Finding real zeros a lot faster through an adaptive grid

Josué Tonelli-Cueto

Coloquio de Matemática Aplicada

Instituto de Matemática
Universidade Federal do Rio de Janeiro

9/7/2021

Internal Story of the Problem

THE PROBLEM

$\mathcal{H}_d[n] \ni f$

DETERMINISTIC
+
NUMERICALLY
STABLE
+
'GOOD' PROBABILISTIC
RUN-TIME (for random f)

$Z_{\mathbb{P}}(f)$

↑
The ALGORITHM
we want!

Real Homogeneous
Polynomial System
in $X_0, \ldots, X_n$
& with $\deg f_i = d_i$

projective
zeros of f

What do we mean by 'numerically stable'?

1) The algorithm can run in finite precision

More precisely: **forward stability**

If the used precision is 'small enough', then the algorithm's output is correct

This might depend on the input

2) Stability **à la Smale**

The obtained approximations can be refined through an iterative scheme

What do we mean by "'good' probabilistic run-time"?

Fact. Numerical algorithms can have very different run-times on inputs of the same size

↳ Why? Run-times might depend on the condition number

Solution (von Neumann, Goldstine, Demmel, Smale)

average framework:

See what is the run-time for a random input.

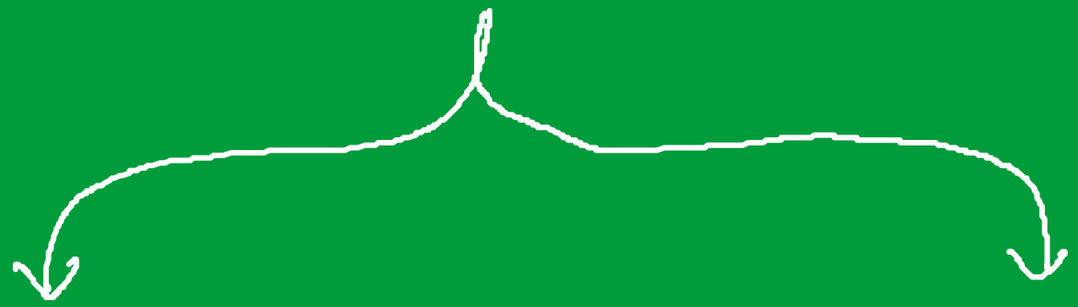
↑ which distribution?

(Spielman, Teng) smoothed framework:

random perturbation of an arbitrary input

What do we mean by "'good' probabilistic run-time"?

Answer: The run-time is reasonably small in the probabilistic sense



Expectation is small

$\mathbb{E}$ run-time $\leq T$

expected complexity

small with high probability

$\mathbb{P}(\text{run-time} \geq T) \leq \varepsilon$

weak complexity

(Ameluxen, Lotz)

Excludes 'black swans'

The Original Trilogy (by Cucker, Krick, Malajovich, Wschebor)

Journal of Complexity 24 (2008) 582–605

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

A numerical algorithm for zero counting, I: Complexity and accuracy

Felipe Cucker [a,*], Teresa Krick [b,c], Gregorio Malajovich [d], Mario Wschebor [e]

[a] Department of Mathematics, City University of Hong Kong, Hong Kong
[b] Departamento de Matemática, Univ. de Buenos Aires, Argentina
[c] CONICET, Argentina
[d] Depto. de Matemática Aplicada, Univ. Federal do Rio de Janeiro, Brazil
[e] Centro de Matemática, Universidad de la República, Uruguay

ARTICLE INFO

Article history:
Received 22 November 2007
Accepted 14 March 2008
Available online 20 April 2008

Keywords:
Counting algorithms
Polynomial systems
Finite precision

ABSTRACT

We describe an algorithm to count the number of distinct real zeros of a polynomial (square) system f. The algorithm performs $\mathcal{O}(\log(n\mathbf{D}\kappa(f)))$ iterations (grid refinements) where n is the number of polynomials (as well as the dimension of the ambient space), $\mathbf{D}$ is a bound on the polynomials' degree, and $\kappa(f)$ is a condition number for the system. Each iteration uses an exponential number of operations. The algorithm uses finite-precision arithmetic and a major feature of our results is a bound for the precision required to ensure that the returned output is correct which is polynomial in n and $\mathbf{D}$ and logarithmic in $\kappa(f)$. The algorithm parallelizes well in the sense that each iteration can be computed in parallel polynomial time in n, $\log \mathbf{D}$ and $\log(\kappa(f))$.

1. Introduction

In recent years considerable attention has been paid to the complexity of counting problems over the reals. The counting complexity class $\#\mathrm{P}_{\mathbb{R}}$ was introduced [20] and completeness results for $\#\mathrm{P}_{\mathbb{R}}$ were established [3] for natural geometric problems notably, for the computation of the Euler characteristic of semialgebraic sets. As one could expect, the "basic" $\#\mathrm{P}_{\mathbb{R}}$-complete problem consists of counting the real zeros of a system of polynomial equations.

* Corresponding author.
E-mail addresses: macucker@cityu.edu.hk (F. Cucker), krick@dm.uba.ar (T. Krick), gregorio@ufrj.br (G. Malajovich), wschebor@cmat.edu.uy (M. Wschebor).

0885-064X/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2008.03.001

J. fixed point theory appl. 6 (2009), 285–294
© 2009 Birkhäuser Verlag Basel/Switzerland
1661-7738/020285-10, *published online* 14.11.2009
DOI 10.1007/s11784-009-0127-4

Journal of Fixed Point Theory and Applications

A numerical algorithm for zero counting. II: Distance to ill-posedness and smoothed analysis

Felipe Cucker, Teresa Krick, Gregorio Malajovich and Mario Wschebor

To Steve, on his 80th birthday, with admiration and esteem

Abstract. We show a Condition Number Theorem for the condition number of zero counting for real polynomial systems. That is, we show that this condition number equals the inverse of the normalized distance to the set of ill-posed systems (i.e., those having multiple real zeros). As a consequence, a smoothed analysis of this condition number follows.

