Toward an Algorithmic Theory of Polynomials

Alperen A. Ergür

Carnegie Mellon University
School of Computer Science

Dec 02, 2019

Outline of today's Colloquium

Outline of today's Colloquium

1. Examples from a variety of subjects with connections to polynomials

Outline of today's Colloquium

1. Examples from a variety of subjects with connections to polynomials
2. Basic Algebraic Geometry with a computational lens

Outline of today's Colloquium

1. Examples from a variety of subjects with connections to polynomials
2. Basic Algebraic Geometry with a computational lens
3. Revisiting the introductory examples with an algebra-geometric perspective

Part I
Examples

Extremal Combinatorics

Extremal Combinatorics

Example

Let P be a set of points in the real plane, and let L be set of lines. How many incidences can happen between the elements of P and L?

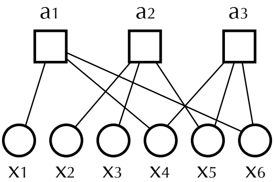
Extremal Combinatorics

Example

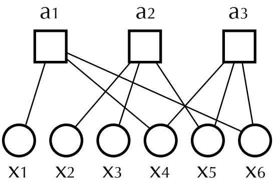
Let P be a set of points in the real plane, and let L be set of lines. How many incidences can happen between the elements of P and L?

Incidence geometry is tightly connected to randomness extraction in computer science, and also to harmonic analysis and number theory.

Probabilistic Combinatorics



Probabilistic Combinatorics



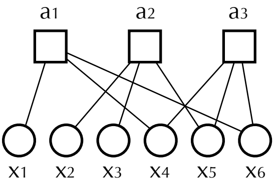
Example

Define a random bipartite graph with m check nodes and n variable nodes as follows

- each check node has degree k, and each variable node has degree $\frac{km}{n}$
- edges have weights from an arbitrary distribution over $\mathbb{F}^*$ for a field $\mathbb{F}$

Let A be the $m \times n$ random matrix defined by this graph. What is the rank of A?

Probabilistic Combinatorics



Example

Define a random bipartite graph with m check nodes and n variable nodes as follows

- each check node has degree k, and each variable node has degree $\frac{km}{n}$
- edges have weights from an arbitrary distribution over $\mathbb{F}^*$ for a field $\mathbb{F}$

Let A be the $m \times n$ random matrix defined by this graph. What is the rank of A?

The rank is the rate of ldpc codes that you probabaly have in your pocket.

Quantum Information Theory

Quantum Information Theory

$A \succ 0$ means A is a PSD matrix.

A map $\phi : \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$ is positive if $\phi(A) \succ 0$ for all $A \succ 0$.

Positive maps are used to detect entanglement.

Quantum Information Theory

$A \succ 0$ means A is a PSD matrix.

A map $\phi : \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$ is positive if $\phi(A) \succ 0$ for all $A \succ 0$.

Positive maps are used to detect entanglement.

Completely positive maps are "nice" positive maps.

Quantum Information Theory

$A \succ 0$ means A is a PSD matrix.

A map $\phi : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ is positive if $\phi(A) \succ 0$ for all $A \succ 0$.

Positive maps are used to detect entanglement.

Completely positive maps are "nice" positive maps.
ϕ is k-positive if the map

$$\phi^k : \mathbb{R}^{k\times k} \otimes \mathbb{R}^{n\times n} \to \mathbb{R}^{k\times k} \otimes \mathbb{R}^{n\times n}$$

$$\phi^k(M \otimes A) = M \otimes \phi(A)$$

is positive. ϕ is completely positive if it is positive for all k.

Quantum Information Theory

Quantum Information Theory

Send ϕ to a biquadratic polynomial by $p_\phi(x, y) = y^T \phi(xx^T) y$. Then,

- ϕ is positive if $p_\phi(x, y) \geq 0$ for all x, y.
- ϕ is completely positive if $p_\phi(x, y) = \sum h_i(x, y)^2$ for some h_i.

Quantum Information Theory

Send ϕ to a biquadratic polynomial by $p_\phi(x,y) = y^T \phi(xx^T) y$. Then,

- ϕ is positive if $p_\phi(x,y) \geq 0$ for all x, y.
- ϕ is completely positive if $p_\phi(x,y) = \sum h_i(x,y)^2$ for some h_i.

We can optimize over completely positive maps (sum of squares) using semidefinite programming.

Quantum Information Theory

Send ϕ to a biquadratic polynomial by $p_\phi(x, y) = y^T \phi(xx^T)y$. Then,

- ϕ is positive if $p_\phi(x, y) \geq 0$ for all x, y.
- ϕ is completely positive if $p_\phi(x, y) = \sum h_i(x, y)^2$ for some h_i.

