gct 2022 : School on Geometric Complexity Theory

Lecture 28 (2021-12-03)

Explicit Dimension Reduction for Varieties, and the Polynomial Identity Testing Problem

Michael A. Forbes (University of Illinois at Urbana-Champaign)
based on joint work w/ Amir Shpilka (Tel-Aviv University)

this lecture : polynomial identity testing (PIT)
dimension reduction for varieties
(Noether Normalization)
simultaneous conjugacy of matrices
=

def (polynomial identity testing (PIT)):

given a polynomial f, is $f = 0$?

↳ f given via
algebraic ckt of
size $\leq S$
$\deg f \leq d$

↳ $\sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$, $\bar{x}^{\bar{a}} = \prod_{i=1}^{n} x_i^{a_i}$, $\alpha_{\bar{a}} \in \mathbb{F}$

$n = \#$ vars

A PIT algo is black-box if only uses ckt to evaluate f at chosen points $\bar{\beta} \in \mathbb{F}^n$, and otherwise white box.

lem: PIT has $\text{poly}(\binom{n+d}{d}, S)$ time deterministic algo

pf: expand each of S operations into $\binom{n+d}{d}$ monomials

params: $n = \#$ vars ← large
$d = \deg \leq n^{O(1)}$
$S = \text{size} \leq n^{O(1)}$

lem (Schwartz Zippel) $S \subseteq \mathbb{F}$, $f \neq 0$

$$\Pr_{\alpha \leftarrow S^n} [f(\alpha) = 0] \leq \frac{d}{|S|}$$

cor: PIT has poly(n, d, s) time randomized algorithm $\hat{}$ black-box

rmk: - PIT powerful algorithmic tool
- computer algebra
- verifying poly identities
eg $\det(AB) = \det(A)\det(B)$
- efficient manipulation of succinct algebraic expressions
eg checking if $f | g$

- non-algebraic problems
- deterministic primality testing [AKS]
- (parallel) algorithms for graph matching [Lovasz, Fenner Gurjar Thierauf]
- black box PIT as strange solution concept
- tight connections to proving lower bounds

def: $\mathcal{C} \subseteq \mathbb{F}[\bar{x}]$. $H \subseteq \mathbb{F}^n$ is a hitting set

if $\forall f \in \mathcal{C}$, $f \neq 0$ iff $f(\bar{\alpha}) \neq 0$, some $\bar{\alpha} \in H$

Def: deterministic t-step black-box PIT

also for $\mathcal{C}$

$\equiv$ hitting set H for $\mathcal{C}$, $|H| \leq t$

Lem: $S \subseteq \mathbb{F}$, $|S| \geq d+1$ then

S^n is a hitting set for

$\mathcal{C} = \{ n\text{-var deg} \leq d \text{ poly} \}$

thm [Heintz Schnorr]: (exists) poly(n,d,s)-size

hitting set for $\mathcal{C} = \left\{ \begin{array}{l} n\text{-var} \\ \deg \leq d \\ \text{size} \leq s \end{array} \right\}$

when $|\mathbb{F}| \geq \text{poly}(n,d,s)$

sketch: for (single) $f \neq 0$

$$\Pr_{\bar{\alpha}_1, \ldots \bar{\alpha}_t \in S^n} [f(\bar{\alpha}_1) = \cdots f(\bar{\alpha}_t) = 0] \leq \left(\frac{d}{|S|}\right)^t \approx 0$$

then apply "union bound" over

all f of small size

- $|\mathbb{F}|$ finite $\Rightarrow$ can count small circuits
- $|\mathbb{F}|$ infinite $\Rightarrow$ use that $\mathcal{C}$ is contained in small dimensional variety

□

Q: construct small hitting sets?

thm [Kabanets Impagliazzo] $\mathrm{char}(\mathbb{F})=0$] hardness
if $n \times n$ permanent requires $2^{\Omega(n)}$ size circ

$\Rightarrow$ explicit $n^{O(\log n)}$ size hitting set] randomness
for n-var deg $\le d$, size $\le s$ circ
$d, s \le n^{O(1)}$

Lem: hitting set for $\mathcal{C}$ of size $< \binom{n+d}{d}$] randomness

$\Rightarrow$ can construct $f \notin \mathcal{C}$] hardness
in time $\mathrm{poly}\left(\binom{n+d}{d}\right)$

A: solving PIT "just" requires proving lower bounds!
but lower bounds are only known for restricted models
but hardness vs randomness often cannot be instantiated
in restricted models

known: many nontrivial white/black-box deterministic PIT also for restricted models

idea:
- reduce number of variables while "preserving structure"
- back to PIT of polys in small # variables