Mathematics Subject Classification (2000). 65Y20, 65H10.

Keywords. Polynomial systems, zero counting, condition numbers, smoothed analysis.

1. Introduction

This paper continues the work in [8], where we described a numerical algorithm to count the number of zeros in n-dimensional real projective space of a system of n real homogeneous polynomials. The algorithm works with finite precision and both its complexity and the precision required to ensure correctness are bounded in terms of n, the maximum $\mathbf{D}$ of the polynomials' degrees, and a condition number $\kappa(f)$.

In this paper we replace $\kappa(f)$—which was originally defined using the computationally friendly infinity norm—by a version $\widetilde{\kappa}(f)$ (defined in Section 2 below) which uses instead Euclidean norms. This difference is of little consequence in complexity estimates since one has (cf. Proposition 3.3 below)

$$\frac{\widetilde{\kappa}(f)}{\sqrt{n}} \leq \kappa(f) \leq \sqrt{2n}\,\widetilde{\kappa}(f). \tag{1}$$

Advances in Applied Mathematics 48 (2012) 215–248

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

A numerical algorithm for zero counting. III: Randomization and condition

Felipe Cucker [a,*,1], Teresa Krick [b,2], Gregorio Malajovich [c,3], Mario Wschebor [d]

[a] Department of Mathematics, City University of Hong Kong, Hong Kong
[b] Departamento de Matemática, Universidad de Buenos Aires & IMAS, CONICET, Argentina
[c] Departamento de Matemática Aplicada, Universidade Federal do Rio de Janeiro, Brazil
[d] Centro de Matemática, Universidad de la República, Uruguay

ARTICLE INFO

Article history:
Received 8 July 2010
Accepted 1 July 2011
Available online 30 August 2011

MSC:
12Y05
60G60
65Y20

Keywords:
Zero counting
Finite precision
Condition numbers
Average-case analysis
Rice formula

ABSTRACT

In a recent paper (Cucker et al., 2008 [8]) we analyzed a numerical algorithm for computing the number of real zeros of a polynomial system. The analysis relied on a condition number $\kappa(f)$ for the input system f. In this paper we look at $\kappa(f)$ as a random variable derived from imposing a probability measure on the space of polynomial systems and give bounds for both the tail $\mathbb{P}(\kappa(f) > a)$ and the expected value $\mathbb{E}(\log \kappa(f))$.

* Corresponding author.
E-mail addresses: macucker@cityu.edu.hk (F. Cucker), krick@dm.uba.ar (T. Krick), gregorio@ufrj.br (G. Malajovich), wschebor@cmat.edu.uy (M. Wschebor).

[1] Partially supported by GRF grant City University 100810.
[2] Partially supported by grants ANPCyT 33671/05, UBACyT X113/2008-2010 and CONICET PIP/2010-2012.
[3] Partially supported by CNPq grants 470031/2007-7, 303565/2007-1, and by FAPERJ.

0196-8858/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.aam.2011.07.001

Part 1 Algorithm & condition-based complexity

↑ Part 2 Condition Number Theorem & probabilistic complexity

↱ Part 3 Probabilistic analysis without integral geometry

The Original Trilogy
(by Cucker, Krick, Malajovich, Wschebor)

Journal of Complexity 24 (2008) 582–605

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

A numerical algorithm for zero counting, I: Complexity and accuracy

Felipe Cucker [a,*], Teresa Krick [b,c], Gregorio Malajovich [d], Mario Wschebor [e]

[a] Department of Mathematics, City University of Hong Kong, Hong Kong
[b] Departamento de Matemática, Univ. de Buenos Aires, Argentina
[c] CONICET, Argentina
[d] Depto. de Matemática Aplicada, Univ. Federal do Rio de Janeiro, Brazil
[e] Centro de Matemática, Universidad de la República, Uruguay

ARTICLE INFO

Article history:
Received 22 November 2007
Accepted 14 March 2008
Available online 20 April 2008