We can optimize over completely positive maps (sum of squares) using semidefinite programming.

What percentage of positive maps are completely positive?

What percentage of biquadratic nonnegative polynomials are sum of squares?

Biochemical Reaction Networks

Biochemical Reaction Networks

We have two input data: $A = \{a_1, a_2, \ldots, a_t\} \subset \mathbb{Z}^n$, $n \times t$ matrix κ.
The pair (κ, A) models a system of equations:

Biochemical Reaction Networks

We have two input data: $A = \{a_1, a_2, \ldots, a_t\} \subset \mathbb{Z}^n$, $n \times t$ matrix κ.
The pair (κ, A) models a system of equations:

$$f_1(x) = \sum_{i=1}^{t} \kappa_{1i} x^{a_i}, f_2(x) = \sum_{i=1}^{t} \kappa_{2i} x^{a_i}, \ldots, f_n(x) = \sum_{i=1}^{t} \kappa_{ni} x^{a_i}$$

Biochemical Reaction Networks

We have two input data: $A = \{a_1, a_2, \ldots, a_t\} \subset \mathbb{Z}^n$, $n \times t$ matrix κ.
The pair (κ, A) models a system of equations:

$$f_1(x) = \sum_{i=1}^{t} \kappa_{1i} x^{a_i}, f_2(x) = \sum_{i=1}^{t} \kappa_{2i} x^{a_i}, \ldots, f_n(x) = \sum_{i=1}^{t} \kappa_{ni} x^{a_i}$$

How many $x \in \mathbb{R}^n_+$ are there with $f_1(x) = f_2(x) = \ldots = f_n(x) = 0$?

Biochemical Reaction Networks

We have two input data: $A = \{a_1, a_2, \ldots, a_t\} \subset \mathbb{Z}^n$, $n \times t$ matrix κ.
The pair (κ, A) models a system of equations:

$$f_1(x) = \sum_{i=1}^{t} \kappa_{1i} x^{a_i}, f_2(x) = \sum_{i=1}^{t} \kappa_{2i} x^{a_i}, \ldots, f_n(x) = \sum_{i=1}^{t} \kappa_{ni} x^{a_i}$$

How many $x \in \mathbb{R}^n_+$ are there with $f_1(x) = f_2(x) = \ldots = f_n(x) = 0$?

$$\frac{\mathrm{d}x}{\mathrm{d}t} = (f_1(x), f_2(x), \ldots, f_n(x))$$

Mass kinematics equation models the dynamical system, we want to count equlibrium (steady) states.

What was common in all the examples?

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)
- Examples are mostly about real zeros, not complex

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)
- Examples are mostly about real zeros, not complex
- In the worst case all these problems are NP-Hard

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)
- Examples are mostly about real zeros, not complex
- In the worst case all these problems are NP-Hard

What needs to be done then?

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)
- Examples are mostly about real zeros, not complex
- In the worst case all these problems are NP-Hard

What needs to be done then?

- Develop structure aware theorems and algorithms

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)
- Examples are mostly about real zeros, not complex
- In the worst case all these problems are NP-Hard

What needs to be done then?

- Develop structure aware theorems and algorithms
- Distinguish between the real and complex geometry

What was common in all the examples?

- Translates to a problem of solving, optimizing, or counting zeros of polynomials
- Corresponding polynomials are structured (e.g. sparse)
- Examples are mostly about real zeros, not complex
- In the worst case all these problems are NP-Hard

What needs to be done then?

- Develop structure aware theorems and algorithms
- Distinguish between the real and complex geometry
- Go beyond the worst case and understand typical instances

Part II

Basic Algebraic Geometry with a Computational Lens

Going back to the beginnings

We go back to univariate polynomials: Let $0 < a_1 < \ldots < a_t$ be a sequence of integers, and consider the following univariate polynomial

$$p(x) = c_0 + c_1 x^{a_1} + \ldots + c_t x^{a_t}$$

where c_i are real numbers. How many zeros does p have?

Going back to the beginnings

We go back to univariate polynomials: Let $0 < a_1 < \ldots < a_t$ be a sequence of integers, and consider the following univariate polynomial

$$p(x) = c_0 + c_1 x^{a_1} + \ldots + c_t x^{a_t}$$

where c_i are real numbers. How many zeros does p have?

1. Fundamental Theorem of Algebra: p has a_t many zeros over the complex numbers.
2. Descartes Rule of Signs: The number of real zeros of p depends on the coefficients, but it is at most $2t$.

