Optimization and approximation problems related to polynomial system solving

Klaus Meer
University of Southern Denmark
Odense, Denmark

CiE 2006 Swansea, July 2006

Introduction

Many problems in mathematics, computer science, engineering closely related to

polynomial systems

Typical questions are concerned with

- solvability
- good estimates for number of solutions
- computing solutions, f.e. numerically

Important from computer science point of view

complexity of dealing with above tasks

Some issues related to polynomial systems treated here

- example from mechanism design
- (non-) existence of approximation algorithms in combinatorial optimization
- probabilistically checkable proofs PCPs

Framework:

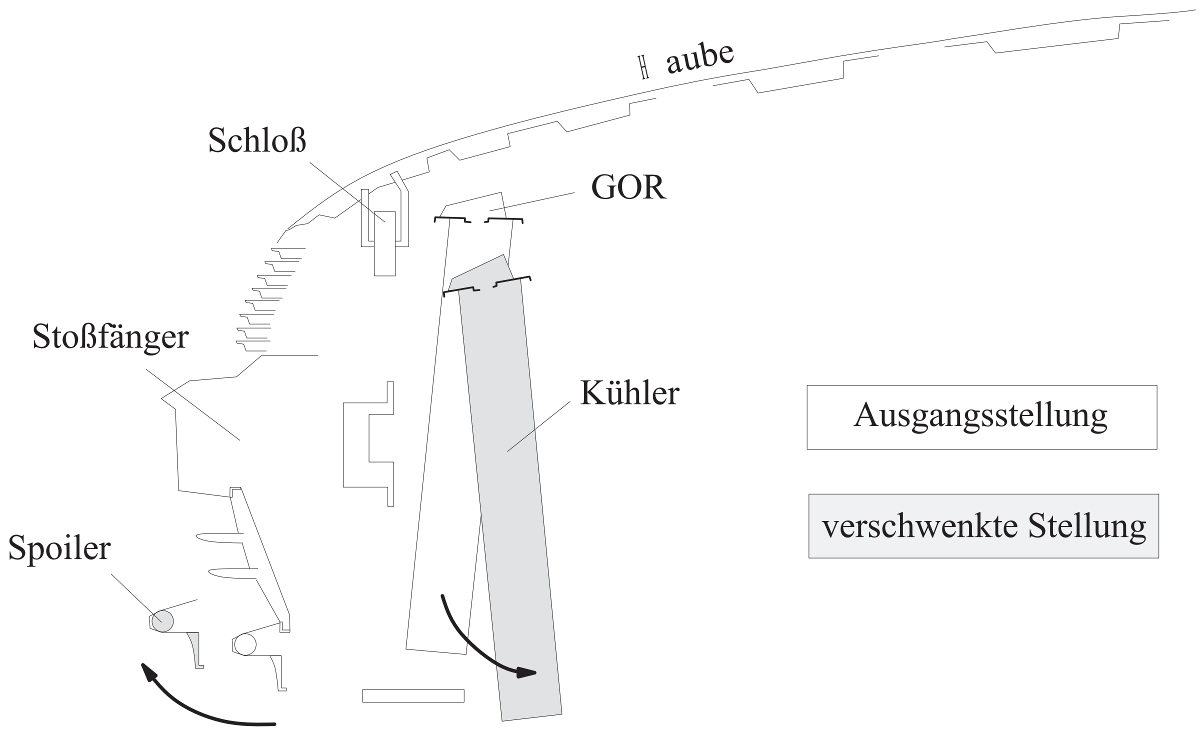
Both classical (Turing) and real number (Blum-Shub-Smale) complexity theory

1. Motivating example: Motion synthesis in robotics

Many practical problems within computational geometry result in question, whether a polynomial system is solvable

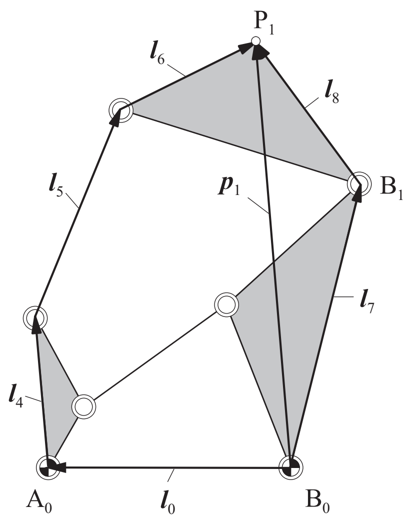
Here: Design of certain mechanisms in mechanical engineering

