Today

Polynomial Method

- Schwartz-Zippel Lemma
- Combinatorial Nullstellensatz
- Frankl-Wilson Theorem

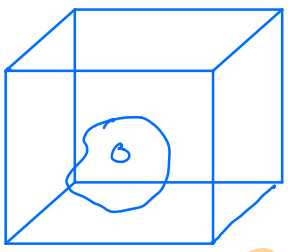
CSS.205.1
Toolkit in TCS
- Lecture #30
(7 June '21)
Instructor: Prahladh Harsha

Recap from last lecture.

Polynomial Identity Lemma (Schwartz-Zippel Lemma)

Let p be a non-zero m-variate poly of deg $\leq d$ over a field $\mathbb{F}$ & $S \subseteq \mathbb{F}$, then

$$\Pr_{(\alpha_1 \ldots \alpha_m) \leftarrow S^m} [p(\alpha_1 \ldots \alpha_m) = 0] \leq \frac{d}{|S|}$$



S^m

$p : S^m \to \mathbb{F}$

$p \neq 0$

Applications of Polynomial Identity Lemma (Schwartz-Zippel Lemma)

(1) Checking Matrix Multiplication

(2) Bipartite Matching.

Checking Matrix Multiplication

Problem: Given $A, B, C \in \mathbb{F}^{n \times n}$

Goal: Check if $C = AB$?

Can do if we do matrix multiplication

Cost

(1) $A \in \mathbb{F}^{n \times n}$; $v \in \mathbb{F}^{n \times 1}$;

Time to compute Av $= O(n^2)$

(2) $A, B \in \mathbb{F}^{n \times n}$

Time to compute $AB = O(n^3)$

$\Omega(n^2)$ = Cost of matrix mult $= O(n^{2.3728\ldots})$

$= n^{\omega}$

Conjecture: $\omega = 2$.

Qn: Is checking easier than matrix multiplication?

Yes. Randomized $O(n^2)$ verification alg (i.e. if $\omega > 2$)

Alg: Input A, B, C

1. Pick a random $v \in \mathbb{F}^n$ (S^n)
2. Check if $ABv = Cv$
   i.e. $A(Bv) = Cv$?
3. Output YES/NO according

Running Time: $\mathcal{O}(n^2)$

Correctness:

Case $AB = C$. Alg outputs YES

Case $AB \neq C$ $\quad D = AB - C \;;\; D \neq 0$

$D \neq 0$.

$$\Pr_v[Dv = 0] = \;?$$

$$D \begin{bmatrix} -D_1- \\ -D_2- \\ -D_n- \end{bmatrix} \qquad D \neq 0 \Rightarrow \exists\, i,\ D_i = 0$$

$$\Pr_v[Dv = 0] \leq \Pr_v[\langle D_i, v\rangle = 0]$$

$$= \Pr_v\left[\sum d_{ij} v_j = 0\right]$$

$$\leq \frac{1}{|S|} \qquad (\text{if } v \leftarrow S^n)$$

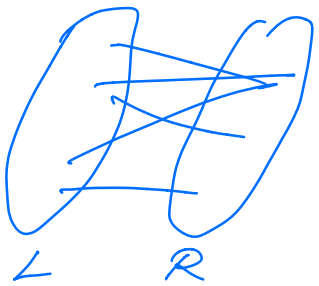
(Freivalds Algorithm)

(2) Bipartite matching

Problem: Input $G = (L, R, E)$

$|L| = |R| = n$

Question: Is there a perfect matching in G?



Bipartite Adj Matrix

$$A \begin{matrix} L \\ \\ \end{matrix} \overbrace{\begin{bmatrix} & a_{ij} & \end{bmatrix}}^{R}$$

$$a_{ij} = \begin{cases} 1 & \text{if } (i,j) \in E \\ 0 & \text{otherwise.} \end{cases}$$

$A(\bar{x})$ $\qquad \bar{x} = (x_e \mid e \in E)$

↳ $|E|$-dimensional vector.

$$= \begin{bmatrix} & x_{ij} & \end{bmatrix}$$

$$A(x)_{ij} = \begin{cases} x_{ij} & \text{if } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

$$\det(A(x)) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod A(x)_{i,\sigma(i)}$$

$$= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \mathbb{1}[\sigma \in E] \cdot \prod x_{i,\sigma(i)}$$

Obs: $\det(A(x))$ is a non-zero polynomial iff E has a perfect bipartite matching.

Alg: 0. Let $S \subseteq \mathbb{F}$ of size $100n$

1. Pick $b_{ij} \leftarrow S \subseteq \mathbb{F}$
2. Compute $A(\bar{b})$
3. If zero output no matching
   else output matching.

Correctness:

Case: G does not have a matching

$A(x) \equiv 0 \Rightarrow$ Alg always o/p's no matching.