Keywords:
Counting algorithms
Polynomial systems
Finite precision

ABSTRACT

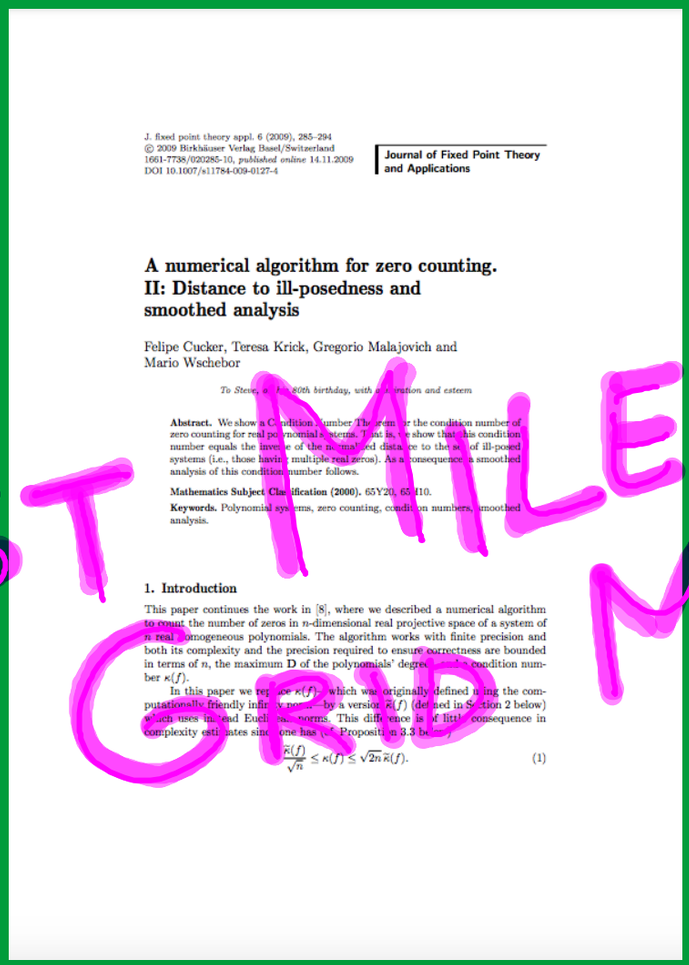
We describe an algorithm to count the number of distinct real zeros of a polynomial (square) system f. The algorithm performs $\mathcal{O}(\log(n\mathbf{D}\kappa(f)))$ iterations (grid refinements) where n is the number of polynomials (as well as the dimension of the ambient space), $\mathbf{D}$ is a bound on the polynomials' degree, and $\kappa(f)$ is a condition number for the system. Each iteration uses an exponential number of operations. The algorithm uses finite-precision arithmetic and a major feature of our results is a bound for the precision required to ensure that the returned output is correct which is polynomial in n and $\mathbf{D}$ and logarithmic in $\kappa(f)$. The algorithm parallelizes well in the sense that each iteration can be computed in parallel polynomial time in n, $\log\mathbf{D}$ and $\log(\kappa(f))$.

1. Introduction

In recent years considerable attention has been paid to the complexity of counting problems over the reals. The counting complexity class $\#\mathrm{P}_{\mathbb{R}}$ was introduced [20] and completeness results for $\#\mathrm{P}_{\mathbb{R}}$ were established [3] for natural geometric problems notably, for the computation of the Euler characteristic of semialgebraic sets. As one could expect, the "basic" $\#\mathrm{P}_{\mathbb{R}}$-complete problem consists of counting the real zeros of a system of polynomial equations.

* Corresponding author.
E-mail addresses: macucker@cityu.edu.hk (F. Cucker), krick@dm.uba.ar (T. Krick), gregorio@ufrj.br (G. Malajovich), wschebor@cmat.edu.uy (M. Wschebor).

0885-064X/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2008.03.001



J. fixed point theory appl. 6 (2009), 285–294
© 2009 Birkhäuser Verlag Basel/Switzerland
1661-7738/020285-10, *published online* 14.11.2009
DOI 10.1007/s11784-009-0127-4

Journal of Fixed Point Theory and Applications

A numerical algorithm for zero counting. II: Distance to ill-posedness and smoothed analysis

Felipe Cucker, Teresa Krick, Gregorio Malajovich and Mario Wschebor

To Steve, on his 60th birthday, with admiration and esteem

Abstract. We show a Condition Number Theorem for the condition number of zero counting for real polynomial systems. That is, we show that this condition number equals the inverse of the normalized distance to the set of ill-posed systems (i.e., those having multiple real zeros). As a consequence, a smoothed analysis of this condition number follows.

Mathematics Subject Classification (2000). 65Y20, 65H10.

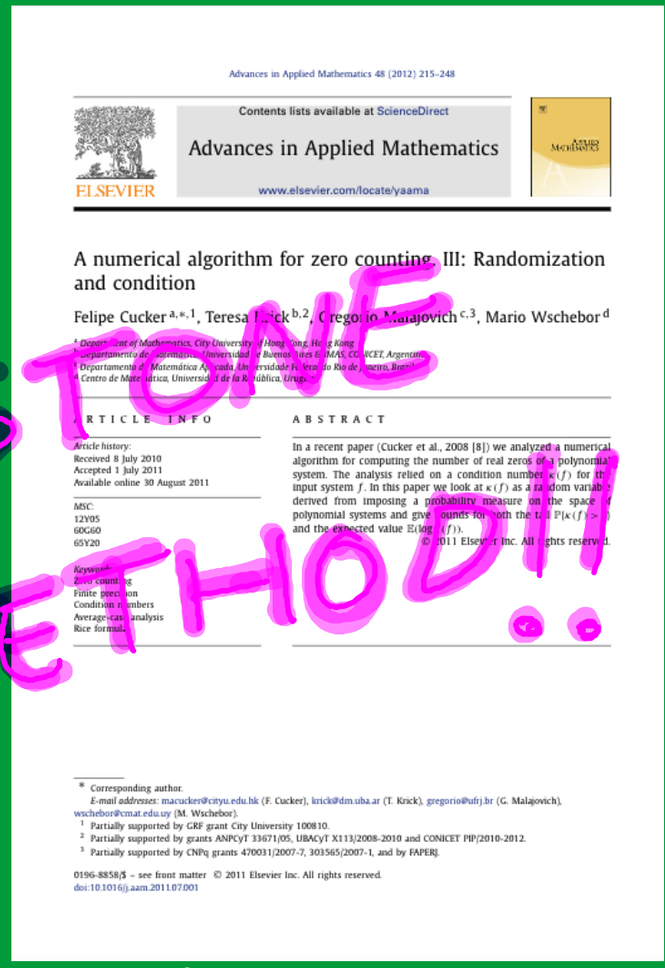
Keywords. Polynomial systems, zero counting, condition numbers, smoothed analysis.

1. Introduction

This paper continues the work in [8], where we described a numerical algorithm to count the number of zeros in n-dimensional real projective space of a system of n real homogeneous polynomials. The algorithm works with finite precision and both its complexity and the precision required to ensure correctness are bounded in terms of n, the maximum $\mathbf{D}$ of the polynomials' degrees, and the condition number $\kappa(f)$.

