Today

Polynomial Method

- Ray Chaudhuri - Wilson / Frankl-Wilson Theorem
- VC dimension (Sauer-Shelah Lemma)

CSS.205.1
Toolkit in TCS
- Lecture #31
(9 June '21)
Instructor: Prahladh Harsha

Easy Nullstellensatz.

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

$f \in \mathbb{F}[x_1, \dots x_n]$; $\deg(f) \leq d$

$f|_{S_1 \times S_2 \dots \times S_n} \equiv 0$ (as a function)

$\Downarrow$

$f = \sum g_i h_i$ where $g_i(x) = Z_{S_i}(x_i)$

& $\deg(h_i) \leq d - |S_i|$

$Z_S(x) = \prod_{s \in S} (x - s)$

Fact: (i) Functions on grid

$\mathcal{F}_1 = \mathcal{F}(S_1, S_2 \dots S_n)$

$= \{ f : S_1 \times S_2 \dots \times S_n \rightarrow \mathbb{F} \}$.

$\mathcal{F}_1$ - $\mathbb{F}$-vector space of dim $\prod_{i=1}^{n} |S_i|$

(ii) Polynomials w/ bdd individual degree

$$\mathcal{F}_2 = \mathcal{P}(\mathbb{F}, n; |S_1|, |S_2| \ldots, |S_n|)$$

$$= \{ p - \text{polynomial over } n \text{ variables s.t. } \deg_{x_i}(p) < |S_i| \}.$$

$\mathcal{F}_2$ - $\mathbb{F}$-vector space of dim $\prod_{i=1}^{n} |S_i|$

$$\text{func}: \mathcal{F}_2 \longrightarrow \mathcal{F}_1$$
$$p \longmapsto f$$

To show $\mathcal{F}_2$ when viewed as a function via the natural mapping func.

Claim: func is bijective

Pf: $\dim(\mathcal{F}_1) = \dim(\mathcal{F}_2)$. suff to show func is surjective (or injective)

Surjective: Suff to show for δ-function on $S_1 \times S_2 \ldots \times S_n$.

$\bar{a} \in S_1 \times \ldots \times S_n$

$$\delta_{\bar{a}}(\bar{x}) = \begin{cases} 1 & \text{if } \bar{x} = \bar{a} \\ 0 & \text{otherwise} \end{cases}$$

$$P_{\bar{a}}(\bar{x}) = \prod_{i=1}^{n} \frac{Z_{S_i \setminus \{a_i\}}(x_i)}{Z_{S_i \setminus \{a_i\}}(a_i)}$$

$$Z_S(x) = \prod_{s \in S} (x - s)$$

(*) $\deg_{x_i}(P_{\bar a}) = |S_i| - 1$

(*) $P_{\bar a}(\bar a) = 1$

(*) $P_{\bar a}(\bar b) = 0$ where $\bar b \neq \bar a$

$P_{\bar a} = \delta_{\bar a}$

Proof of Easy Nullstellensatz:

Given f s.t. (i) $\deg(f) \le d$

(ii) $f|_{S_1 \times \dots \times S_n} = 0$

Apply the univariate division algorithm

$$f(x_1 \dots x_n) = Z_{S_1}(x_1)\underbrace{h_1(x_1 \dots x_n)}_{\deg h_1 \le d - |S_1|} + \underbrace{R_1(x_1 \dots x_n)}_{\substack{\deg(R_1) \le d \\ \deg_{x_1}(R_1) < |S_1|}}$$

$$= Z_{S_1}(x_1)h_1 + Z_{S_2}(x_2)\cdot \underbrace{h_2}_{\deg h_2 \le d - |S_2|} + \underbrace{R_2(x_1 \dots x_n)}_{\substack{\deg(R_2) \le d \\ \deg_{x_1}(R_2) < |S_1| \\ \deg_{x_2}(R_2) < |S_2|}}$$

$$= \sum_{i=1}^{n} Z_{S_i}(x_i)\cdot h_i + \underbrace{R_n(x_1 \dots x_n)}_{\substack{\deg(R_n) \le d \\ \forall i,\ \deg_{x_i}(R_n) < |S_i|}}$$