Going back to the beginnings

We go back to univariate polynomials: Let $0 < a_1 < \ldots < a_t$ be a sequence of integers, and consider the following univariate polynomial

$$p(x) = c_0 + c_1 x^{a_1} + \ldots + c_t x^{a_t}$$

where c_i are real numbers. How many zeros does p have?

1. Fundamental Theorem of Algebra: p has a_t many zeros over the complex numbers.
2. Descartes Rule of Signs: The number of real zeros of p depends on the coefficients, but it is at most $2t$.

Example

Consider $p(x) = 3 + 5x + 7x^{100}$. It has at most 4 real zeros, and 100 complex zeros.

Basic Algebraic Geometry

Theorem (Bézout)

Let $p = (p_1, \ldots, p_{n-1})$ be a system of homogenous polynomials with n variables where p_i have degree d. Then the polynomial system p has at most d^{n-1} many non-degenerate zeros, and this bound is generically exact.

Basic Algebraic Geometry

Theorem (Bézout)

Let $p = (p_1, \ldots, p_{n-1})$ be a system of homogenous polynomials with n variables where p_i have degree d. Then the polynomial system p has at most d^{n-1} many non-degenerate zeros, and this bound is generically exact.

Example

Let A be a $n \times n$ matrix, and consider the eigenpair problem:

$$(A - \lambda)x = 0$$

This is a quadratic system of equations in (λ, x).
Bézout's theorem gives the bound 2^n.

Basic Algebraic Geometry

Basic Algebraic Geometry

Theorem (Kushnirenko, 70's)

Let $A = \{a_1, a_2, \ldots, a_m\} \subset \mathbb{Z}^n$ be set of lattice points. Consider the following polynomial equations

$$p_1(x) = \sum_{i=1}^{m} c_{1i} x^{a_i}, \ldots, p_n(x) = \sum_{i=1}^{m} c_{ni} x^{a_i}$$

Then the system of equations $p = (p_1, p_2, \ldots, p_n)$ has at most $|conv(A)|$ many non-degenerate zeros (where $|.|$ denotes volume), and this bound is generically exact.

Basic Algebraic Geometry

Theorem (Kushnirenko, 70's)

Let $A = \{a_1, a_2, \ldots, a_m\} \subset \mathbb{Z}^n$ *be set of lattice points. Consider the following polynomial equations*

$$p_1(x) = \sum_{i=1}^{m} c_{1i} x^{a_i}, \ldots, p_n(x) = \sum_{i=1}^{m} c_{ni} x^{a_i}$$

Then the system of equations $p = (p_1, p_2, \ldots, p_n)$ *has at most* $|conv(A)|$ *many non-degenerate zeros (where* $|.|$ *denotes volume), and this bound is generically exact.*

This theorem gives the bound $2n$ for the eigenpair problem.

Basic Algebraic Geometry

Theorem (Kushnirenko, 70's)

Let $A = \{a_1, a_2, \ldots, a_m\} \subset \mathbb{Z}^n$ be set of lattice points. Consider the following polynomial equations

$$p_1(x) = \sum_{i=1}^{m} c_{1i} x^{a_i}, \ldots, p_n(x) = \sum_{i=1}^{m} c_{ni} x^{a_i}$$

Then the system of equations $p = (p_1, p_2, \ldots, p_n)$ has at most $|conv(A)|$ many non-degenerate zeros (where $|.|$ denotes volume), and this bound is generically exact.

This theorem gives the bound $2n$ for the eigenpair problem.
There is a series of papers titled complexity of Bézout's theorem, but there is no paper (yet) titled complexity of Kushnirenko's theorem.

An example

Example

$$f_1 = 10500t - t^2u^{492} - 3500u^{463}v^5w^5$$
$$f_2 = 10500t - t^2 - 3500u^{691}v^5w^5$$
$$f_3 = 14000 - 2t + tu^{492} - 2500v$$
$$f_4 = 14000 + 2t - tu^{492} - 3500w$$

How many zeros are there?

1. Bezout bound: 82 billion in $\mathbb{C}^4$
2. Volume (Kushnirenko) bound: 7663 in $(\mathbb{C}^*)^4$
3. Number of positive real zeros: 6 in $(\mathbb{R}_+)^4$

What happens over the reals?

What happens over the reals?

Theorem (Khovanskii, 1988)

Let $A = \{a_1, a_2, \ldots, a_t\} \subset \mathbb{Z}^n$ be set of lattice points. Consider the following polynomial equations

$$p_1(x) = \sum_{i=1}^{t} c_{1i} x^{a_i}, \ldots, p_n(x) = \sum_{i=1}^{t} c_{ni} x^{a_i}$$

Then the system of equations $p = (p_1, p_2, \ldots, p_n)$ has at most

$$2^{\binom{t-1}{2}} (n+1)^{t-1}$$

non-degenerate real zeros.