Case: G has a perfect matching

$A(x) \not\equiv 0 \quad \because \deg(\det(A(x))) = n$

$$\Pr_{b \in S^{|E|}}\left[\det(A(b)) = 0\right] \leq \frac{n}{|S|} \leq \frac{1}{100}$$

$\boxtimes$

Combinatorial Nullstellensatz

Noga Alon

Thm Let $\mathbb{F}$ - field, $S_1 \dots S_n \subseteq \mathbb{F}$

$|S_i| = t_i + 1$,

$S_1 \times S_2 \dots \times S_n$: n-dimensional grid

$f \in \mathbb{F}[X_1 \dots X_n]$

- total deg $(f) = d = t_1 + t_2 + \dots + t_n$.

- Coeff of $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ is nonzero in f.

Then, there exists a $(a_1 \dots a_n) \in S_1 \times S_2 \dots \times S_n$ s.t $f(a_1 \dots a_n) \neq 0$.

Applications:

(1) Cauchy-Davenport Theorem.

p - prime

$\mathbb{F}_p = \{0, 1, 2, 3, \dots, p-1\}$ - finite field.

$A, B \subseteq \mathbb{F}_p$

$A + B = \{a + b \mid a \in A, b \in B\}$.

Qn: How large can $A+B$ be?

eg: $A = \{0, 1, \dots, a\}$ $(a+b < p)$

$B = \{0, 1, \dots, b\}$ $A+B = \{0, 1, \dots, a+b\}$

$$|A+B| = |A| + |B| - 1$$

Thm [Cauchy-Davenport]
p prime, $A, B \subseteq \mathbb{F}_p$

$$|A+B| \geq \min\{|A|+|B|-1, p\}$$

Pf:

Case(i) $|A|+|B| > p$

For any $x \in \mathbb{F}_p$, A, $x-B = \{x-b \mid b \in B\}$

$$|A| + |x-B| > p$$

$$\Rightarrow A \cap (x-B) \neq \emptyset$$

i.e., $\exists$ a $a \in A$ & $b \in B$ s.t

$$a+b = x$$

Hence, $A+B = \mathbb{F}_p$.

Case(ii) $|A| + |B| \leq p$.

For contradiction let us assume

$$|A+B| \leq |A| + |B| - 2 \leq p-2.$$

Let $C \supseteq A+B$ s.t $|C| = |A| + |B| - 2$

$$f(X,Y) = \prod_{c \in C} (X+Y-c)$$

$$\deg(f) = |C|$$

$$\text{Coeff of } X^{|A|-1} \cdot Y^{|B|-1} = \binom{|C|}{|A|-1}$$

$$= \binom{|A|+|B|-2}{|A|-1} \neq 0 \quad (\mathbb{F}_p)$$

Since $|A|+|B|-2 < p$

f on $A \times B$

$\exists\, a \in A,\ b \in B$ s.t. $f(a,b) \neq 0$

This contradicts that $A+B \subseteq C$.

Hence, $|A+B| \geq |A|+|B|-1$ ∎

---

(2) Covering Boolean hypercube w/ hyperplanes

$B = \{0,1\}^n \subseteq \mathbb{R}^n$

Hyperplane $\sum a_i x_i + b = 0$ $\quad -h$

Qn: How many hyperplanes are needed to cover B

ie, What is the min m s.t.

$\exists\ h_1 \ldots h_m$ - hyperplanes

$\forall x \in \{0,1\}^n$, $\exists i$, $h_i(x) = 0$

2: $x_1 = 0$; $x_1 = 1$ - Not interesting

Qn2: How many hyperplanes are needed to cover $B \setminus 0^n$

i.e, What is the min m s.t

$\exists\ h_1 \ldots h_m$ - hyperplanes

$\forall x \in \{0,1\}^n \setminus 0^n$, $\exists i$, $h_i(x) = 0$

& $\nexists i$ s.t $h_i(0^n) = 0$

eg: (1) $x_1 = 1$; $x_2 = 1$, . . . $x_n = 1$

(2) $\sum x_i = 1$; $\sum x_i = 2$; $\sum x_i = n$

Surprisingly, n is necessary.

Pf: (Via Combinatorial Nullstellensatz)

Suppose $h_1 \ldots h_m$ cover $B \setminus 0^n$

& don't cover 0^n

for some $m < n$.

(Wlog; $h_i(x) = 1 - \ell(x)$)

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{m} (1 - \ell_i(x)) - \prod_{j=1}^{n} (1 - x_j)$$

$\deg(f) = n$

Coeff of $x_1 \ldots x_n = (-1)^n \neq 0$

f on $\{0,1\}\times\{0,1\}\cdots\times\{0,1\}$

CN: $\exists\,(a_1 \ldots a_n) \in \{0,1\}^n$ s.t

$f(a_1 \ldots a_n) \neq 0$.

For all $a \in B \setminus 0^n$; h_i's cover a

$\Rightarrow f(a) = 0$

For $a = 0^n$; $f(0^n) = 1 - 1 = 0$

Hence $m \geq n$.