$f|_{S_1 \times \dots S_n} = 0$ & $Z_{S_i}|_{S_i} = 0$

$\Rightarrow R_n|_{S_1 \times \dots \times S_n} = 0$

But by observation, $R \equiv 0$

Hence, $f = \sum_{i=1}^{n} Z_{S_i}(x_i) \cdot h_i$ $\boxtimes$

A - arbitrary set

$A \subseteq \mathbb{F}^n$

$\mathcal{F} = \{f : A \to \mathbb{F}\}$. ; $\mathcal{F}_1$ - $\mathbb{F}$-vector space of dim $|A|$

$\mathcal{F} \subseteq \text{span}\{P_1, \dots P_m\} = \mathcal{F}_2$.

$\dim(\mathcal{F}_2) \leq m$

$\Rightarrow |A| \leq m$

Method: Bound the size of a set A.

Application 1:

Frankl-Wilson Theorem

F - family of subsets of $[n] = \{1, \dots, n\}$

$F \subseteq 2^{[n]}$ & $L = \{l_1, \dots l_s\}$

l_i - non-negative integer

F is L-intersecting
(ie $\forall$ distinct $A, B \in F$, $|A \cap B| \in L$

$\Downarrow$

$$|F| \leq \binom{n}{\leq s} = \sum_{i=0}^{s} \binom{n}{i}$$

Eg: $L = \{0, 1, \ldots, s-1\}$.

$\mathcal{F} = \binom{[n]}{\leq s}$; $|\mathcal{F}| = \sum_{i=0}^{s} \binom{n}{i}$

Pf: $\mathcal{F} = \{f : F \to \mathbb{R}\}$.

$\mathcal{F}$ - $\mathbb{R}$-vector space of dim $|F|$

$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$; $x, y \in \mathbb{R}^n$

$S, T \subseteq [n]$, $\mathbb{1}_S, \mathbb{1}_T$ - indicator vectors.

$\langle \mathbb{1}_S, \mathbb{1}_T \rangle = |S \cap T|$

F is L-intersecting.
$\forall$ distinct $A, B \in F$, $\langle \mathbb{1}_A, \mathbb{1}_B \rangle \in L$

For each $A \in F$

$\tilde{P}_A(x) \in \mathbb{R}[x_1, \ldots x_n]$

$$\tilde{P}_A(x) = \prod_{i : l_i < |A|} (\langle \mathbb{1}_A, x \rangle - l_i)$$

$F = \{A_1, A_2 \ldots \qquad A_{|F|}\}$

in non-decreasing order of size of sets.

$$\left.\begin{array}{ll} (*) & \tilde{P}_{A_i}(A_i) \neq 0 \\ (*) & j<i \; : \quad \tilde{P}_{A_i}(\mathbb{1}_{A_j}) = 0 \end{array}\right\} \Rightarrow \tilde{P}_A \text{ - linearly independent}$$

$(*')$ $\{\tilde{P}_{A_i} \mid i\}$ - linearly independent

Suppose not

$f = \alpha_1 P_{A_{i_1}} + \alpha_2 P_{A_{i_2}} + \ldots + \alpha_r P_{A_{i_r}} = 0$

$i_1 < i_2 \ldots < i_r$ -

& $\bar{\alpha} \neq 0$

$f(\mathbb{1}_{A_{i_1}}) = \alpha_1 \cdot \text{non-zero} \Rightarrow \alpha_1 = 0$

Continuing $\bar{\alpha} = 0 \Rightarrow \Leftarrow$

$\{\tilde{P}_{A_i}\}$ - linearly independent when viewed as fns

$$\tilde{P}_A(x) = \prod_{i : l_i < |A|} (\langle \mathbb{1}_A, x\rangle - l_i)$$

$\tilde{P}_A$ - not multilinear (individually each var ≤ 1)

P_A — Multilinearization $\tilde{P}_A$.