In this paper we replace $\kappa(f)$, which was originally defined using the computationally friendly infinity norm, by a version $\widetilde{\kappa}(f)$ (defined in Section 2 below) which uses instead Euclidean norms. This difference is of little consequence in complexity estimates since one has (cf. Proposition 3.3 below)

$$\frac{\widetilde{\kappa}(f)}{\sqrt{n}} \le \kappa(f) \le \sqrt{2n}\,\widetilde{\kappa}(f). \tag{1}$$



Advances in Applied Mathematics 48 (2012) 215–248

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

A numerical algorithm for zero counting. III: Randomization and condition

Felipe Cucker [a,*,1], Teresa Krick [b,2], Gregorio Malajovich [c,3], Mario Wschebor [d]

[a] Department of Mathematics, City University of Hong Kong, Hong Kong
[b] Departamento de Matemática, Universidad de Buenos Aires, IMAS, CONICET, Argentina
[c] Departamento de Matemática Aplicada, Universidade Federal do Rio de Janeiro, Brazil
[d] Centro de Matemática, Universidad de la República, Uruguay

ARTICLE INFO

Article history:
Received 8 July 2010
Accepted 1 July 2011
Available online 30 August 2011

MSC:
12Y05
60G60
65Y20

Keywords:
Zero counting
Finite precision
Condition numbers
Average-case analysis
Rice formula

ABSTRACT

In a recent paper (Cucker et al., 2008 [8]) we analyzed a numerical algorithm for computing the number of real zeros of a polynomial system. The analysis relied on a condition number $\kappa(f)$ for the input system f. In this paper we look at $\kappa(f)$ as a random variable derived from imposing a probability measure on the space of polynomial systems and give bounds for both the tail $\mathbb{P}(\kappa(f) > t)$ and the expected value $\mathrm{E}(\log \kappa(f))$.

* Corresponding author.
E-mail addresses: macucker@cityu.edu.hk (F. Cucker), krick@dm.uba.ar (T. Krick), gregorio@ufrj.br (G. Malajovich), wschebor@cmat.edu.uy (M. Wschebor).

[1] Partially supported by GRF grant City University 100810.
[2] Partially supported by grants ANPCyT 33671/05, UBACyT X113/2008-2010 and CONICET PIP/2010-2012.
[3] Partially supported by CNPq grants 470031/2007-7, 303565/2007-1, and by FAPERJ.

0196-8858/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.aam.2011.07.001

FIRST MILESTONE OF THE CUCKER METHOD!!

Part 1 ↑ Algorithm & condition-based complexity

↑ Part 2 Condition Number Theorem & probabilistic complexity

↱ Part 3 Probabilistic analysis without integral geometry

The CKMW algorithm

$\mathcal{H}_d[n] \ni g$ → CKMW → $Z_{\mathbb{P}}(g)$

- DETERMINISTIC
- NUMERICALLY STABLE

'GOOD' PROBABILISTIC RUN-TIME

With 'high probability', run-time(CKMW, g) $\leq D^{O(n^2)}$

for g KSS (average / smoothed)

KSS = Kostlan-Shub-Smale Gaussian

$D := \max d_i$

Probabilistic Model

$g \in \mathcal{H}_d[n]$ KSS random system if

$$g_i = \sum_\alpha \sqrt{\binom{d_i}{\alpha}}\, c_{i,\alpha} X^\alpha$$

with $c_{i,\alpha}$ independent, normal random variables of mean 0 and variance 1.

We also have a smoothed version!

Why this? Invariant under orthogonal changes of variables

$f \circ \|\cdot\|_w g$

The Spin-offs (by Ergür, Paouris, Rojas)

Found Comput Math (2019) 19:131–157
https://doi.org/10.1007/s10208-018-9380-5

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

Probabilistic Condition Number Estimates for Real Polynomial Systems I: A Broader Family of Distributions

Alperen A. Ergür[1] · **Grigoris Paouris**[2] · **J. Maurice Rojas**[2]

Received: 8 December 2016 / Revised: 6 June 2017 / Accepted: 30 October 2017 /
Published online: 31 January 2018

Abstract We consider the sensitivity of real roots of polynomial systems with respect to perturbations of the coefficients. In particular—for a version of the condition number defined by Cucker and used later by Cucker, Krick, Malajovich, and Wschebor—we establish new probabilistic estimates that allow a much broader family of measures than considered earlier. We also generalize further by allowing overdetermined systems. In Part II, we study smoothed complexity and how sparsity (in the sense of restricting which terms can appear) can help further improve earlier condition number estimates.

Keywords Condition number · Epsilon net · Probabilistic bound · Kappa · Real-solving · Overdetermined · Subgaussian

Communicated by Felipe Cucker.

Alperen A. Ergür was partially supported by NSF Grant CCF-1409020, NSF CAREER Grant DMS-1151711 and Einstein Foundation, Berlin. Grigoris Paouris was partially supported by BSF Grant 2010288 and NSF CAREER Grant DMS-1151711. J. Maurice Rojas was partially supported by NSF Grants CCF-1409020 and DMS-1460766.

✉ Alperen A. Ergür
erguer@math.tu-berlin.de

Grigoris Paouris
grigoris@math.tamu.edu

J. Maurice Rojas
rojas@math.tamu.edu

[1] Institut für Mathematik, Technische Universität Berlin, Sekretariat MA 3-2, Strae des 17. Juni 136, 10623 Berlin, Germany

[2] Department of Mathematics, Texas A&M University TAMU 3368, College Station, TX 77843-3368, USA

Springer

1st non-gaussian average complexity in Numerical Alg. Geom!

