Algebraic Independence

A modest survey

Tushant Mittal

Table of contents

Introduction

Let us generalize the familiar notion of linear dependence.

- A subset S of a field L is algebraically dependent over a subfield K if the elements of S satisfy a non-trivial polynomial equation with coefficients in K.
- **Algebraic/Transcendental Numbers** : $L = \mathbb{C}\ , K = \mathbb{Q}, S = \{\alpha\}$
- **Polynomials** : $L = \mathbb{F}(x_1, \cdots, x_n),\ K = \mathbb{F},\ S = \{f_1, \cdots, f_n\}$

The problem is then,

- Given a set of polynomials $\{f_1, \cdots, f_n\}$ determine if they are algebraically dependent i.e does there $\exists\ A \in\ \mathbb{F}[x_1, \cdots, x_n]$ such that $A(f_1, \cdots, f_n) = 0$. (A is called its annihilating polynomial) .

Why Care?

- Why not? A *natural* algebraic question
- Connections to field of Math like Algebraic Geometry
  - [Płoski ’05] Elementary proof of Bezout’s inequality
  - [Płoski, Jelonek] Proper polynomial maps - relations to Jacobian conjecture
  - Jelonek has given a proof of the effective Nullstellensatz based on Perron’s Theorem
- Algebraic formulation of control theory
- Not convinced yet ?

TCS Applications

Application 1 - Schönhage's Proof

- [Shönhage '76] gave an elementary proof of Strassen's lower bound
- The classical proof uses Bezout's theorem awhose proof is quite involved and uses many tools from Algebraic Geometry

Theorem - Strassen '73

Every circuit computing the n polynomials $x_1^r, x_2^r, \cdots, x_n^r$ has size $\Omega(n \log r)$.

Application 2 - Kalorkoti's Lower Bounds

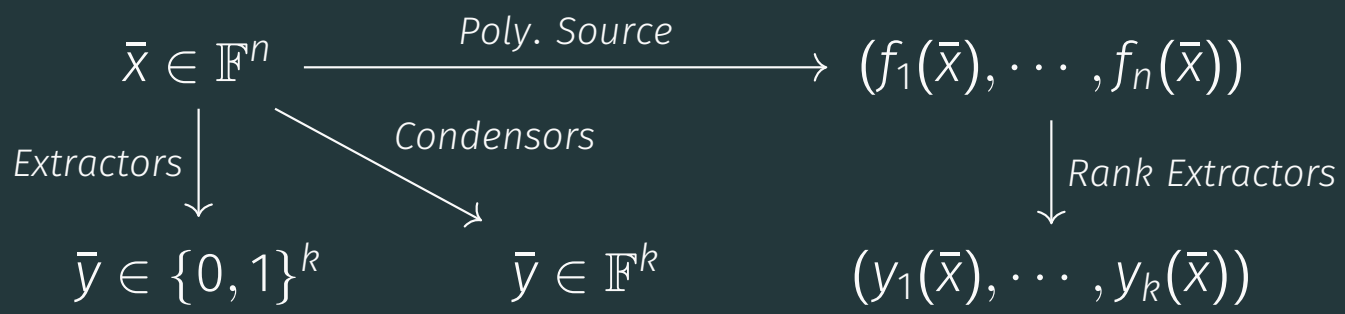
- A formula is an arithmetic circuit in which every gate has outdegree one.
- [Kalorkoti '85] gave a lower bound for formula size of rational functions.

Theorem - Kalorkoti '85

Every formula computing the determinant of an n × n matrix is of size at least $\Omega(n^3)$

Application 3 - Rank Extractors, Condensors

- [Dvir,Gabizon, Wigderson '07] Construction of explicit rank extractors, extractors.
- Rank extractor is set of k polynomial maps that outputs n polynomials to k algebraically independent polynomials of slightly higher degree.
- $E : \mathbb{F}^n \to \{0,1\}^m$ is a extractor for polynomial sources if for every (n, k, d)-polynomial source the random variable $E(X)$ is ϵ^2-close to the uniform distribution on $\{0,1\}^m$.



Application 4 - Depth-4 Blackbox PIT

- Polynomial Independence Testing : Given a circuit, test whether it computes the 0 polynomial.
- Depth 4 means that the circuit represented by $\sum\prod\sum\prod_{\delta}(k,s,n)$ can be written as $\sum_{i=1}^{k}\prod_{j=1}^{s} f_{i,j}$ and degree is bounded by δ.
- [Beecken,Mittmann, Saxena '13] defined a notion of rank for circuits as $rk(C) := trdeg_K\{f_{i,j}\}$

Theorem - BMS '13

Let $r = R_{\delta}(k,s)$. If $char(K) = 0$ or $> \delta^r$, then there is a blackbox $poly(\delta rsn)^{\delta^2 kr}$ time identity test for $\sum\prod\sum\prod_{\delta}(k,s,n)$ circuits

The Easy Case

Characteristic 0 (or large) fields

The earliest criterion was due to *Carl Gustav Jacob Jacobi* in 1841 which naturally leads to a randomized poly-time algorithm .