□

Proof of Combinatorial Nullstellensatz.

Hilbert's Nullstellensatz.

$\mathbb{F}$ - field (algebraically closed)

$g_1 \ldots g_m \in \mathbb{F}[x_1 \ldots x_n]$

m n-variate polynomials

$f \in \mathbb{F}[x_1 \ldots x_n]$ s.t

$\forall a \in \mathbb{F}^n \quad g_1(a) = g_2(a) \cdots = g_m(a) = 0$

$\Downarrow$

$f(a) = 0$

then $\exists$ poly $h_1 \dots h_m \in \mathbb{F}[x_1 \dots x_n]$
& $k \in \mathbb{N}$ s.t

$$f^k = \sum g_i h_i$$

Proof is simpler:

$m = n$

Each $g_i(x) = \prod_{s \in S_i} (x_i - s)$ $\Rightarrow$ Then prof of HN is simpler.

(Easy Nullstellensatz)

Thm: Let $\mathbb{F}$ - field, $S_1 \dots S_n \subseteq \mathbb{F}$.

$g_i(x_i) = \prod_{s \in S_i} (x_i - s)$, & $f \in \mathbb{F}[x_1 \dots x_n)$ of deg d.

$\forall a \in \mathbb{F}^n$: $g_1(a) = g_2(a) = \dots = g_n(a) = 0$

$\Downarrow$

$f(a) = 0$

Then there exist $h_1 \dots h_n \in \mathbb{F}[x_1 \dots x_n]$ such that

(1) $f = \sum g_i h_i$

(2) $\forall i$, $\deg(h_i) \leq d - |S_i|$

Proof of CN from EN:

f: $\deg(f) = d = t_1 + \dots + t_n$

Coeff of $x_1^{t_1} \dots x_n^{t_n} \neq 0$.

S_i, $|S_i| = t_i + 1$

Assume for contradiction that

$$f|_{S_1 \times \dots \times S_n} = 0.$$

EN $\Rightarrow$
$$f = \sum g_i h_i$$
$$= \sum_{i=1}^{n} h_i \cdot \prod_{s \in S_i} (x_i - s)$$
$$\cdot \deg(h_i) \leq d - |S_i| = \sum_{j=1}^{n} t_j - (t_i + 1)$$

Coeff of $x_1^{t_1} \dots x_n^{t_n}$ in f $\neq 0$

However Coeff of $x_1^{t_1} \dots x_n^{t_n} = 0$ in $\sum g_i h_i$.

$\Rightarrow\Leftarrow$

Hence, $\exists\, a \in S_1 \times \dots \times S_n$ s.t.

$f(\bar{a}) \neq 0$. ☒

Proof of Easy Nullstellensatz.

Observation:

① $S_1 \times S_2 \times \dots \times S_n$; $|S_i| = t_i + 1$

$\mathcal{F}_1 = \mathcal{F}(S_1, \dots, S_n) = \{ f : S_1 \times S_2 \times \dots \times S_n \to \mathbb{F} \}$.

$\mathcal{F}_1$ is an $\mathbb{F}$-vector space of dim $|S_1| \times |S_2| \times \dots \times |S_n|$

$\mathcal{F}_2 = \{ f \in \mathbb{F}[x_1 \dots x_n] \mid \deg_{x_i}(f) \le t_i = |S_i| - 1 \}$

$\mathcal{F}_2$ is also an $\mathbb{F}$-vector space of
dim $(t_1+1) \times (t_2+1) \times \dots \times (t_n+1)$
$= |S_1| \times \dots \times |S_n|$

$\mathcal{F} \cong \mathcal{F}_2$

f - poly of deg (d)

$f|_{S_1 \times \dots S_n} = 0$.

$g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ | Division algorithm Divide f by g_1

$f(x_1 \dots x_n) = g_1(x_1) h_1(x) + \underbrace{R_1(x_1 \dots x_n)}_{\deg_{x_1} R_1 < t_1 + 1}$

$= g_1(x_1) h_1(x) + g_2(x_2) h_2(x) + R_2(x_1 \dots x_n)$

$$\left(\deg_{x_1}(R_1) < \ell_1 + 1 \right.$$
$$\left. \deg_{x_2}(R_2) < \ell_2 + 1 \right)$$

$$= \sum g_i(x_i) h_i(x) + R_n(x_1 \dots x_n)$$

$$\text{w/} \quad \deg_{x_i}(R_n) < \ell_i + 1$$

$$f|_{S_1 \times \dots \times S_n} = 0 \;\; \text{i.e.} \;\; g_i|_{S_i} = 0 \Rightarrow R_n|_{S_1 \times \dots S_n} = 0$$

$R_n : S_1 \times \dots S_n \to 0$

$R_n \in \mathcal{F}_2 \Rightarrow R_n \equiv 0$

Hence, $f = \sum g_i h_i$ ∎