)-list-decodable code $C \subseteq \{0,1\}^n$,

$$\text{Rate}(C) \ge 1 - H(p) - \frac{1}{L+1}$$



$\#$ edges $\le 2^n \cdot L$

$\#$ edges $= |C| \cdot B(pn)$

$$\Rightarrow \quad |C| \cdot B(pn) \le 2^n \cdot L$$

$$\Rightarrow \quad |C| \le \frac{2^n \cdot L}{B(pn)}$$

$\Rightarrow$ $\text{Rate} = \dfrac{\log_2 |C|}{n}$

$= \dfrac{n + \log(L) - \log_2(B(\beta n))}{n}$

$= \dfrac{n + \log(L) - H(\beta) n}{n}$

$= 1 - H(\beta) + \dfrac{\log(L)}{n}$

Lec-8

Theorem [Johnson]

If $\mathcal{C}$ is a code with rel. dist δ, then $\mathcal{C}$ is (ρ, L)-decodable for $\rho = 1-\sqrt{1-\delta}$, $L = O(n)$.

Eg: **Reed-Solomon Codes**

$k = 0.01\,n$

$\delta = 0.99$

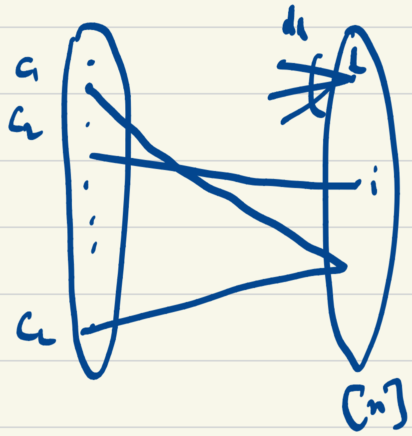
$\rho = 1-\sqrt{0.01}$

$= 1-0.1$

$= 0.9$

Proof: $x \in \Sigma^n$

$\Delta(x, c_i) \leq \rho n$



$c_j \sim i$ iff c_j and x agree on the ith coordinate

$$\deg(c_i) \geq (1-\rho)n$$

$$|N(c_i) \cap N(c_j)| \leq n(1-\delta)-1$$

Count $(\{c_i, c_j\}, l)$ where $c_i \sim l$ and $c_j \sim l$.

$$\# \text{ vees} \leq \binom{L}{2}(n(1-\delta)-1)$$

$$\# \text{ vees} = \sum_{l \in [n]} \binom{d_l}{2}$$

$$\Rightarrow \sum_l \binom{d_l}{2} \leq \binom{L}{2}\left(n(1-\delta)-1\right)$$

$$\sum_l d_l \geq L(1-\rho)n$$

$$\frac{\sum_l \binom{d_l}{2}}{n} \geq \binom{\frac{\sum_l d_l}{n}}{2}$$

$$\Rightarrow \binom{\frac{L(1-\rho)n}{n}}{2} \leq \binom{L}{2}\left(n(1-\delta)-1\right)$$

<u>Johnson Bound for RS Codes</u>

$$\rho = 1 - \sqrt{1-\delta} \qquad \Rightarrow \qquad \rho = 1 - \sqrt{k/n}$$

$$\delta = 1 - \frac{k}{n} \qquad \Rightarrow \qquad \rho n = n - \sqrt{kn}$$

$$= 0.9n$$

Theorem [Sudan, Guruswami-Sudan]

RS codes can be efficiently decoded up to the Johnson Bound.

Sudan - $n - \sqrt{2kn}$

Guruswami-Sudan - $n - \sqrt{kn}$

Berlekamp-Welch

1) Interpolation : Find a $Q(x,y) : A_0(x)y + A_1(x)$, non-zero, low-deg s.t $\forall i$, $Q(\alpha_i, \beta_i) = 0$

2) Output $P(x)$ s.t $Q(x, P(x)) = 0$

$\#$ agreements $\geq \max\limits_{P, \deg k} \deg(Q(x, P(x)))$

Sudan : Consider a Q of large Y. degree

$$Q = A_0(x) + A_1(x)X + A_2(x)X^2 + \dots + A_l(x)Y^l$$

$$Q(x, P(x)) = A_0 + A_1 P + A_2 P^2 + \dots + A_l P^l$$

$$\deg(Q(x, P(x))) \leq \max_i (\deg(A_i) + i.k)$$

$D \sim \sqrt{2kn}$

$\deg(A_i) : D - ik$

Algorithm 1

1) Find a non-zero $Q(x,y) = \sum_{i=0}^{l} A_i(x) \cdot y^i$ s.t.

a) $\deg(A_i) \leq D - ki$, b) $\forall j$, $Q(\alpha_j, \beta_j) = 0$

2) Output all deg k polys $P(x)$ s.t. $Q(x, P(x)) \equiv 0$

Step 2

Want $P(x)$ s.t. $Q(x, P(x)) \equiv 0$

$$\Leftrightarrow (y - P(x)) \mid Q(x,y)$$

Theorem:

There are efficient randomized algos for factoring bivariate polynomials over finite fields.

Claim 1: For $D \geq \sqrt{2kn}$, the linear system in step 1 has a non-zero solution $\left(l \sim \frac{D}{k} = \sqrt{2n/k}\right)$

Claim 2: If $P \in \mathbb{F}[x]$, $\deg \leq k$ s.t. $\text{agree}(P, (\alpha_i, \beta_i)_{i=1}^{n}) > \sqrt{2kn}$ then $Q(x, P(x)) \equiv 0$

Proof of Claim 1:

$\#$ constraints $= n$

$\#$ variables $= \sum_i \deg(A_i) + 1 = \sum_{i=0}^{D/k} (D - ki + 1)$

$> \frac{D^2}{2k}$

Proof of claim 2:

$R(x) := Q(x, P(x))$, $\deg(R) \leq D$

If $P(\alpha_j) = \beta_j$, then $R(\alpha_j) = Q(\alpha_j, P(\alpha_j))$
$= Q(\alpha_j, \beta_j)$
$= 0$

$\Rightarrow$ $\mathrm{Agree}(P, (\alpha_i, \beta_i)_{i=1}^{n}) > D$, then R has $> D$ roots.

$\Rightarrow$ $R \equiv 0$

Multiplicities: A polynomial $Q(x)$ vanishes with multiplicity $\geq s$ at a point α if all the (partial) derivatives of Q of order $< s$ vanish at α.

Fact: $P(x) \in \mathbb{F}[x]$, non-zero univariate then
$\sum_{\alpha \in \mathbb{F}} \mathrm{Multiplicity}(P, \alpha) \leq \deg(P)$

Guruswami - Sudan:

1) Find a non-zero low deg $Q(x,y)$ st $\mathrm{Mult}(Q, (\alpha_i, \beta_i)) \geq m$

2) Output all $P(x)$, deg k s.t. $Q(X, P(x)) \equiv 0$.

Claim: If $P(\alpha_j) = \beta_j$, then
$Q(X, P(X))$ vanishes with multiplicity $\geq m$ at α_j.

- Folded Reed-Solomon Codes
- Univariate Multiplicity Codes.