Algebraic Independence and Applications

Nitin Saxena (Hausdorff Center for Mathematics, Bonn)

Joint work with

Malte Beecken & Johannes Mittmann (HCM, Bonn)

Contents

- **What is algebraic independence?**
- The computational problem
- I: A formula lower bound
- II: A notion of entropy
- III: Polynomial identity testing (PIT)
  - Depth-4 PIT
- At the end …

What is algebraic independence?

- Let $f_1,\ldots,f_m$ be polynomials in $F[x_1,\ldots,x_n]$.
- Definition: $\{f_1,\ldots,f_m\}$ are called algebraically independent if there is no non-zero polynomial $A \in F[y_1,\ldots,y_m]$ such that $A(f_1,\ldots,f_m)=0$.
- Definition: Otherwise the polynomials are algebraically dependent and A is their annihilating polynomial.
- This generalizes the notion of linear independence to higher degree.
- For example, $\{x_1, x_2\}$ are algebraically independent. While $\{x_1, x_2, x_1^3+x_2^2\}$ are not.

The annihilating polynomial here is $(y_1^3+y_2^2-y_3)$.

Transcendence degree

- We can now define a notion of *rank.*
- Definition: The transcendence degree $\mathrm{trdeg}\{f_1,\ldots,f_m\}$ is the the maximum number of algebraically independent polynomials.
- This word comes from *field theory.*
  - The field $F(f_1,\ldots,f_m)$ is *transcendental* over F with *degree* $\mathrm{trdeg}\{f_1,\ldots,f_m\}$.
  - Also, trdeg is well defined.

Examples

- As we noticed before $\mathrm{trdeg}\{x_1, x_2, x_1^3+x_2^2\} = 2$.
- $\mathrm{trdeg}\{x_1, x_2-x_1^d, x_2^d\} =?\, 2$.
  - The annihilating polynomial is $(y_1^d+y_2)^d-y_3$.
- $\mathrm{trdeg}\{x_1, x_2-x_1^d, x_3-x_2^d, \ldots, x_n-x_{n-1}^d, x_n^d\} = n$.
  - The annihilating polynomial has degree d^n .
- Annihilating polynomial can be exponentially large!

Contents

- What is algebraic independence?
- **The computational problem**
- I: A formula lower bound
- II: A notion of entropy
- III: Polynomial identity testing (PIT)
    - Depth-4 PIT
- At the end …

The computational problem

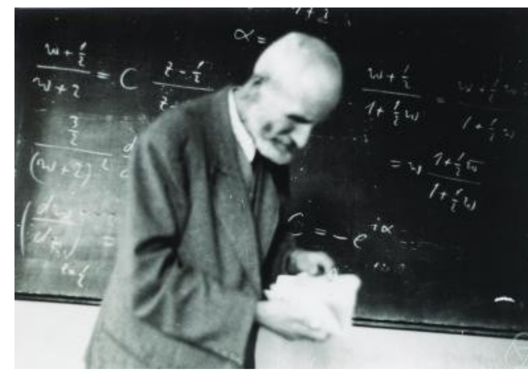
- Problem 1: Given *explicit* polynomials $f_1,\ldots,f_m$ over a field F. Compute their trdeg.

- Problem 2: Same as above but with *circuits* as inputs.

- We would want an *efficient* algorithm in terms of the input size:
  - In Problem 1 it is mainly the sparsity of the f's.
  - In Problem 2 it is the size of the circuits defining f's.

Solving by first principles ?

- Given *explicit* polynomials $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$ of degrees at most d.
- An annihilating polynomial could have degree d^n, so a direct approach requires exponential time.
- [Perron 1927] The degree is at most d^n.
- Thus, using linear-algebra we can produce the annihilating polynomial in PSPACE !



Oskar Perron

- [Kayal '09] showed that computing the annihilating polynomial is #P hard.
- The problem of computing trdeg looks hopeless

Enter geometry – the differentials

- Consider the action of *function* f_i on the *tangent space* of F^n.
  - i.e., the differential df_i .