SMOOTHED ANALYSIS FOR THE CONDITION NUMBER OF STRUCTURED REAL POLYNOMIAL SYSTEMS

ALPEREN A. ERGÜR, GRIGORIS PAOURIS, AND J. MAURICE ROJAS

Abstract. We consider the sensitivity of real zeros of structured polynomial systems to perturbations of their coefficients. In particular, we provide explicit estimates for condition numbers of structured random real polynomial systems, and extend these estimates to smoothed analysis setting.

1. Introduction

Efficiently finding real roots of real polynomial systems is one of the main objectives of computational algebraic geometry. There are numerous algorithms for this task, but the core steps of these algorithms are easy to outline: They are some combination of algebraic manipulation, a discrete/polyhedral computation, and a numerical iterative scheme.

From a computational complexity point of view, the cost of numerical iteration is much less transparent than the cost of algebraic or discrete computation. This paper constitutes a step toward understanding the complexity of numerically solving structured real polynomial systems. Our main results are Theorems 1.14, 1.16, and 1.18 below, but we will first need to give some context for our results.

1.1. **How to control accuracy and complexity of numerics in real algebraic geometry?** In the numerical linear algebra tradition, going back to von Neumann and Turing, condition numbers play a central role in the control of accuracy and speed of algorithms (see, e.g., [3, 6] for further background). Shub and Smale initiated the use of condition numbers for polynomial system solving over the field of complex numbers [36, 37]. Subsequently, condition numbers played a central role in the solution of Smale's 17th problem [2, 5, 25].

The numerics of solving polynomial systems over the real numbers is more subtle than complex case: small perturbations can cause the solution set to change cardinality. One can even go from having no real zero to many real zeros by an arbitrarily small change in the coefficients. This behaviour doesn't appear over the complex numbers as one has theorems (such as the Fundemantel Theorem of Algebra) proving that root counts are "generically" constant. Luckily, a condition number theory that captures these subtleties was developed by Cucker [11]. Now we set up the notation and present Cucker's definition.

Definition 1.1 (Bombieri-Weyl Norm). *We set* $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *where* $\alpha := (\alpha_1, \ldots, \alpha_n)$, *and let* $P = (p_1, \ldots, p_{n-1})$ *be a system of homogenous polynomials with degree pattern* $d_1, \ldots, d_{n-1}$. *Let* $c_{i,\alpha}$ *denote the coefficient of* x^α *in a* p_i. *We define the* Weyl-Bombieri norms *of* p_i *and* P *to be, respectively,*

$$\|p_i\|_W := \sqrt{\sum_{\alpha_1+\cdots+\alpha_n=d_i} \frac{|c_{i,\alpha}|^2}{\binom{d_i}{\alpha}}}$$

A.E. was partially supported by Einstein Foundation, Berlin and by the Pravesh Kothari of CMU. G.P. was partially supported by Simons Foundation Collaboration grant 527498 and NSF grant DMS-1812240. J.M.R. was partially supported by NSF grants CCF-1409020, DMS-1460766, and CCF-1900881.

1st non-gaussian smoothed complexity in NAG! (+ structured systems)

THE SPIN-OFFS
(by Ergür, Paouris, Rojas)

Found Comput Math (2019) 19:131–157
https://doi.org/10.1007/s10208-018-9380-5

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

Probabilistic Condition Number Estimates for Real Polynomial Systems I: A Broader Family of Distributions

Alperen A. Ergür[1] · Grigoris Paouris[2] · J. Maurice Rojas[2]

Received: 8 December 2016 / Revised: 6 June 2017 / Accepted: 30 October 2017 /
Published online: 31 January 2018

Abstract We consider the sensitivity of real roots of polynomial systems with respect to perturbations of the coefficients. In particular—for a version of the condition number defined by Cucker and used later by Cucker, Krick, Malajovich, and Wschebor—we establish new probabilistic estimates that allow a much broader family of measures than considered earlier. We also generalize further by allowing overdetermined systems. In Part II, we study smoothed complexity and how sparsity (in the sense of restricting which terms can appear) can help further improve earlier condition number estimates.

Keywords Condition number · Epsilon net · Probabilistic bound · Kappa · Real-solving · Overdetermined · Subgaussian

Communicated by Felipe Cucker.

Alperen A. Ergür was partially supported by NSF Grant CCF-1409020, NSF CAREER Grant DMS-1151711 and Einstein Foundation, Berlin. Grigoris Paouris was partially supported by BSF Grant 2010288 and NSF CAREER Grant DMS-1151711. J. Maurice Rojas was partially supported by NSF Grants CCF-1409020 and DMS-1460766.

✉ Alperen A. Ergür
erguer@math.tu-berlin.de

Grigoris Paouris
grigoris@math.tamu.edu

J. Maurice Rojas
rojas@math.tamu.edu

[1] Institut für Mathematik, Technische Universität Berlin, Sekretariat MA 3-2, Straße des 17. Juni 136, 10623 Berlin, Germany

[2] Department of Mathematics, Texas A&M University TAMU 3368, College Station, TX 77843-3368, USA

Springer

ROBUST PROBABILISTIC TOOLBOX

SMOOTHED ANALYSIS FOR THE CONDITION NUMBER OF STRUCTURED REAL POLYNOMIAL SYSTEMS

ALPEREN A. ERGÜR, GRIGORIS PAOURIS, AND J. MAURICE ROJAS

Abstract. We consider the sensitivity of real zeros of structured polynomial systems to perturbations of their coefficients. In particular, we provide explicit estimates for condition numbers of structured random real polynomial systems, and extend these estimates to smoothed analysis setting.

1. Introduction

Efficiently finding real roots of real polynomial systems is one of the main objectives of computational algebraic geometry. There are numerous algorithms for this task, but the core steps of these algorithms are easy to outline: They are some combination of algebraic manipulation, a discrete/polyhedral computation, and a numerical iterative scheme.

