Algebraic dependence is not hard

and filling the GCT Chasm

Nitin Saxena (CSE@IIT Kanpur, India)

(Joint work with Zeyu Guo & Amit Sinhababu, *CCC'18*)

2018, Dagstuhl

Overture

- Consider map $\mathbf{f} : F^n \to F^m$.
- **Problem (AD):** $\dim \overline{\mathrm{Img}}(\mathbf{f}) <? \ m$.
- **Problem (ZC):** $\mathbf{0} \in? \ \overline{\mathrm{Img}}(\mathbf{f})$.

Contents

Algebraic dependence testing

- Given polynomials $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$ we call them *algebraically dependent* if there is an *annihilator* $A(y_1,\ldots,y_m)$.
  - i.e. $A(f_1,\ldots,f_m)=0$.
  - Input polynomials may be algebraic circuits.
  - The maximum number of independent polynomials in $f_1,\ldots,f_m$ is called *transcendence-degree* (trdeg).
  - Eg. trdeg of $\{x_1+x_2\,,\ x_1^2+x_2^2\}$ is two when char(F)$\neq 2$, else it is one.

- Problem AD(F): Given polynomials $\mathbf{f}$, test the algebraic dependence over field F.
  - Computability/ Complexity of this problem?
  - What about the annihilator?

Algebraic dependence-- Applications

- Fundamental in commutative algebra, algebraic-geometry.
- (Dvir,Gabizon,Wigderson'07) use it to design *extractors* for sources that are polynomial maps.
- (Kalorkoti'85) (Beecken,Mittmann,S.'07) (Agrawal,Saha,Saptharishi,S.'12) (Kumar,Saraf'16) (Pandey,S.,Sinhababu'16) prove circuit lower bounds or design hitting-sets (*blackbox PIT*).
- (Heintz,Schnorr'80) (Agrawal,Ghosh,S.'18) (Kumar,Saptharishi,Tengse'18) use annihilators to *bootstrap* bad hitting-sets to nearly optimal ones.
- Current work yields new applications of annihilators.
  - eg. polynomial system solving. GCT questions.

Alg. dependence-- previous results

- (Perron 1927) Minimal annihilator has degree $\leq \prod_i \deg(f_i)$.
  - So, the annihilator $A(y_1,\ldots,y_m)$ has *exponentially* many coefficients.
  - Their existence can be checked by doing *linear algebra*.
  - AD(F) is in PSPACE.

- (Mittmann,S.,Scheiblechner'14) improved it to co-NP$^{\#P}$.

- (Jacobi 1841)'s criterion puts AD(F) in coRP, if char(F) is *zero or large*.
  - Rank of Jacobian $((\partial_{x_i} f_j))$ equals trdeg of f_j's.
  - When $F(\mathbf{x}) \supseteq F(\mathbf{f})$ is a *separable* extension.

$\mathbf{x}_i$ has distinct conjugates

- (Pandey,S.,Sinhababu'16) extends Jacobi criterion to input $\mathbf{f}$ with *constant inseparable-degree*.

Contents

- Algebraic dependence testing
- Entropy & Protocols
- Three problems; algebra & geometry
- <u>Approximate</u> polynomials satisfiability (APS)
- APS is in PSPACE
- Conclusion

Polynomial map-- Entropy

- Consider map $\mathbf{f} : F^n \to F^m$.
  - Wlog assume $n=m$ and F large enough.

- What can we say about the *geometry* of the map?
  - Eg. the dimensions of *image*, *preimage*?
  - Eg. the *Zariski closure* of the image?
  - They seem unrelated to zeroset of the *ideal* $\langle f_1 ,\ldots, f_m \rangle$.

- Intuitively, alg.independent $\mathbf{f}$ should have a *large* image.
  - Analogously, preimage $\mathbf{f}^{-1}(b)$ should be usually *small*.

- Consider the case of finite fields $F= GF(q)$.
  - For $b \in F^m$, denote $\#\mathbf{f}^{-1}(b)$ by $N(b)$.
  - Denote $\#\{\mathbf{x} \in \overline{F}^n : \mathbf{f}(\mathbf{x})=b\}$ by $\overline{N}(b)$.

Allow points in *algebraic closure*.