"preserving structure"

eg: (exactly) preserve complexity measure Γ used in lower bound proofs

Γ(small ckt) $\leq$ small

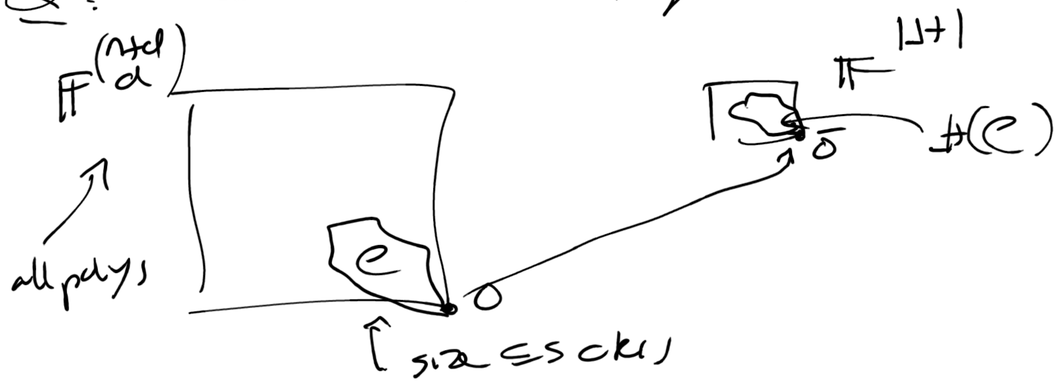
$\Rightarrow$ not "expensive" to preserve

Γ(non-zero poly) > 0

$\Rightarrow$ non-zeroness is preserved

models:
- sparse polys
- $\Sigma^{O(1)}\Pi\Sigma$
- read once models
  - formulas
  - ABPs
  - determinants
- $\Sigma\wedge\Sigma$
- noncommutative
  - formulas & division
  - ABPs
- constant depth formulas
- ...

Q: connection to alg geom?



$$f \overset{H}{\mapsto} \big(f(x)\big)_{x \in H}$$

H hitting set for C $\Rightarrow$

H injective on 0 over C

Lem: H hitting set for size $\le 2s$ ckts

$\Rightarrow$ H hitting set for $\{f-g : f, g \text{ sizes}\}$

$\Rightarrow$ H injective on $\{\text{size} \le s\}$

interpolating set

Lem (Noether Normalization)

$V \subseteq \mathbb{F}^N$ variety $\dim V \le s$

then random linear map

$L : \mathbb{F}^N \to \mathbb{F}^{s+1}$ is injective on zeros of V.

Q (Mulmuley #2): derandomize NN

$\leftarrow$ "impure" variety?

- generalize PIT to AG
- NN fundamental
- related to class. hyp. problems in geometric invariant thy

def: the simultaneous conjugation action of $GL_n(\mathbb{C})$ on $(\mathbb{C}^{n\times n})^r$ is

$$\bar{M} = (M_1, \dots, M_r) \mapsto (PM_1P^{-1}, \dots, PM_rP^{-1}) = P\bar{M}P^{-1}$$

eg: $I_2 = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$ $\quad PI_2P^{-1} = I_2$

$$\begin{bmatrix} \delta & \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \varepsilon \\ & 1 \end{bmatrix} \begin{bmatrix} \delta & \\ & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \varepsilon\delta \\ & 1 \end{bmatrix}$$

$$\Rightarrow GL_2(\mathbb{C}) \begin{bmatrix} 1 & \varepsilon \\ & 1 \end{bmatrix} \overset{\neq 0}{=} \begin{bmatrix} 1 & \neq 0 \\ & 1 \end{bmatrix}$$

"

$$= \begin{bmatrix} 1 & * \\ & 1 \end{bmatrix}$$

recall: **def**: a poly $f(\bar{M})$ is **invariant** if

$$f(P\bar{M}P^{-1}) = f(\bar{M}), \quad \forall P \in GL_n(\mathbb{C})$$

the set of invariants is $\mathbb{C}[\bar{M}]^{GL_n(\mathbb{C})}$

thm: $\mathbb{C}[\bar{M}]^{GL_n(\mathbb{C})}$ is a ring, finitely generated as algebra

GIT quotient $(\mathbb{C}^{n\times n})^r /\!/ GL_n(\mathbb{C})$ is a variety whose regular functions are

Q: dead NN?

A: $r = 1$

$M \mapsto$ coeff char poly

Q: $r > 1$?

recall:

lem: invariants are constant on orbits

thm: $\overline{GL_n(\mathbb{C})\,\bar{A}} \cap \overline{GL_n(\mathbb{C})\,\bar{B}} \neq \emptyset$

iff $\exists\, f \in \mathbb{C}[\bar{m}]^{GL_n(\mathbb{C})}$ s.t. $f(\bar{A}) \neq f(\bar{B})$

(orbit closures)

goal: given $\bar{A}, \bar{B}$, decide ↑

def: $S' \subseteq \mathbb{C}[\bar{m}]^{GL_n(\mathbb{C})}$ is called separating invariants if $\forall\, \bar{A}, \bar{B} \in (\mathbb{C}^{n\times n})^r$

$\exists\, f \in \mathbb{C}[\bar{m}]^{GL_n(\mathbb{C})}$ $f(\bar{A}) \neq f(\bar{B})$

if $\exists\, g \in S'$ $g(\bar{A}) \neq g(\bar{B})$

cor: if S' generates $\mathbb{C}[\bar{m}]^{GL_n(\mathbb{C})}$

then S' is separating set.