    Eg, $d(x_1^3+x_1x_2)=3x_1^2dx_1+x_1dx_2+x_2dx_1$
  - Fact: $df=(\partial_1 f)dx_1+\ldots+(\partial_n f)dx_n$.

    $\partial_1(x_1^3+x_1x_2)=3x_1^2+x_2$
- Do $df_1,\ldots,df_m$ carry enough *information* to determine $\mathrm{trdeg}\{f_1,\ldots,f_m\}$?
- YES!
- (Almost-)Theorem: $df_1,\ldots,df_m$ are linearly independent over $F(x_1,\ldots,x_n)$ iff $\{f_1,\ldots,f_m\}$ are algebraically independent.

Enter geometry – the Jacobian

- **Definition:** The $m \times n$ matrix $(\partial_j f_i)_{i,j}$ is called the Jacobian $J_x(f_1,\ldots,f_m)$.

- **Theorem** [Jacobi 1841, Us]: If $\mathrm{char}(F)=0$ or $>d^r$ then $\mathrm{rk}\, J_x(f_1,\ldots,f_m) = \mathrm{trdeg}\{f_1,\ldots,f_m\}$.

- **Proof sketch:** Suppose $f_1,\ldots,f_i$ are algebraically dependent and $A(y_1,\ldots,y_i)$ annihilates them.
  - Expanding the differential $d(A(f_1,\ldots,f_i))=0$ shows that $df_1,\ldots,df_i$ are linearly dependent.
  - Thus, those rows of the Jacobian are dependent.

  - Suppose $f_1,\ldots,f_i$ are algebraically independent.
  - A similar argument shows those rows of the Jacobian independent. ■

This is trickier & needs $\mathrm{char}(F)$ 0 or large.

Carl Gustav Jacob Jacobi

Jacobian saves the day!

- The Jacobian $J_x(f_1,\ldots,f_m) := (\partial_j f_i)_{i,j}$ has as entries n-variate polynomials.

- Why not evaluate these at a random point $\alpha \in F^n$?

- Fact [Schwartz'80, Zippel'79, DeMillo Lipton'78]: With high probability $\mathrm{rk}\,(J_x(f_1,\ldots,f_m)|_{x=\alpha}) = \mathrm{rk}\,J_x(f_1,\ldots,f_m)$.

- Thus, we have a randomized poly-time algorithm for trdeg:
  1. Pick a random point $\alpha \in F^n$.
  2. Compute $\mathrm{rk}\,J_x(f_1,\ldots,f_m)|_{x=\alpha}$ by usual linear-algebra.

- This even works when $f_1,\ldots,f_m$ are given as circuits, using [Baur Strassen'83, Morgenstern'85].

MORAL: Jacobian linearizes our non-linear problem.

Better algorithm ?

- Could we derandomize the algorithm based on the Jacobian?

- We don't know. But we will now relate it to another derandomization question – Graph-matching $\in$? NC.

- Lemma 1: A bipartite graph $G=([n]\cup[n],E)$ has a perfect matching iff $|(E_{ij}x_j^{\,i})_{i,j}|\neq 0$.

The monomials are $x_{\pi(1)}^{\,1}\ldots x_{\pi(n)}^{\,n}$ for some matching π.

$E_{ij}=1$ iff $(i,j)\in E$

- Lemma 2: $|(E_{ij}x_j^{\,i})_{i,j}|\neq 0$ iff $\{f_i:=E_{i1}x_1^{\,i+1}+\ldots+E_{in}x_n^{\,i+1}\}_i$ are algebraically independent.

The i-th row of $J_x(f_1,\ldots,f_n)$ is a multiple of our row!

- Thus, if we could find a hitting-set for the Jacobian then the same hitting-set would put graph-matching in NC!

α's such that $\mathrm{rk}\, J_x(f_1,\ldots,f_m)|_{x=\alpha}$ is correct.