$\hookrightarrow$ Multilinearizing does not affect the value of fn at $\{0,1\}^n$-vectors

Hence $\{P_A \mid A \in F\}$ — linearly independent

$$P_{A_i}(\mathbb{1}_{A_j}) = \begin{cases} \text{nonzero} & \text{if } i = j \\ 0 & \text{if } j < i \end{cases}$$

<u>Obs</u>: Any monomial in P_A is of deg at most s.

So, in particular P_A can be written as a linear combination of x_I where $x_I = \prod_{i \in I} x_i$ for all $|I| \leq s$.

$$\text{span}\{P_A \mid A \in F\} \subseteq \text{span}\{x_I \mid |I| \leq s\}$$

$$|F| \leq \sum_{i=0}^{s} \binom{n}{i}$$

$\boxtimes$

Application 2.

VC-dimension (Sauer-Shelah Lemma).

U - universe of points
(finite, infinite)

$\mathcal{S}$ - family of subsets of U

eg: (1) $U = \mathbb{R}^1$

$\mathcal{S} = \{[a,b] \mid a, b \in \mathbb{R}, \ a \le b\}$ | VC=2

(2) $U = \mathbb{R}^n$

$\mathcal{S}$ = sets described by a hyperplane.

| VC=3.

$X \subseteq U$, X - finite.

$$\mathcal{S}(X) \triangleq \{X \cap S \mid S \in \mathcal{S}\} \subseteq 2^X$$

Defn: A finite set $X \subseteq U$ is shattered by set system $\mathcal{S}$ if

$$\mathcal{S}(X) = 2^X$$

$$\pi_{\mathcal{S}}(m) = \max_{\substack{X \subseteq U \\ |X| = m}} \{ |\mathcal{S}(X)| \}$$

Vapnik- Chervonenkis (VC) dimension.

$$VC(\mathcal{S}) = \max\{d \mid \pi_{\mathcal{S}}(d) = 2^d\}$$

Set systems w/ bdd VC-dimension

$\pi_{\mathcal{S}}(m)$ - growth $\begin{cases} \text{poly} \\ \text{or} \\ \text{exponential} \end{cases}$

Sauer-Shelah Lemma

$(U, \mathcal{S})$ - VC-dim d

$\forall m, \quad \pi_{\mathcal{S}}(m) \le \binom{m}{\le d}$

Tight: $\mathcal{S}$ = family of subsets of size $\le d$

eg: (1) $U = \mathbb{R}^2$

$\mathcal{S}$ = set of halfspaces

VC-3

$$\pi_{\mathcal{S}}(m) \le \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \binom{m}{3} = O(m^3)$$

(2) $U = \mathbb{R}^d$

$\mathcal{S}$ = set of convex bodies

X = d+1 vertices of a simplex

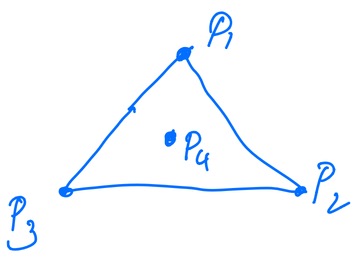
X - shattered by $\mathcal{S}$

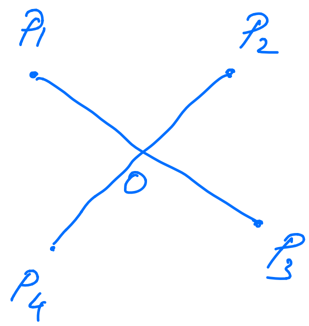
$\Rightarrow VC(\mathcal{S}) \geq d+1$

Radons Theorem: $P_1, \dots, P_{d+2}$ - $d+2$ distinct pts in $\mathbb{R}^d$, then $\exists$ subset $S \subseteq [d+2]$ s.t

$$Conv(P_i / i \in S) \cap Conv(P_i / i \notin S) \neq \phi$$

$d = 2.$





$P_4 \in Conv(P_1, P_2, P_3)$

$$O \in Conv(P_1, P_3) \cap Conv(P_2, P_4)$$

$VC(\mathcal{S}) \leq d+1.$