Theorem - Jacobi

Let $f_i \in K[x]$ be a set of non-constant polynomials with $deg(f_i) < d$ and let $char(K) = 0$ or $> d^r$

$$rk_{K[x]}(J_x(\mathbf{f})) = trdeg(\mathbf{f}) \quad where \;\; J_x(\mathbf{f}) = (\partial_j f_i)_{i,j}$$

or less precisely, $\mathbf{f}$ is algebraically dependent *iff* its Jacobian is 0.

Using the DeMillo-Lipton-Schwartz-Zippel lemma, we can check whether the $det(J_x) = 0$ by evaluating it at a random set of points in polynomial time.

What's the deal with finite characteristic fields ?

- Algebraic dependence depends on the field we are working in. For example, $x + y, x^p + y^p$ are independent over $\mathbb{Q}$ but dependent over $\mathbb{F}_p$ (or any p characteristic field)
- The single polynomial $f = x^p$ has a 0 Jacobian but it is clearly independent.
- Also, p^{th} powers are not the only bad cases. For example, $|J_x(x^{p-1}y,\ xy^{p-1})| = 0$
- Thus, there is no trivial way to "fix" the Jacobian criterion

Partial Results

Sufficient Conditions

Since the Jacobian criterion doesn't hold in the finite characteristic case, we can try to see if there are any unidirectional results

Theorem

Let $f_i \in K[x]$ be a set of non-constant polynomials. If under some monomial ordering σ the th leading coefficient f_is are algebraically independent, then $f_1 \cdots f_n$ are independent

Theorem

If f_is are algebraically dependent, then $rk(J_x(f_1 \cdots f_n)) < n$

These, however, give us no algorithm to compute independence

Is it computable?

Perron's Bound

Oskar Perron in 1927 gave a degree bound for the annihilating polynomial which enables computability via a natural algorithm.

Theorem - Perron

Let $f_i \in K[x_1, \cdots, x_n]$ be a set of $n+1$ non-constant polynomials and let $\delta_i := deg(f_i)$. Then $\exists A \in K[y_1, \cdots, y_{n+1}]$ such that $A(f_1, \cdots, f_{n+1}) = 0$ and

$$deg(A) \leq \frac{\delta_1 \cdots \delta_{n+1}}{min\{\delta_1, \cdots, \delta_{n+1}\}} \leq (max\{\delta_1, \cdots, \delta_{n+1}\})^n$$

Kayal [Kay '09] generalized it to sets with arbitrary number of polynomials over fields of zero characteristic. His result depended on the transcendence degree and was independent of the number of variables. Mittman [Mit '13] generalised Kayal's result to fields of arbitrary characteristic.

Generalized Perron's Bound

Theorem - [Jelonek '05] Generalized Perron

Let $f_i \in K[x_1, \cdots, x_m]$ be a set of $n+1$ non-constant polynomials and let $\delta_i := deg(f_i)$. Assume that $X \subset K^m$ is an affine variety of dimension n and of degree D. If the mapping $F = (f_1, \cdots, f_{n+1}) : X \to K^{n+1}$ is generically finite, then $\exists A \in K[y_1, \cdots, y_{n+1}]$ such that $A(f_1, \cdots, f_{n+1}) = 0$ and $deg(A(y_1^{d_1}, \cdots, y_{n+1}^{d_{n+1}})) \leq D\delta_1 \cdots \delta_{n+1}$

The “trivial” algorithm

- Since, the annihilating polynomial’s degree is bounded we can consider a general equation of the polynomial

$$F = \sum_{\prod_i w_i < d^n} a_w \prod_i {y_i}^{w_i}, \quad a_w \in K$$

- Now substituting the f_is in y_is and setting coefficient of each monomial to 0 will lead to a system of linear equations.
- If no solution exists then the polynomials are independent.
- But since the degree (d^r) is high, this is not an efficient solution and its complexity is in PSPACE.