Applications of algebraic independence

Contents

- What is algebraic independence?
- The computational problem
- **<u>I: A formula lower bound</u>**
- **<u>II: A notion of entropy</u>**
- **<u>III: Polynomial identity testing (PIT)</u>**
  - Depth-4 PIT
- At the end …

I: A formula lower bound

- How small a formula can compute the $n \times n$ determinant?
- By computing matrix-powers up to n we can manage in size $n^{\log n}$.

However, a $\mathrm{poly}(n)$ sized circuit suffices!

- Conjecture: Determinant requires a super-polynomial sized formula.
- Theorem [Kalorkoti '85]: $n \times n$ determinant requires $\Omega(n^3)$ sized formula.
- Proof idea: For a subset X of the variables define $\mathrm{trdeg}_X(\det_n)$ to be trdeg of the minors wrt variables in X.
- Show that any formula computing $\det_n$ has size at least $\mathrm{trdeg}_X(\det_n)$. ■

Ⅱ: A notion of entropy

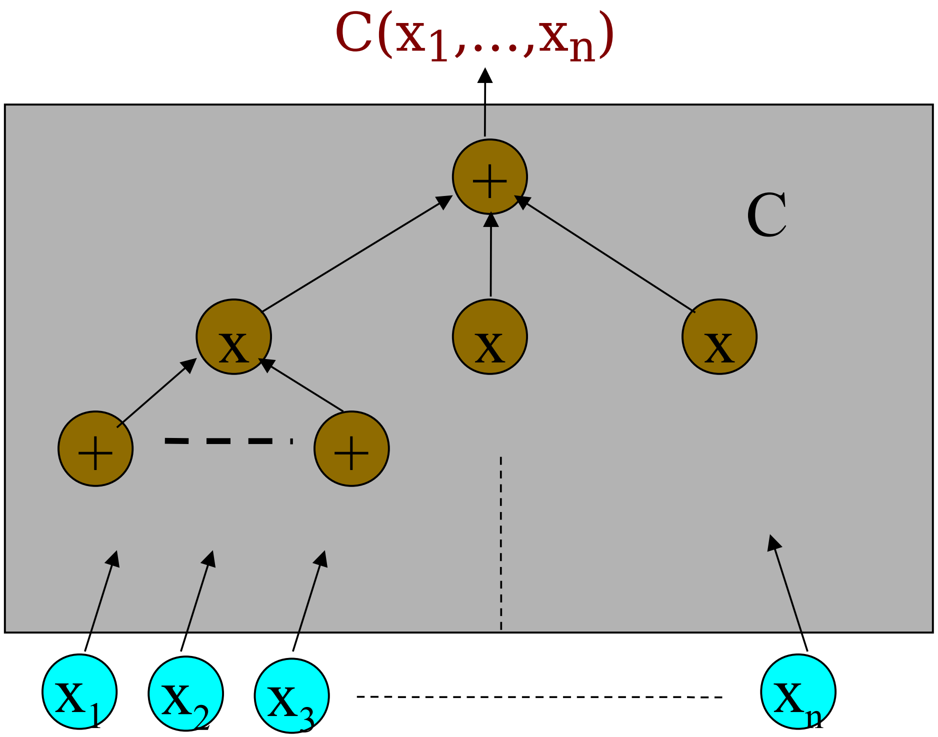
- Let $f_1,\ldots,f_n \in F_p[x_1,\ldots,x_n]$ be polynomials of degrees $\leq d$.
- Consider the map $G\colon F_p^{\ n} \to F_p^{\ n}$ that maps $x=(x_1,\ldots,x_n) \mapsto (f_1(x),\ldots,f_n(x))$.
- What is the image of G on the uniform distribution U?
- Theorem [Wooley '96]: If $f_1,\ldots,f_n$ are algebraically independent and $p>2dn$, then $G(U)$ is close to a uniform distribution.