What happens over the reals?

Kushnirenko's Conjecture, 70's

Fix the number of variables n. The number non-degenerate real solutions to a system of polynomials with t terms is bounded by t^n.

What happens over the reals?

Kushnirenko's Conjecture, 70's

Fix the number of variables n. The number non-degenerate real solutions to a system of polynomials with t terms is bounded by t^n.

Example

Consider a system of two polynomials, two variables, with 8 terms in each. Khovanskii says $2^{21} \times 3^7$, Kushnirenko claims 64.

What happens over the reals?

Kushnirenko's Conjecture, 70's

Fix the number of variables n. The number non-degenerate real solutions to a system of polynomials with t terms is bounded by t^n.

Example

Consider a system of two polynomials, two variables, with 8 terms in each. Khovanskii says $2^{21} \times 3^7$, Kushnirenko claims 64.

In general, this conjecture is open for any fixed $n \geq 2$. Descartes solved $n = 1$ in 1636.

What happens typically over the reals?

What happens typically over the reals?

Let $A \subset \mathbb{Z}^n$ be a set of cardinality t, and let $\sigma : A \to \mathbb{R}_+$ be a function. We consider the following system of random polynomials:

$$f_1(x) = \sum_{\alpha \in A} \sigma(\alpha)\xi_{1\alpha}x^\alpha, \ldots, f_n(x) = \sum_{\alpha \in A} \sigma(\alpha)\xi_{n\alpha}x^\alpha$$

where $\xi_{i\alpha}$ are i.i.d. standard Gaussian random variables.

What happens typically over the reals?

Let $A \subset \mathbb{Z}^n$ be a set of cardinality t, and let $\sigma : A \to \mathbb{R}_+$ be a function. We consider the following system of random polynomials:

$$f_1(x) = \sum_{\alpha \in A} \sigma(\alpha)\xi_{1\alpha} x^\alpha, \ldots, f_n(x) = \sum_{\alpha \in A} \sigma(\alpha)\xi_{n\alpha} x^\alpha$$

where $\xi_{i\alpha}$ are i.i.d. standard Gaussian random variables.

Theorem (Bürgisser, Ergür, Tonelli-Cueto, 19)

Let $E(A, \sigma)$ denote the expected number of non-degenerate real zeros of $f = (f_1, f_2, \ldots, f_n)$. Then, we have

$$E(A, \sigma) \leq 2\binom{t}{n} \leq 2t^n.$$

What happens typically over the reals?

Let $A \subset \mathbb{Z}^n$ be a set of cardinality t, and let $\sigma : A \to \mathbb{R}_+$ be a function. We consider the following system of random polynomials:

$$f_1(x) = \sum_{\alpha \in A} \sigma(\alpha)\xi_{1\alpha}x^{\alpha}, \ldots, f_n(x) = \sum_{\alpha \in A} \sigma(\alpha)\xi_{n\alpha}x^{\alpha}$$

where $\xi_{i\alpha}$ are i.i.d. standard Gaussian random variables.

Theorem (Bürgisser, Ergür, Tonelli-Cueto, 19)

Let $E(A, \sigma)$ denote the expected number of non-degenerate real zeros of $f = (f_1, f_2, \ldots, f_n)$. Then, we have

$$E(A, \sigma) \leq 2\binom{t}{n} \leq 2t^n.$$

This confirms Kushnirenko's conjecture for average instances.

Complexity of Bézout's Theorem

Smale's 17th Problem

Can a zero of a system of n complex polynomial equatins in n unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?

Complexity of Bézout's Theorem

Smale's 17th Problem

Can a zero of a system of *n* complex polynomial equatins in *n* unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?

Smale adds: Similar but harder questions can be asked over the reals.

Complexity of Bézout's Theorem

Theorem (Shub, Smale, Beltran, Pardo, Bürgisser, Cucker, Lairez)

There exists an algorithm that computes a zero of a system of equations $(p_1, p_2, \ldots, p_n)$ *with degrees* $d_1, d_2, \ldots, d_n$ *on average time*

$$O(nd^{\frac{3}{2}} N^2) \text{ where } N = \sum_{i=1}^{n} \binom{n+d_i}{d_i}, d = \max_i d_i$$

and average is with respect to Kostlan-Shub-Smale ensemble.

Complexity of Bézout's Theorem

Theorem (Shub, Smale, Beltran, Pardo, Bürgisser, Cucker, Lairez)

There exists an algorithm that computes a zero of a system of equations $(p_1, p_2, \dots, p_n)$ with degrees $d_1, d_2, \dots, d_n$ on average time

$$O(nd^{\frac{3}{2}} N^2) \text{ where } N = \sum_{i=1}^{n} \binom{n+d_i}{d_i}, d = \max_i d_i$$

and average is with respect to Kostlan-Shub-Smale ensemble.