From a computational complexity point of view, the cost of numerical iteration is much less transparent than the cost of algebraic or discrete computation. This paper constitutes a step toward understanding the complexity of numerically solving structured real polynomial systems. Our main results are Theorems 1.14, 1.16, and 1.18 below, but we will first need to give some context for our results.

1.1. How to control accuracy and complexity of numerics in real algebraic geometry? In the numerical linear algebra tradition, going back to von Neumann and Turing, condition numbers play a central role in the control of accuracy and speed of algorithms (see, e.g., [3, 6] for further background). Shub and Smale initiated the use of condition numbers for polynomial system solving over the field of complex numbers [36, 37]. Subsequently, condition numbers played a central role in the solution of Smale's 17th problem [2, 5, 25].

The numerics of solving polynomial systems over the real numbers is more subtle than complex case: small perturbations can cause the solution set to change cardinality. One can even go from having no real zero to many real zeros by an arbitrarily small change in the coefficients. This behaviour doesn't appear over the complex numbers as one has theorems (such as the Fundamental Theorem of Algebra) proving that root counts are "generically" constant. Luckily, a condition number theory that captures these subtleties was developed by Cucker [11]. Now we set up the notation and present Cucker's definition.

Definition 1.1 (Bombieri-Weyl Norm). *We set $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ where $\alpha := (\alpha_1, \ldots, \alpha_n)$, and let $P = (p_1, \ldots, p_{n-1})$ be a system of homogenous polynomials with degree pattern $d_1, \ldots, d_{n-1}$. Let $c_{i,\alpha}$ denote the coefficient of x^α in a p_i. We define the* Weyl-Bombieri norms *of p_i and P to be, respectively,*

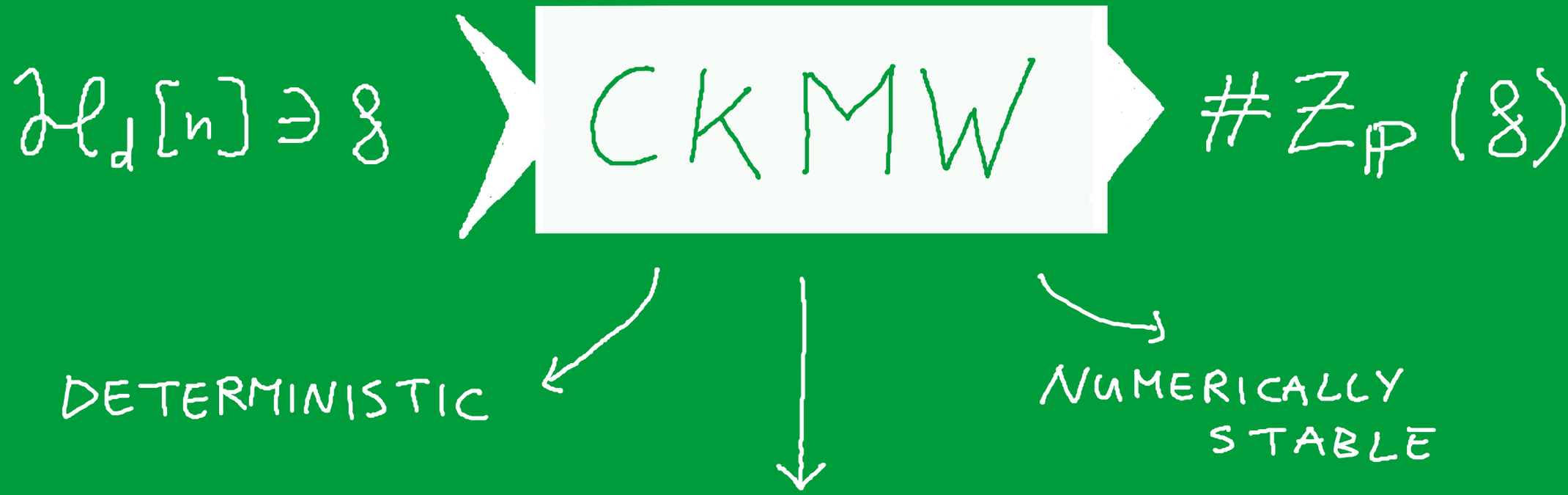
$$\|p_i\|_W := \sqrt{\sum_{\alpha_1+\cdots+\alpha_n=d_i} \frac{|c_{i,\alpha}|^2}{\binom{d_i}{\alpha}}}$$

A.E. was partially supported by Einstein Foundation, Berlin and by the Pravesh Kothari of CMU. G.P. was partially supported by Simons Foundation Collaboration grant 527498 and NSF grant DMS-1812240. J.M.R. was partially supported by NSF grants CCF-1409020, DMS-1460766, and CCF-1900881.

1st non-gaussian average complexity in Numerical Alg. Geom!

1st non-gaussian smoothed complexity in NAG! (+ structured systems)

The CKMW algorithm (after the spin-offs)



With 'high probability', run-time(CKMW, $\mathcal{S}$) $\leq D^{O(n^2)}$

for a wide class of random systems

$D := \max d_i$

Probabilistic Model II

$g \in \mathcal{H}_d[n]$ dobro random system

$$g_i = \sum_\alpha \sqrt{\binom{d_i}{\alpha}}\, c_{i,\alpha} X^\alpha$$

with $c_{i,\alpha}$ independent,

Also with smoothed version!

centered
i.e. $\mathbb{E}\, c_{i,\alpha} = 0$

subgaussian with cte. $\leq K_i$;
i.e. $\mathbb{E}\,|c_{i,\alpha}|^q \leq K_i^q\, q^{q/2}$ for $q \geq 1$

anticoncentration cte. $\leq \rho_i$;
i.e. $\mathbb{P}(|c_{i,\alpha} - t| \leq \varepsilon) \leq 2\rho_i \varepsilon$ for $t \in \mathbb{R}$

Important properties of gaussians!