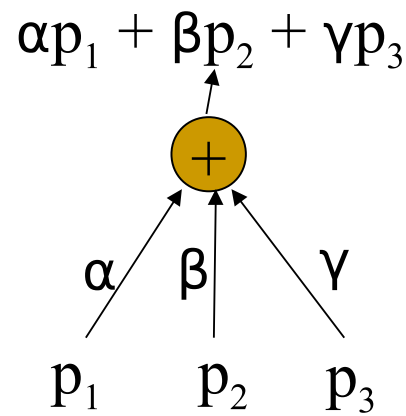
If $\mathrm{trdeg}(f_1,\ldots,f_n)=r$ then the min-entropy of $G(U)$ is close to r.

- [Dvir Gabizon Wigderson '07] used this to construct explicit *extractors*, *condensers* and *dispersers* for polynomial sources.

Ⅲ: Polynomial identity testing (PIT)

- PIT is the problem of testing whether a given arithmetic circuit $C(x_1,\ldots,x_n)$ is identically zero or not.





We want algorithm whose running time is polynomial in size of the circuit.

Randomized poly-time algo exists!

- Blackbox: Cannot look inside C.
- Could only feed values. Hitting-set?

Contents

- What is algebraic independence?
- The computational problem
- I: A formula lower bound
- II: A notion of entropy
- III: Polynomial identity testing (PIT)
  - **Depth-4 PIT**
- At the end …

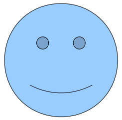
Depth-4 PIT

- The special case where $C(x_1,\ldots,x_n)$ has at most 4 levels.
- Essentially $C(x_1,\ldots,x_n)=\sum_i \prod_j f_{ij}$, where f_{ij} are explicitly given polynomials in variables $x_1,\ldots,x_n$.

Sparse polynomials.

- How easy is PIT for such circuits?
- OPEN, but many partial results are there.
  - [S '08] [Shpilka Volkovich '09] [Karnin Mukhopadhyay Shpilka Volkovich '10] [Arvind Mukhopadhyay '10] [Anderson vanMelkebeek Volkovich '10] [Saraf Volkovich '11] [Saha Saptharishi S '11] [Us '11]....

Depth-4 PIT : Why care?

- It's a natural algebraic problem!
- [Kabanets Impagliazzo '03] Derandomizing PIT implies circuit lower bounds for permanent.
- [Heintz Schnorr '80, Agrawal '05 '06] Hitting-set implies $VP \neq VNP$.
- PIT appears in many algorithms: primality, matching,....
- [Agrawal Vinay '08] Blackbox PIT for depth-4 is *almost* the general case.
- In particular, it being in P implies $VP \neq VNP$ 

Notion of rank for depth-4 - via trdeg

- Let $C(x_1,\ldots,x_n) = \sum_i \prod_j f_{ij}$, where $f_{ij} \in F[x_1,\ldots,x_n]$.
- Definition: Rank $rk(C) := trdeg\{f_{ij}\}_{i,j}$.
- Could we do PIT when $rk(C)$ is *small*?
- $rk(C)$ is like the minimum number of variables needed to describe the 'essence' of C.
- Intuitively, when $rk(C)$ is constant, blackbox PIT should be doable.

Blackbox PIT for low trdeg

- Idea1: Suppose we can construct a linear homomorphism $\psi: F[x_1,\ldots,x_n] \to F[y_1,\ldots,y_r]$ such that:
  - Transcendence degrees up to r are preserved.
  - Definition: Call ψ faithful.

- Ψ will map $C(x_1,\ldots,x_n)$ to $C'(y_1,\ldots,y_r) := C(\psi(x_1),\ldots,\psi(x_n))$.
  - Assume $r=rk(C)$.

- Could a non-identity go to an identity ?

- Theorem [Us]: $C(x_1,\ldots,x_n)=0$ iff $C'(y_1,\ldots,y_r)=0$.
  - An application of Krull's Hauptidealsatz.