goal: construct small set of separating invariants

ex: $tr(M_1) \mapsto tr(PM_1P^{-1})$

$= tr(M_1P^{-1}P)$

$= tr(M_1)$

$\det(M_1) \mapsto \det(PM_1P^{-1})$

$= \det(P)\det(M_1)\det(P^{-1})$

(cancel)

$= \det(M_1)$

$tr(M_1M_2\cdots M_r) \mapsto tr(PM_1P^{-1}PM_2P^{-1} \cdots PM_rP^{-1})$

$= tr(M_1\cdots M_r)$

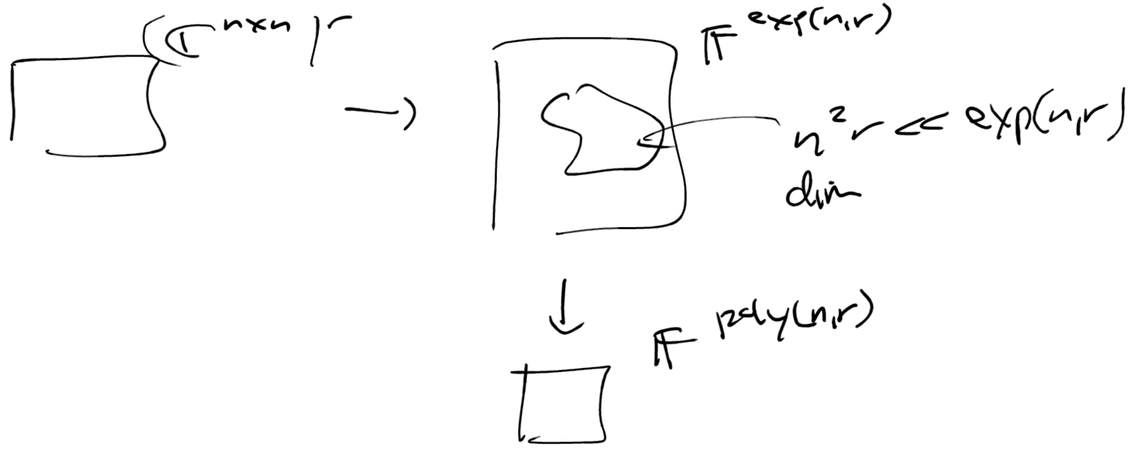
thm [Procesi, Razmyslov, Formanek]

$\mathbb{C}[\bar{m}]^{GL_n(\mathbb{C})}$ is generated by trace monomials

$$\mathcal{T} = \left\{ tr(M_{i_1}\cdots M_{i_\ell}) : \begin{matrix} 1 \le i_j \le r \\ 0 \le \ell \le n^2 \end{matrix} \right\}$$

cor: explicit $\exp(nr)$ size SAS of separating invariants

$\Rightarrow$ explicit orbit closure intersection also



def [Forbes Shpilka 13a] given $\bar{M} = (M_1, \dots, M_r)$

define $M(x) = \sum_{i=0}^{r} M_i x^i$

$\leftarrow M_0 := I_n$

define $f_\ell^{FS}(\bar{M}, \bar{x}) = \mathrm{tr}(M(x_1) M(x_2) \cdots M(x_\ell))$

lem: any ℓ, $\bar{\alpha}$, $f_\ell^{FS}(\bar{M}, \bar{\alpha})$ is invariant

prop: $\bar{A}, \bar{B}$ separated by some invariant iff

$f_{n^2}^{FS}(\bar{A}, \bar{x}) \neq f_{n^2}^{FS}(\bar{B}, \bar{x})$

pf: $\Leftarrow$:

$\Rightarrow$:

$\Rightarrow$ $\bar{A}, \bar{B}$ separated by some trace monomial

$\mathrm{tr}(M_{i_1} \cdots M_{i_\ell})$, $\ell \le n^2$

$= \mathrm{coeff}_{x_1^{i_1} \cdots x_\ell^{i_\ell}} (f_{n^2}^{FS}(\bar{M}, \bar{x}))$

$\Rightarrow$

thm [Mulmuley 12] and polytime also for orbit closure intersection

ker [Forbes Shpilka 13a]:

any $\bar{A}, \bar{B}$, $f_n^{\bar{A}}(\bar{A}, \bar{x}) - f_n^{\bar{B}}(\bar{B}, \bar{x})$

is a poly(n, r) size read-once oblivious ABP (roABP)

thm [Nisan]: determ requires $2^{\Omega(n)}$ size roABP

thm [RS05, AJS09]: polytime det (white box) PIT for roABP

thm [FS13b]: (quasipoly time black box) PIT for roABP

thm [Forbes Shpilka 13a]

det polytime also for orbit closure intersection for simultaneous conjugacy

explicit poly$(n, r)^{O(\log n)}$ size set of separating invariants

rmk: same analogues for null-cone & left-right action, but explicit roABP separating invariants yield black box PIT for

$$\det\left(\sum_{i=1}^{n^2} A_i \otimes x_i\right)$$

(poly(n, d))