For random $g \in \mathcal{L}_d[n]$ as before,

$\mathbb{E}_g$ run-time$(CKMW, g) < \infty$?

NO!

Why? run-time$(CKMW, g) \leq O^{O(n)}\, \kappa(g)^n$

& $\mathbb{E}_g\, \kappa(g)^n = \infty$

$\|g\|_W = \sqrt{\sum_{i,\alpha} \binom{d_i}{\alpha}^{-1} g_{i,\alpha}^2}$ (Weyl norm)

$\kappa(g) = \max_{x \in S^n} \kappa(g,x)$ $\quad \kappa(g,x) = \|g\|_W / \sqrt{\|g(x)\|^2 + \|D_x g^{-1} \Delta^{1/2}\|^{-2}}$ $\quad \Delta = \mathrm{diag}(d_i)$

Idea!

Make CKMW adaptive,

then complexity should depend on

$$\mathbb{E}_{x \in S^n} \mathcal{K}(f,x)^n$$

which has <u>finite expectation</u>

for a random f!

$\|f\|_w = \sqrt{\sum_{i,\alpha} \binom{d_i}{\alpha}^{-1} f_{i,\alpha}^2}$ (Weyl norm) $\mathcal{K}(f,x) = \|f\|_w / \sqrt{\|f(x)\|^2 + \|D_x f \Delta^{-1}\|^{-2}}$ $\Delta = \mathrm{diag}(d_i)$

Inspiration: (Cucker, Ergür, T.-C.; 2019) while studying PV algorithm

Naive adaptive version fails!

(Eckhardt, 2020) (Han, 2018)

Run-time bound in terms of

$$\mathop{\mathbb{E}}_{x \in S^n} \mathcal{K}(g,x)^{2n}$$

which has <u>infinite expectation</u>

for a random g!

$\|g\|_W = \sqrt{\sum_{i,\alpha} \left(\frac{d_i}{\alpha}\right)^{-1} g_{i,\alpha}^2}$ (Weyl norm) $\mathcal{K}(g,x) = \|g\|_W / \sqrt{\|g(x)\|^2 + \|D_x g^{-T} \Delta^g\|^{-2}}$ $\Delta = \mathrm{diag}(d_i)$

What goes wrong?

The criterion to select zeros!

The CKMW algorithm

1) Refine grid $G \subseteq \mathbb{S}^n$ until $d_{\mathbb{S}}(G, \mathbb{S}^n)$ 'small'

2 {
- Exclude points $x \in G$ s.t. $\|g(x)\|/\|g\|_w$ 'big'
- Include points $x \in G$ s.t. $\|g(x)\|/\|g\|_w$ 'small'
}

3 Post-process the selected points to get approximation of $Z_{ip}(g)$

How do we exclude points?

Exclusion Lemma. Let $g \in \mathcal{H}_d[n]$, the map

$$S^n \ni x \mapsto g(x)/\|g\|_w$$

is $\sqrt{D}$-Lipschitz. In particular, if

$$r \geq \frac{\|g(x)\|}{\sqrt{D}\,\|g\|_w},$$

the $B_S(x,r) \cap \mathcal{Z}_S(g) = \emptyset$.

$\|g\|_w = \sqrt{\sum_{i,\alpha} \binom{d_i}{\alpha}^{-1} g_{i,\alpha}^2}$ (Weyl norm) $\qquad D := \max d_i$

How do we include points?

Spherical Newton operator: $N_g(x) := \dfrac{x - D_x g^{-1} g(x)}{\|x - D_x g^{-1} g(x)\|}$

$$N_g^{n+1}(x) = N_g(N_g^n(x))$$

Smale's α-criterion:

$$\alpha(g,x) := \beta(g,x)\gamma(g,x) \leq \alpha_*$$

$$\hookrightarrow \#B_S(x, 1.5\beta(g,x)) \cap Z_S(g) = 1$$

$$\& \quad N_g^n(x) \xrightarrow[\text{quadratically}]{} \text{zero of } g$$

where $\beta(g,x) := \|D_x g^{-1} g(x)\|$ & $\gamma(g,x) := \sup_{k\geq 2} \|D_x g^{-1} \frac{1}{k!} D_x^k g\|$

Assume $\sqrt{2}\,\kappa(g,x)\,\|g(x)\|/\|g\|_w < 1 \ldots$

- Higher Derivative Estimate: $\gamma(g,x) \leq \frac{1}{2} D^{3/2} \kappa(g,x)$
- An estimate for β: $\beta(g,x) \leq \kappa(g,x)\,\|g(x)\|/\|g\|_w$

The CKMW algorithm

1) Refine grid $G \subseteq \mathbb{S}^n$ until $\underbrace{d_{\mathbb{S}}(G, \mathbb{S}^n)}_{=:\delta} \leq \frac{1}{cD^2\kappa(g)^2}$

2 {
- Exclude points $x \in G$ s.t. $\|g(x)\|/\|g\|_w \geq \sqrt{D}\,\delta$
- Include points $x \in G$ s.t. $\|g(x)\|/\|g\|_w \leq \frac{1}{\tilde{c}D^2\kappa(g)^2}$

3 Post-process the selected points to get approximation of $Z_{ip}(g)$

Note quadratic condition in the inclusion criterion!