Polynomial map-- Preimage

So, *Image* is dimension n (= trdeg); *Preimage* is dimension 0.

- Consider map $\mathbf{f} : F^n \to F^n$.
  - Let $D := \prod_i \deg(f_i)$.
- **Lemma 1 [Preimage]:** For alg.independent $\mathbf{f}$, $N(\mathbf{f}(a)) \leq D$ for all except (D^2/q)-fraction of $a \in F^n$.
  - *Pf idea*: Consider the annihilators $A_i(x_i,\mathbf{f})=0$, for $i \in [n]$.
  - Degree bound is D and it constrains the bad a's.
- **Lemma 2 [Preimage]:** For dependent $\mathbf{f}$, $N(\mathbf{f}(a)) > k$ for all except (kD/q)-fraction of $a \in F^n$.
  - *Pf idea*: Consider the annihilator $A(\mathbf{f})=0$.
  - Degree bound is D and it constrains the bad a's.
- (Goldwasser-Sipser'86)'s *set-lowerbound method* on $\mathbf{f}^{-1}(\mathbf{f}(a))$ proves: AD is in AM.

Polynomial map-- Image

- Consider map $\mathbf{f} : F^n \to F^n$.
  - Let $D := \prod_i \deg(f_i)$.

- **Lemma 1 [Image]:** For alg.independent $\mathbf{f}$, $N(b)>0$ for at least $(D^{-1} - D/q)$-fraction of $b \in F^n$.
  - *Pf idea*: Let S be the a's for which $N(\mathbf{f}(a)) \leq D$.
  - By Lemma 1 [Preimage], $\#f(S)/q^n \geq \#S/Dq^n \geq (D^{-1} - D/q)$.

- **Lemma 2 [Image]:** For dependent $\mathbf{f}$, $N(b)=0$ for all except (D/q)-fraction of $b \in F^n$.
  - *Pf idea*: Consider the annihilator $A(\mathbf{f})=0$.
  - Degree is D and it constrains the *image* b.

AD $\in$ AM $\cap$ coAM rules out AD's NP-hardness !

- (Goldwasser-Sipser'86)'s Set Lowerbound method on Image($\mathbf{f}$) proves: AD is in coAM.

Contents

- Algebraic dependence testing
- Entropy & Protocols
- Three problems; algebra & geometry
- <u>Approximate</u> polynomials satisfiability (APS)
- APS is in PSPACE
- Conclusion

Polynomial map-- Zariski closure

- Consider map $\mathbf{f} : F^n \rightarrow F^m$.

- Zariski closure $\overline{\mathrm{Img}}(\mathbf{f}) := Z(I)$, where I is the annihilating-ideal of $\mathbf{f}$.
  - It's the smallest affine variety in $\overline{F}^m$ containing image of $\mathbf{f}$.
  - Zerosets are closed sets in Zariski topological space F^m.

- Problem ZC: Given polynomials $\mathbf{f}$, test whether $\mathbf{0} \in? \overline{\mathrm{Img}}(\mathbf{f})$.

- Eg. $\mathbf{0} \in \overline{\mathrm{Img}}(x_1, x_1x_2\text{-}1)$, though $\mathbf{0} \notin \mathrm{Img}(x_1, x_1x_2\text{-}1)$.
  - Annihilating-ideal of $(x_1, x_1x_2\text{-}1)$ is $\langle 0 \rangle$.

- ZC can be solved using Elimination theory or Gröbner bases.
  - It takes EXPSPACE.
  - i.e. *doubly*-exponential time!
  - Annihilating-ideal may be terribly complicated.

Polynomial map-- AnnAtZero

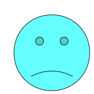
- Consider map $\mathbf{f} : F^n \to F^m$ with I as the annihilating-ideal.

- Problem AnnAtZero: Given polynomials $\mathbf{f}$, is the *constant term* of *every* annihilator zero?

- If $\mathrm{trdeg}(\mathbf{f})=m$, then the answer is trivially YES.

- If $\mathrm{trdeg}(\mathbf{f})=m-1$, then the annihilating-ideal is principal.
  - Check constant term, by doing *linear algebra,* in PSPACE.
  - (Kayal'09) Even this is NP-hard.