Complexity of Bézout series started in Berkeley, 1992, and the solution of Smale's 17th problem was completed in Berlin, 2015.

Homotopy Continuation Algorithms

Main idea behind the solution of Smale's 17th problem: Homotopy continuation.

Homotopy Continuation Algorithms

Main idea behind the solution of Smale's 17th problem: Homotopy continuation.

1. Pick an "easy" polynomial system g that you know how to solve
2. Deform "easy" g into your target system f
3. Track the change in the zeros of $(1-t)g + tf$ for $t \in [0,1]$ by Newton's method

So, are we done?

Homotopy Continuation Algorithms

Main idea behind the solution of Smale's 17th problem: Homotopy continuation.

1. Pick an "easy" polynomial system g that you know how to solve
2. Deform "easy" g into your target system f
3. Track the change in the zeros of $(1-t)g + tf$ for $t \in [0,1]$ by Newton's method

So, are we done?

- The solution of Smale's 17th takes a random polynomial system g with a very specific distribution which has special algebraic properties.
- These special properties obstruct solving structured polynomials.

Homotopy Continuation Algorithms

Main idea behind the solution of Smale's 17th problem: Homotopy continuation.

1. Pick an "easy" polynomial system g that you know how to solve
2. Deform "easy" g into your target system f
3. Track the change in the zeros of $(1-t)g + tf$ for $t \in [0,1]$ by Newton's method

So, are we done?

- The solution of Smale's 17th takes a random polynomial system g with a very specific distribution which has special algebraic properties.
- These special properties obstruct solving structured polynomials.
- $N = \sum_{i=1}^{n} \binom{n+d_i}{d_i}$ is huge!

Homotopy Continuation Algorithms

Main idea behind the solution of Smale's 17th problem: Homotopy continuation.

1. Pick an "easy" polynomial system g that you know how to solve
2. Deform "easy" g into your target system f
3. Track the change in the zeros of $(1-t)g + tf$ for $t \in [0,1]$ by Newton's method

So, are we done?

- The solution of Smale's 17th takes a random polynomial system g with a very specific distribution which has special algebraic properties.
- These special properties obstruct solving structured polynomials.
- $N = \sum_{i=1}^{n} \binom{n+d_i}{d_i}$ is huge!
- Practically works well for finding all complex zeros: Bertini, PSS5, PHCPack, JuliaHomotopy

Complexity of Kushnirenko's Theorem

Sparse Smale's 17th Problem

Let $A \subset \mathbb{Z}^n$ be a set of t lattice points with bounded degree d. Is there an algorithm that finds a complex zero of a of system of n polynomial equations with support set A on average time $poly(t, n, \log(d))$?

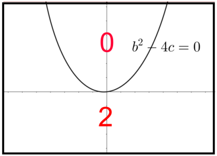
Complexity of Kushnirenko's Theorem

Sparse Smale's 17th Problem

Let $A \subset \mathbb{Z}^n$ be a set of t lattice points with bounded degree d. Is there an algorithm that finds a complex zero of a of system of n polynomial equations with support set A on average time $poly(t, n, \log(d))$?

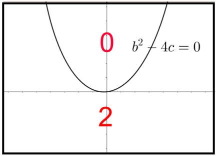
Necessary tool box under development: Ergür, Rojas, Paouris (18 and 19), Malajovich (17 and 19), Ergür and Malajovich (ongoing work).

Smale's Question over the Reals



How many real zeros does $x^2 + bx + c$ have? It is determined by the equation $b^2 - 4c$.

Smale's Question over the Reals

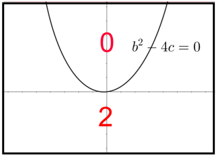


How many real zeros does $x^2 + bx + c$ have? It is determined by the equation $b^2 - 4c$.

How many real zeros does the following simple system of equations have?

$$p_1(x, y) = x^6 + by^3 - y \,,\; p_2(x, y) = y^6 + cx^3 - x$$

Smale's Question over the Reals



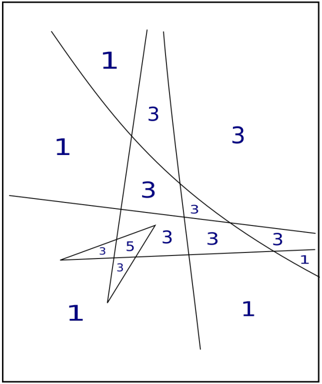
How many real zeros does $x^2 + bx + c$ have? It is determined by the equation $b^2 - 4c$.