Computational cul de sac

Bound is tight :-(

Let $\delta_1, \cdots, \delta_n \geq 1$ and consider the polynomials $f_1 := x_1$, $f_2 := x_2 - x_1^{\delta_1}, \cdots, \quad f_n := x_n - x_{n-1}^{\delta_{n-1}}, \quad f_{n+1} := x_n^{\delta_n}$

- Moreover, Kayal showed that computing even the constant term of the annihilating polynomial is $\#P-$hard
- These results thus prove that any route via the annihilating polynomial is inefficient and that other methods have to be devised

A New Criterion

Witt-Jacobian Criterion

- [Mittmann, Saxena, Scheilblechner '12] gave the first non-trivial algoithm to test independence.
- The idea is to lift the problem to a *char* 0 field namely, the p-adic field ($\hat{\mathbb{Z}}_p$).
- Reduces the complexity to $NP^{\#P}$
- Details too gory to present (read, I don't understand it)

A poly-time algorithm ?

Generalizing the Jacobian

- Pandey, Saxena, Sinhababu (2016) gave a new criterion that relates algebraic dependence to approximate functional dependence
- It identifies the *inseparable degree* as a crucial parameter and shows that if a set of polynomials are independent then they can't be *approximately functionally dependent* up to any precision greater than this inseparable degree.
- Conversely, any set of polynomial if truncated beyond their inseparable degree become approximately functionally dependent.
- This gives an algorithm to check if $\mathbf{f}$ is alg. independent by checking approx. functional dependence upto the inseparable degree .

Mathematical Preliminaries

Field Extensions

- If K is a subfield of L then L is said to be a field extension of K denoted by L/K .
- If L/K, then $\alpha \in L$ is said to be algebraic over K if $\exists\, f \in K[x]$ such that $f(\alpha) = 0$. Of all such fs, the one with the lowest degree is called the minimal polynomial of α denoted by $MiPo(\alpha)$.
- If every element of L is algebraic over K, then the extension L/K is said to be an algebraic extension; otherwise it is said to be a transcendental extension.
- An algebraic extension L/K is said to be separable if $\forall \alpha \in L, MiPo(\alpha)$ has no repeated roots in its splitting field.

The Theorem

Denote $\mathbf{f} = \{f_1, \cdots, f_m\}$

Theorem

If trdeg $\mathbf{f} = k$, then there exist algebraically independent $\{g_1, \cdots, g_k\} \subset \mathbf{f}$ such that for random $a \in \bar{\mathbb{F}}^n$, there are polynomials $h_i \in \bar{\mathbb{F}}[Y_1, \cdots, Y_k]$ satisfying, $\forall\, i \in [m]$,
$f_i^{\leq t}(x+a) = h_i^{\leq t}(g_1(x+a), ..., g_k(x+a))$

Theorem

If $\mathbf{f}$ are algebraically independent with inseparable degree p^i. Then,

- $\forall\, 1 \leq t \leq p^i$ for random $a \in \bar{\mathbb{F}}^n$ $\exists h_j \in \bar{\mathbb{F}}[Y_1, \cdots, Y_{n-1}]$, $\forall\, j \in [m]$,
  $f_j^{\leq t}(x+a) = h_j^{\leq t}(f_1(x+a), \cdots, f_{j-1}(x+a), f_{j+1}(x+a), \cdots, f_n(x+a))$
- $\forall\, t > p^i$ for random $a \in \bar{\mathbb{F}}^n$ $\nexists h$,
  $f_n^{\leq t}(x+a) = h^{\leq t}(f_1(x+a), \cdots, f_{n-1}(x+a))$

Proof in the next talk !

Questions?

References

- *Zeev Dvir, Ariel Gabizon, and Avi Wigderson*. Extractors and rank extractors for polynomial sources. Computational Complexity, 18(1):1–58, 2009.
- *K. A. Kalorkoti*. A Lower Bound for the Formula Size of Rational Functions. SIAM J. on Computing, 14(3):678–687, 1985
- *Neeraj Kayal*. The Complexity of the Annihilating Polynomial. In Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC), pages 184–193, 2009
- *Malte Beecken, Johannes Mittmann, and Nitin Saxena*. Algebraic independence and blackbox identity testing. Information and Computation, 222:2–19, 2013
- *Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner*. Algebraic Independence in Positive Characteristic – A p-Adic Calculus

References

- *Oskar Perron*. Algebra I (Die Grundlagen). Walter de Gruyter, Berlin, 1927
- *Arkadiusz Ploski*. Algebraic Dependence of Polynomials After O. Perron and Some Applications. In Svetlana Cojocaru, Gerhard Pfister, and Victor Ufnarovski, editors, Computational Commutative and Non-Commutative Algebraic Geometry, pages 167– 173. IOS Press, 2005
- *Mittmann*, Independence in Algebraic Complexity Theory, Master's Thesis
- *V. Strwsen*, Die Berechnungskomgiexität von elementarsymmetrischen Funktionen und van Interpolationskoeffizienten, .Numer.Math. 20 (1973) 238-251.