- **Lemma:** ZC iff AnnAtZero.
  - *Proof idea:* $\mathbf{0} \in \overline{\mathrm{Img}}(\mathbf{f}) := Z(I)$ iff $I \subseteq \langle y_1, \ldots, y_m \rangle$.

- AnnAtZero is in EXPSPACE. 

Approx. polynomials satisfiability- APS

- Problem APS: Given circuits $\mathbf{f}$, is there $\beta \in \overline{F}(\varepsilon)^n$ such that, for all i, $f_i(\beta) \in \varepsilon\overline{F}[\varepsilon]$?
  - *Real Analytic motivation:* Think of $\varepsilon \to 0$.
  - Then, we want ``roots'' β of $\mathbf{f}$ such that $f_i(\beta) \to 0$.
  - We're allowing ``values'' $1/\varepsilon \to \infty$.
- <u>Note:</u> If $\beta \in \overline{F}[\varepsilon]^n$ then we get actual roots of $\mathbf{f}$ in $\overline{F}^n$.
  - Classical PS (or Hilbert Nullstellensatz) is in PSPACE.
  - (Koiran'96) Conditionally, it's in AM.
- **Lemma:** ZC iff APS.
  - *Proof idea:* (Lehmkuhl-Lickteig'89) reduce to a *curve* & deduce:

    $\mathbf{0} \in \overline{\mathrm{Img}}(\mathbf{f}) := Z(I)$ iff ``approximate root'' $\beta \in \overline{F}(\varepsilon)^n$ exists.
- APS is in EXPSPACE.

Infinitesimally approximate root

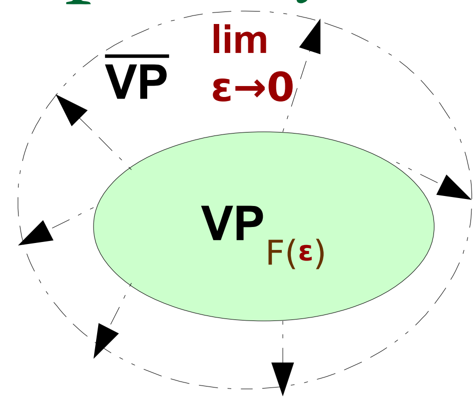
Equivalence of the three

- Consider map **f** : $F^n \to F^m$.
- **Theorem:** ZC iff AnnAtZero iff APS.
- Can we do better than EXPSPACE ?
- Going by degree/ precision bounds, it looks hopeless.....
- Exploit the geometry in ZC?
  - Dimension reduction?

Contents

- Algebraic dependence testing
- Entropy & Protocols
- Three problems; algebra & geometry
- Approximate polynomials satisfiability (APS)
- APS is in PSPACE
- Conclusion

APS models Approximative Complexity



- Family $\{f_n(\mathbf{x})\}$ is in $\overline{\text{VP}}$ if, over $F(\varepsilon)$, there is a poly(n)-size circuit family $\{g_n(\mathbf{x})\}$ such that

$$f_n - g_n \in \varepsilon F[\varepsilon][\mathbf{x}] \, .$$

  - We define $\overline{\text{size}}(f_n)$ to be size(g_n).
  - Potentially, $\overline{\text{size}}(f)$ may be *much smaller* than size(f).

- Blackbox polynomial identity testing/ *Hitting-set generator* for $\overline{\text{VP}}$:

- Problem [$\overline{\text{VP}}$ hsg]: Given oracle to $f(\mathbf{x})$, test whether it's zero.
  - [Verification]: Given a set $\mathcal{H}$, is it a *hitting-set* for $\overline{\text{size}}$-s circuits?
  - *Infinitely* many circuits to verify!

- We reduce the verification problem to APS.