How many real zeros does the following simple system of equations have?

$$p_1(x, y) = x^6 + by^3 - y \ , \ p_2(x, y) = y^6 + cx^3 - x$$

The corresponding discriminant equation has degree 36 with very large coefficients, it fills pages.

Handling the Discriminant Variety



X is a complex algebraic variety in $(\mathbb{C}^*)^m$.

$$Log : X \to \mathbb{R}^m \;,\; Log(z_1, \ldots, z_n) = (log|z_1|, \ldots, log|z_n|)$$

This is called amoeba of a variety.

Real Homotopy Continuation Algorithm

Let be a set of lattice points $A \subset \mathbb{Z}^n$ with t elements, and let $p = (p_1, p_2, \ldots, p_n)$ be a system of equations supported with A.

Real Homotopy Continuation Algorithm

Let be a set of lattice points $A \subset \mathbb{Z}^n$ with t elements, and let $p = (p_1, p_2, \ldots, p_n)$ be a system of equations supported with A.

Theorem (Ergür, de Wolff, 19)

If p is located in the unbounded components of the complement of discriminant amoeba, then p has at most $O(t^n)$ many real zeros. Moreover, there exist a real homotopy algorithm to compute the real zeros of p.

Real Homotopy Continuation Algorithm

Let be a set of lattice points $A \subset \mathbb{Z}^n$ with t elements, and let $p = (p_1, p_2, \ldots, p_n)$ be a system of equations supported with A.

Theorem (Ergür, de Wolff, 19)

If p is located in the unbounded components of the complement of discriminant amoeba, then p has at most $O(t^n)$ many real zeros. Moreover, there exist a real homotopy algorithm to compute the real zeros of p.

The algorithm also provides a certificate of being in the unbounded components of the amoeba complement.

Part III

Revisiting the examples with an algebra-geometric perspective

Multihomogenous Nonnegative Polynomials

$H_{n,2d}$: $2d$ homogenous in first n variables, and $2d$ homogenous in the second n variables.

$$p(x) = x_1^2 x_3 x_4 + x_2^2 x_3^2 + x_1 x_2 x_4^2 \quad p \in H_{2,2}$$

Multihomogenous Nonnegative Polynomials

$H_{n,2d}$: $2d$ homogenous in first n variables, and $2d$ homogenous in the second n variables.

$$p(x) = x_1^2 x_3 x_4 + x_2^2 x_3^2 + x_1 x_2 x_4^2 \quad p \in H_{2,2}$$

$$P_{n,2d} := \{p \in H_{n,2d} : p(x,y) \geq 0 \text{ for every } (x,y) \in \mathbb{R}^{2n}\}$$

$$\Sigma_{n,2d} := \{p \in H_{n,2d} : p(x,y) = \sum h_i(x,y)^2 \text{ for some } h_i \in H_{n,d}\}$$

Multihomogenous Nonnegative Polynomials

$H_{n,2d}$: $2d$ homogenous in first n variables, and $2d$ homogenous in the second n variables.

$$p(x) = x_1^2 x_3 x_4 + x_2^2 x_3^2 + x_1 x_2 x_4^2 \quad p \in H_{2,2}$$

$$P_{n,2d} := \{p \in H_{n,2d} : p(x,y) \geq 0 \text{ for every } (x,y) \in \mathbb{R}^{2n}\}$$

$$\Sigma_{n,2d} := \{p \in H_{n,2d} : p(x,y) = \sum h_i(x,y)^2 \text{ for some } h_i \in H_{n,d}\}$$

We define the following hyperplane:

$$L := \{p \in H_{n,2d} : \int_{S^{n-1}} \int_{S^{n-1}} p(x,y)\, \sigma(x)\, \sigma(y) = 1\}$$

Multihomogenous Nonnegative Polynomials

$H_{n,2d}$: $2d$ homogenous in first n variables, and $2d$ homogenous in the second n variables.

$$p(x) = x_1^2 x_3 x_4 + x_2^2 x_3^2 + x_1 x_2 x_4^2 \quad p \in H_{2,2}$$

$$P_{n,2d} := \{p \in H_{n,2d} : p(x,y) \geq 0 \text{ for every } (x,y) \in \mathbb{R}^{2n}\}$$

$$\Sigma_{n,2d} := \{p \in H_{n,2d} : p(x,y) = \sum h_i(x,y)^2 \text{ for some } h_i \in H_{n,d}\}$$

We define the following hyperplane:

$$L := \{p \in H_{n,2d} : \int_{S^{n-1}} \int_{S^{n-1}} p(x,y)\, \sigma(x)\, \sigma(y) = 1\}$$