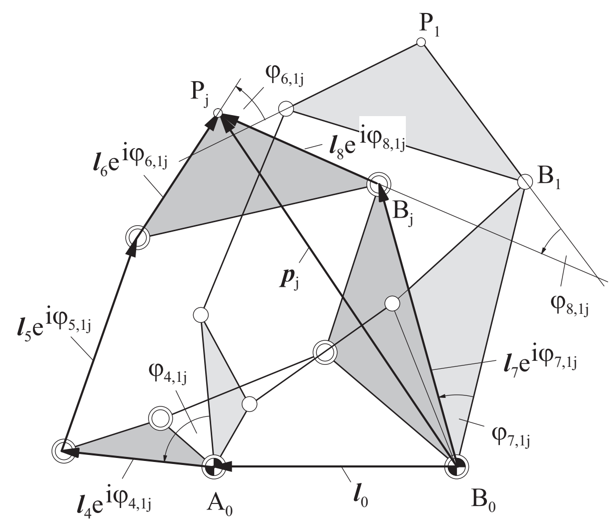
Example: Protection of pedestrians in traffic



Required motion of cooler and spoiler

Problem in kinematics: Design gearing mechanism satisfying certain demands





Stephenson gear

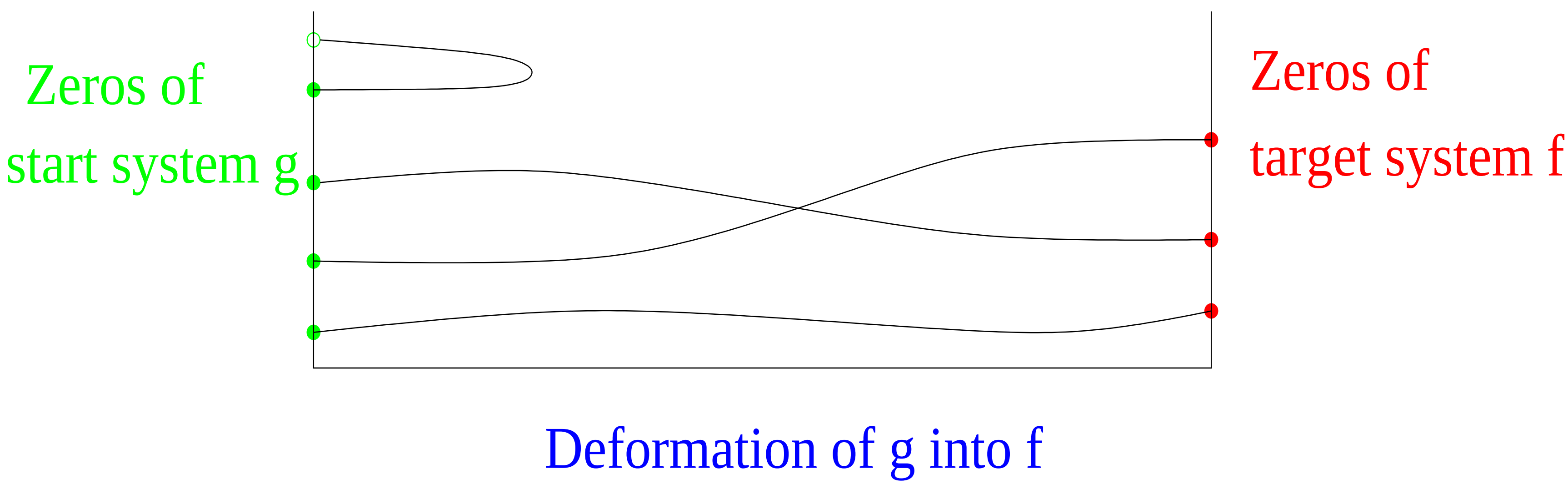
Example of a required motion:

Move point P through certain positions

Typically leads to problem of solving a polynomial system with real or complex coefficients

Difficulty: Already few variables and low degrees can result in a system out of range of current solution methods!