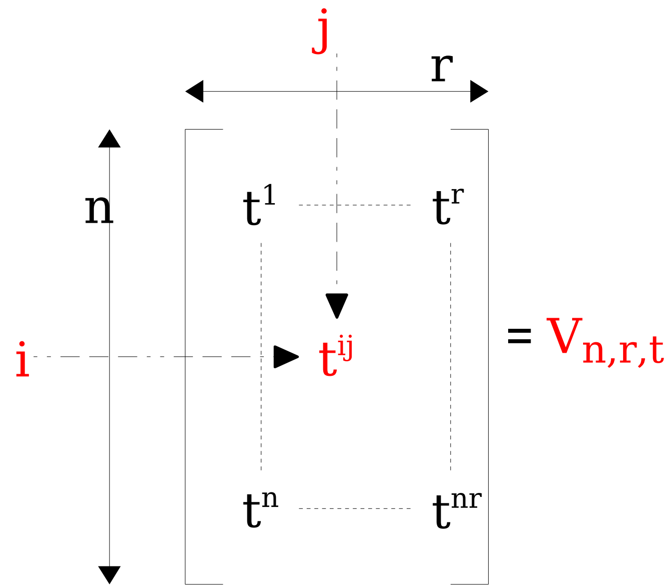
Wolfgang Krull

- Using the faithful map & Schwartz-Zippel we will get a hitting-set for any depth-4 C in time $poly(size(C)^{trdeg(C)})$.

A faithful map

- We construct several faithful maps....
  - Details too scary to present !
- The key property of Jacobian that helps us:
- Fact: For any homomorphism $\varphi: F[x_1,\ldots,x_n] \to F[y_1,\ldots,y_r]$, $J_y(\varphi(f_1),\ldots,\varphi(f_m)) = \varphi(J_x(f_1,\ldots,f_m)) \cdot J_y(\varphi(x_1),\ldots,\varphi(x_n))$.
  - Easy to prove using the chain-rule of derivatives.
- Design φ such that $J_y(\varphi(x_1),\ldots,\varphi(x_n))$ is *Vandermonde*!
  - And, $\varphi(J_x(f_1,\ldots,f_m))$ is of rank r.

Designing a faithful map



- Vandermonde matrix $V_{n,r,t}$ is in $F(t)^{n \times r}$.
  - Think of $r \leq n$.
- Classical fact: $V_{n,r,t}$ has rank r.
- [Gabizon Raz'05] showed a stronger property:
- Theorem [GR'05]: If a matrix A in $F^{r \times n}$ has *full* rank, then $A.V_{n,r,t}$ is an *invertible* matrix over $F(t)$.
  - Thus, $\det(A.V_{n,r,t})$ is a *nonzero* polynomial of *degree* at most nk^2.
  - *Proof:* Do row operations on A and consider the leading term in t.
- We define $\varphi : x_i \mapsto t^{i.1}y_1 + \ldots + t^{i.r}y_r$, for all $i=1,\ldots,n$.

PIT for low trdeg done!

- Recall $J_y(\varphi(f_1),\ldots,\varphi(f_m)) = \varphi(J_x(f_1,\ldots,f_m)) \,.\, J_y(\varphi(x_1),\ldots,\varphi(x_n))$.
- Thus, φ is a faithful map.
- I.e. given circuit C with $rk(C)=r$:
  - $C(x_1,\ldots,x_n)=0$ iff $\varphi\circ C(x_1,\ldots,x_n)=0$,
  - And, $\varphi\circ C(x_1,\ldots,x_n)$ is r-variate,
- So blackbox PIT can be done in $poly(size(C)^r)$ time.

At the end …

- Algebraic independence is a fundamental concept.
  - An elegant randomized test – works for most fields.
- For small characteristic (like $p=2$) ?
  - A gaping hole in the theory...
  - No better test known than PSPACE.
  - OPEN: Find a randomized poly-time test.
- OPEN: A deterministic poly-time test.
- Do all depth-4 identities arise from low trdeg identities?
  - For real depth-3 identities there are such results.

Thank you!