$\kappa(g) := \max_{x \in \mathbb{S}^n} \|g\|_w \,/\, \sqrt{\|g(x)\|^2 + \|D_x g^{-1} \Delta^{1/2}\|^{-2}}$ condition number

The adaptive CKMW algorithm

NAIVE EDITION

1) Refine adaptively $G \subseteq \mathbb{S}^n \times (0,\infty)$ so that
   1) $\mathbb{S}^n \subseteq \bigcup \{B_g(x,r) \mid (x,r) \in G\}$
   & 2) $\forall (x,r) \in G,\ r \leq 1/cD\kappa(g,x)^2$
2) $\begin{cases} \text{Exclude } (x,r) \in G & \text{if } \|g(x)\|/\|g\|_w \geq \sqrt{D}\, r \\ \text{Include } (x,r) \in G & \text{if } \|g(x)\|/\|g\|_w \leq 1/\hat{c}D^2\kappa(g,x)^2 \end{cases}$
3) Post-process the selected points to get approximation of $Z_{lp}(g)$

Still quadratic inclusion criterion!

$\kappa(g,x) := \|g\|_w / \sqrt{\|g(x)\|^2 + \|D_x g^{-1}\Delta^{1/2}\|^{-2}}$ local condition number

Where does the square come from?

$$\beta(\xi, x) \leq \mathcal{K}(\xi, x) \frac{\|\xi(x)\|}{\|\xi\|_W}$$

is a very bad estimate!

The $\mathcal{K}(\xi, x)$ in the upper bound causes the square

We should use β directly!

Converse Smale's α-theorem:

$$\gamma(f,x)\,\mathrm{dist}_S(x, Z_S(f)) < 1$$

$$\Leftrightarrow \quad \alpha(f,x) \le \frac{\gamma(f,x)\,\mathrm{dist}_S(x, Z_S(f))}{1-\gamma(f,x)\,\mathrm{dist}_S(x, Z_S(f))}$$

'If x is sufficiently near $Z_S(f)$,
then Smale's α-criterion at x holds'

Corollary. If $\sqrt{2}\,K(f,x)\,\|f(x)\|/\|f\|_W < 1$,

then $\alpha(f,x) < \alpha_*$

or $B_S\left(x, c/D^2K(f,x)\right) \cap Z_S(f) = \emptyset$

The adaptive CKMW algorithm

NON NAIVE EDITION!!!

1) Refine adaptively $G \subseteq S^n \times (0,\infty)$ so that
   1) $S^n \subseteq \bigcup \{B_S(x,r) \mid (x,r) \in G\}$
   & 2) $\forall (x,r) \in G,\ r \leq 1/c D K(g,x)$
2) Exclude $(x,r) \in G$ if $\|g(x)\|/\|g\|_w \geq \sqrt{D}\, r$
   Include $(x,r) \in G$ if $\beta(g,x) \leq 1/c D^2 K(g,x)$
3) Post-process the selected points to get approximation of $Z_{IP}(g)$

Using β gives the desired $\mathbb{E}_{x \in S^n} K(g,x)^n$ bound!

$K(g,x) := \|g\|_w / \sqrt{\|g(x)\|^2 + \|D_x g^{-1} \Delta^{1/2}\|^{-2}}$ local condition number

Some extra tricks

$$\chi_2(g,x) := \frac{\|g\|_w}{\sqrt{\|g(x)\|^2 + \|D_x g^{-1}\Delta^{1/2}\|^{-2}}}$$

Change of norm

$$\hookrightarrow C(g,x) := \frac{\|g\|_\infty}{\max\{\|\Delta^{-1}g(x)\|_\infty, \|D_x g^{-1}\Delta^2\|_{\infty,2}^{-1}\}}$$

where $\Delta := \mathrm{diag}(d_i)$

Extra normalization

Row-normalization

$$\hat{g} := (g_i/\|g_i\|_\infty)_i$$

Interlude: $\|\cdot\|_w$ vs. $\|\cdot\|_\infty$

Definition

$g \in \mathcal{H}_d[n]$

$$\|g\|_w := \sqrt{\sum_{i,\alpha} \binom{d_i}{\alpha}^{-1} g_{i,\alpha}^2} \qquad \|g\|_\infty := \max_{i, x \in S^n} |g_i(x)|$$

Similar inequalities $\Rightarrow$ Similar condition-based theory

$$\|D_x g(v)\|_w \le D \|g\|_w \qquad \|D_x g(v)\|_\infty \le D \|g\|_\infty$$

where $D_x g(v) = \sum_j \frac{\partial g}{\partial x_j} v_j \in \mathcal{H}_{d-1}[n]$ ← Kellogg's inequality

Different probabilistic behaviours

$$\mathbb{E}_g \|g\|_w \sim \sqrt{N} \sim \min\{n^{D/2}, D^{n/2}\} \qquad \mathbb{E}_g \|g\|_\infty \sim \sqrt{n \log D}$$

There is a catch! $\|g\|_\infty$ harder to compute

Main Result

MAIN THEOREM

There is a DETERMINISTIC, NUMERICALLY STABLE algorithm a CKMW that given $f \in \mathbb{Z}_q[u]$ computes $\#Z_p(f)$ and such that

$$\mathbb{E}_f \text{ run-time}(\text{a CKMW}, f) \leq 2^{\mathcal{O}(u \log u)} D^u N + 2^{\mathcal{O}(u \log u)} \mathcal{D}^{2.5} (N + \mathcal{D})$$

(for f dobro random (with bounded parameters)

'GOOD' PROBABILISTIC RUN-TIME

where $D := \max d_i$ $\mathcal{D} := \prod d_i$

$N := \sum \binom{u+d_i}{u} = \#$ of zero & nu-zero coeff. of f

+ PARALLELIZABLE

Future Work

We can produce correct adaptive samples!

Homology computation of semialgebraic sets

Post-processing step has to be improved!

Can we have a Monte-Carlo version without computing $\|\delta\|_\infty$?

Obrigado
pela atenção!