Theorem (Ergür, 2018)

$$c_1 \pi^{-2d} \left(\frac{n}{2} + 2d\right)^{-2d} \leq \frac{|\Sigma_{n,2d} \cap L|}{|P_{n,2d} \cap L|} \leq c_2 n^{\frac{1}{2}} \left(\frac{n}{d} + 1\right)^{-2d}$$

Sum of Squares Hierarchy

Sum of Squares Hierarchy

Theorem (Putinar,93)

Consider the following semialgebraic set

$$\mathcal{V} := \{x \in \mathbb{R}^n : g_1(x) \geq 0, g_2(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

If g_i creates an Archimedean quadratic module (a technical condition a bit stronger then assuming $\mathcal{V}$ is compact), then

$$f(x) > 0 \textit{ for all } x \in \mathcal{V} \Leftrightarrow f(x) = u_o(x) + \sum_{i=1}^{m} g_i(x) u_i(x)$$

where u_i are sum of squares.

Sum of Squares Hierarchy

Theorem (Putinar,93)

Consider the following semialgebraic set

$$\mathcal{V} := \{x \in \mathbb{R}^n : g_1(x) \geq 0, g_2(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

If g_i creates an Archimedean quadratic module (a technical condition a bit stronger then assuming $\mathcal{V}$ is compact), then

$$f(x) > 0 \textit{ for all } x \in \mathcal{V} \Leftrightarrow f(x) = u_o(x) + \sum_{i=1}^{m} g_i(x) u_i(x)$$

where u_i are sum of squares.

I am interested in bounds on the degrees of u_i for typical situations.

Grids and Incidence Geometry

Grids and Incidence Geometry

Let $n = \lambda_1 + \lambda_2 + \ldots + \lambda_m$ be an m partition of n. Let $S_i \subseteq \mathbb{C}^{\lambda_i}$ be finite sets.

$$S := S_1 \times S_2 \times \ldots \times S_m \subset \mathbb{C}^n$$

be a multigrid.

Grids and Incidence Geometry

Let $n = \lambda_1 + \lambda_2 + \ldots + \lambda_m$ be an m partition of n. Let $S_i \subseteq \mathbb{C}^{\lambda_i}$ be finite sets.

$$S := S_1 \times S_2 \times \ldots \times S_m \subset \mathbb{C}^n$$

be a multigrid.

Example

Let $S_1 \subset \mathbb{C}^2$ represent points, let $S_2 \subset \mathbb{C}^2$ represent lines $ay + bz + 1 = 0$. Define the polynomial $p(x) = x_3x_1 + x_4x_2 + 1$.

$$|Z(p) \cap S_1 \times S_2| = \text{ number of incidences between points and lines}$$

The Multivariate Schwartz-Zippel Lemma

Theorem (Dogan, Ergür, Tsigaridas, Mundo, 19)

Let p be a degree d and λ-irreducible polynomial, then for any $\varepsilon > 0$ we have

$$|Z(p) \cap S| = O_{d,\varepsilon}\left(\prod_{i=1}^{m} |S_i|^{1+\varepsilon-\frac{1}{\lambda_i}} + \sum_{i} \prod_{j \neq i} |S_j|\right)$$

The Multivariate Schwartz-Zippel Lemma

Theorem (Dogan, Ergür, Tsigaridas, Mundo, 19)

Let p be a degree d and λ-irreducible polynomial, then for any $\varepsilon > 0$ we have

$$|Z(p) \cap S| = O_{d,\varepsilon}\left(\prod_{i=1}^{m} |S_i|^{1+\varepsilon-\frac{1}{\lambda_i}} + \sum_i \prod_{j \neq i} |S_j| \right)$$

We have an algorithm to detect λ-reducibility, let's skip the definition for now.

The Multivariate Schwartz-Zippel Lemma

Theorem (Dogan, Ergür, Tsigaridas, Mundo, 19)

Let p be a degree d and λ-irreducible polynomial, then for any $\varepsilon > 0$ we have

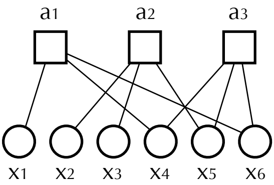
$$|Z(p) \cap S| = O_{d,\varepsilon}\left(\prod_{i=1}^{m} |S_i|^{1+\varepsilon-\frac{1}{\lambda_i}} + \sum_{i} \prod_{j \neq i} |S_j|\right)$$

We have an algorithm to detect λ-reducibility, let's skip the definition for now.