APS models Approximative Complexity

- Reduce the $\overline{VP}$ hsg verification problem to APS.
- Let $\Psi(\mathbf{y},\mathbf{x})$ be a universal circuit with $\mathbf{y}$ as *auxiliary variables*.
  - Fixing $\mathbf{y} \in F(\varepsilon)^{s'}$ approximates any desired $\overline{\text{size}}$-s circuit.
- Set $\mathcal{H}$ is *not* a hitting-set for $\overline{\text{size}}$-s degree-r circuits, if there is a fixing of $\mathbf{y}$ such that resulting polynomial *fools* $\mathcal{H}$.
- Criterion [non-hitting-set]: There exist $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ s.t.:

Fools the set

1) $\Psi(\boldsymbol{\alpha},\mathbf{v}) \in \varepsilon F[\varepsilon]$, for $\mathbf{v} \in \mathcal{H}$.
2) $\Psi(\boldsymbol{\alpha},\boldsymbol{\beta}) - 1 \in \varepsilon F[\varepsilon]$.
3) $\beta_i^{r+1} - 1 \in \varepsilon F[\varepsilon]$, for all i.

Nonzeroness

*\`\`Real" points (i.e. avoid **1/ε**) certify the existence of* $\Psi(\boldsymbol{\alpha},\mathbf{x})$ mod $\boldsymbol{\varepsilon}$

- Reduction in poly(n,s,r,h) time.

APS models Approximative Complexity

- APS models *any* computational problem where infinitesimal approximation is involved.
  - Recipe is field and char independent.
- *Border rank* computation of a tensor reduces to APS.
- *Explicit system of parameters* (esop) in GCT reduces to APS.
  - (Mulmuley'12) GCT Chasm: $\overline{\text{VP}}$ hsg vs. VP hsg.
- *Null-cone problem*, from invariant theory, reduces to APS.
  - Whether input *tensor* X is in the null cone of the *group action* G?
  - (Bürgisser-Garg-Oliveira-Walter-Wigderson '17) Applicable in combinatorial optimization, etc.
  - A really special case of APS.

Whether 0 is in the **orbit closure**?

Contents

Solving APS

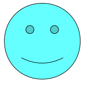
- We give a nontrivial algorithm for APS.
- Input circuits $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$.
  - Recall that AnnAtZero on $\mathbf{f}$ is equivalent to APS.
- We intend to reduce to the case where $\mathrm{trdeg}(\mathbf{f})=m-1$.
  - Check constant term of the unique annihilator, by doing *linear algebra,* in PSPACE.

Else, there are *too many/ high degree* annihilators!

- Let $\mathrm{trdeg}(\mathbf{f})=:k$.
  - Case [$k\geq m-1$]: We know a PSPACE algorithm solving APS.
- Assume we have $k<m-1$.
  - $\mathbf{g}:= \{g_1 ,\ldots, g_{k+1}\}$ be $k+1$ random linear combinations of $\mathbf{f}$.

Solving APS

- $\mathbf{g} := \{g_1, \ldots, g_{k+1}\}$ is $k+1$ random linear combinations of $\mathbf{f}$.
  - Claim: Whp, $\mathrm{trdeg}(\mathbf{g}) = k$.
- Theorem: Whp, $\mathbf{g}$ is in APS iff $\mathbf{f}$ is in APS .
  - *Proof idea*: Converse is relatively easy to show.
  - For forward direction, assume $\mathrm{trdeg}(\mathbf{g}) = k$ and $\mathbf{g} \in$ APS.
  - Let $\pi : F^m \to F^{k+1}$ be *random linear* map with kernel W.
  - Let $V := \overline{\mathrm{Img}}(\mathbf{f})$ and $V' := \overline{\pi(V)}$ be relevant varieties.
  - We show: $\pi^{-1}(V') = \cup_{P\in V} W_P$, where W_P is the translate variety.
  - $\mathbf{0}\in V' \Rightarrow W \subseteq \pi^{-1}(V') \Rightarrow W = W_P$ for some $P\in V \Rightarrow P\in V\cap W$ (*false* whp).
- We solve APS in PSPACE.
  - Down with EXPSPACE !



Contents

- Algebraic dependence testing
- Entropy & Protocols
- Three problems; algebra & geometry
- Approximate polynomials satisfiability (APS)
- APS is in PSPACE
- Conclusion

At the end …

- Algebraic dependence testing is in AM ∩ coAM .
  - Open: Randomized subexp-time algorithm?

- Approx.polynomials satisfiability is in PSPACE .
  - Open: in AM? PH?
  - Would solve a host of other problems.

- An input instance open for both the problems:

  - Open: Set of quadratic polynomials over GF(2) ?

Thank you!