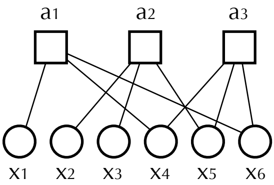
For $m = 2$, we have

$$|Z(p) \cap S| = O_{d,\varepsilon}\left(|S_1|^{1-\frac{1}{\lambda_1}+\varepsilon}|S_2|^{1-\frac{1}{\lambda_2}+\varepsilon} + |S_1| + |S_2|\right)$$

A Sparse Random Matrix Model

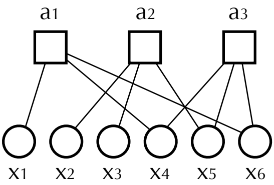


A Sparse Random Matrix Model



- let $\mathbb{F}$ be a field and let $\mathbf{d}, \mathbf{k}$ satisfy $\mathbb{E}[\mathbf{d}^2], \mathbb{E}[\mathbf{k}^2] < \infty$

A Sparse Random Matrix Model

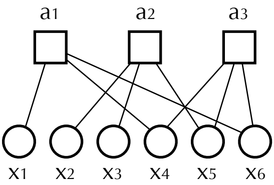


- let $\mathbb{F}$ be a field and let $\mathbf{d}, \mathbf{k}$ satisfy $\mathbb{E}[\mathbf{d}^2], \mathbb{E}[\mathbf{k}^2] < \infty$
- with $d = \mathbb{E}[\mathbf{d}]$, $k = \mathbb{E}[\mathbf{k}]$ and $m \sim Po(dn/k)$ and given

$$\sum_{i=1}^{n} \mathbf{d}_i = \sum_{i=1}^{m} \mathbf{k}_i$$

generate a random bipartite graph G with degrees $\mathbf{d}_i, \mathbf{k}_i$

A Sparse Random Matrix Model



- let $\mathbb{F}$ be a field and let $\mathbf{d}, \mathbf{k}$ satisfy $\mathbb{E}[\mathbf{d}^2], \mathbb{E}[\mathbf{k}^2] < \infty$
- with $d = \mathbb{E}[\mathbf{d}]$, $k = \mathbb{E}[\mathbf{k}]$ and $m \sim Po(dn/k)$ and given

$$\sum_{i=1}^{n} \mathbf{d}_i = \sum_{i=1}^{m} \mathbf{k}_i$$

  generate a random bipartite graph G with degrees $\mathbf{d}_i, \mathbf{k}_i$
- insert entries from a distribution on $\mathbb{F}^*$ to obtain A.

Lots of Work on Different Ground Fields

- full rank: $\mathbb{F}_2$, $\mathbf{d} \sim Po(d)$, $\mathbf{k} = k$ [DM03,DGMMPR10,PS16]
- rank for $\mathbb{F}_2$, $\mathbf{d} \sim Po(d)$, $\mathbf{k} = k$ [CFP18]
- full rank: $\mathbb{F}_3$, $\mathbf{d} \sim Po(d)$, $\mathbf{k} = k$ [FG12]
- rank for $\mathbb{F}_q$, $\mathbf{d} \sim Po(d)$, $\mathbf{k} = k$ [ACOGM17]
- dense matrices [K96,BKW97,CV10,...]

The Rank of Sparse Random Matrices

Theorem (Coja-Oghlan, Ergür, Gao, Hettereich, Rolvien, 19)

Let $D(x)$, $K(x)$ the probability generating functions of $\mathbf{d}, \mathbf{k}$, let

$$\Phi(z) = D\left(1 - K'(z)/k\right) + \frac{d}{k}\left(K(z) + (1-z)K'(z) - 1\right)$$

Then,

$$\lim_{n\to\infty} rank(A)/n = 1 - \max_{\alpha\in[0,1]} \Phi(\alpha)$$

This confirms a conjecture of Lelarge(2013), also explains where cavity method produces wrong predictions.

The Rank of Sparse Random Matrices

Theorem (Coja-Oghlan, Ergür, Gao, Hettereich, Rolvien, 19)

Let $D(x)$, $K(x)$ the probability generating functions of $\mathbf{d}, \mathbf{k}$, let

$$\Phi(z) = D\left(1 - K'(z)/k\right) + \frac{d}{k}\left(K(z) + (1-z)K'(z) - 1\right)$$

Then,

$$\lim_{n\to\infty} rank(A)/n = 1 - \max_{\alpha\in[0,1]} \Phi(\alpha)$$

This confirms a conjecture of Lelarge(2013), also explains where cavity method produces wrong predictions.

The proof is a combination of algebraic insight with statistical physics techniques.

This is the first step of a long term project on using real algebraic tools for approximating partition functions.

Thank you for your attention!