Homotopy methods: Deform an easy to handle start system into the target system; follow numerically zeros of start system into those of target system



Complete motion synthesis for so called Stephenson mechanisms can be performed efficiently by homotopy methods

M.& Schmitt & Schreiber, 2002

Efficiency of homotopy methods relies on existence and number of zeros (paths)

$\rightsquigarrow$ analysis needs more theory

2. Approximation algorithms

Several (deep) mathematical methods for bounding number of zeros for polynomial systems $f : \mathbb{C}^n \mapsto \mathbb{C}^n$:

Bézout number	generalizes fundamental theorem of algebra, easy to compute, too a large bound
Mixed Volumes	Minkowski sum of Newton polytopes, hard to compute, (generically) correct bound
multi-homogeneous Bézout numbers	partitioning of variables, then Bézout for each group; mainly used in practice; so far no complexity results

Example: Eigenpairs

Find eigenpairs $(\lambda, v) \in \mathbb{C}^{n+1}$ of $M \in \mathbb{C}^{n\times n}$:

$$M \cdot v - \lambda \cdot v = 0 \ , \ v_n - 1 = 0$$

Has (generically) n solutions, but Bézout number 2^n.

Multi-homogeneous Bézout numbers: Group variables as

$$M \cdot v - \lambda \cdot v = 0 \ , \ v_n - 1 = 0$$

and homogenize w.r.t. both groups

$$\lambda_0 \cdot M \cdot v - v \cdot \lambda = 0 \ , \ v_n - v_0 = 0$$

Then the number of isolated roots in $(\mathbb{C})^n$ is bounded by the 2-homogeneous Bézout number, which here is n.

Theorem (Malajovich & M., 2005):

a) Given a polynomial system $f : \mathbb{C}^n \to \mathbb{C}^n$ there is no efficient algorithm that computes the minimal multi-homogeneous Bézout number (unless P = NP).

b) The same holds with respect to efficiently approximating the minimal such number within an arbitrary constant factor.

Sketch of proof:

Relate problem to 3-coloring problem for graphs

Establish multiplicative structure of multi-hom. Bézout numbers

In practice: Balance whether additional effort for constructing start system pays out

Remark. MHBN important in analysis of central path in interior point methods (Shub et al.)

3. Complexity theory over $\mathbb{R}$

Above systems particular in that solutions generically exist

Related interesting questions:

- deciding existence of solutions for general polnomials
- exact counting of number of solutions in general

Theorem (Blum & Shub & Smale '89):

Deciding solvability of real polynomial systems is $\mathrm{NP}_{\mathbb{R}}$-complete over $\mathbb{R}$; similarly for complex systems and $\mathrm{NP}_{\mathbb{C}}$.

Remark. All problems in $\mathrm{NP}_{\mathbb{R}}$ can be decided in simple exponential time in the real number model. Similarly over $\mathbb{C}$.

Corollary (Bürgisser & Cucker '05):

Counting the number of solutions is $\#\mathrm{P}_{\mathbb{R}}$-complete and $\#\mathrm{P}_{\mathbb{C}}$-complete, respectively.

Many other recent completeness results for counting problems in algebraic geometry by Bürgisser & Cucker & Lotz

Clear: also the following optimization problem is hard

MAX-Quadratic Polynomial Systems MAX-QPS:

Input: $n, m \in \mathbb{N}$, real polynomials in n variables $p_1, \ldots, p_m \in \mathbb{R}[x_1, \ldots, x_n]$ of degree at most 2; find maximal number of p_i's that have a common real root

But what's about approximating this maximum?

Theorem (M., 2005): If total number of non-vanishing coefficients in system is $O(m^2)$ there is no $\mathrm{APX}_{\mathbb{R}}$ algorithm for MAX-QPS unless $\mathrm{P}_{\mathbb{R}} = \mathrm{NP}_{\mathbb{R}}$.

Close relation also over the reals to PCPs

Example. $\mathrm{NP}_{\mathbb{R}}$ verification for solvability of system

$$p_1(x) = 0 \ , \ \ldots, p_m(x) = 0$$

guesses solution $x^* \in \mathbb{R}^n$ and plugs it into all p_i's ; obviously all components of x^* have to be seen

Question. Can we rewrite $\mathrm{NP}_{\mathbb{R}}$-verification proofs in such a way that seeing only constantly many positions of the proof suffices to detect faults with high probability?

Formalization using verifiers gives family of complexity classes

$$\mathrm{PCP}_{\mathbb{R}}(r, q)$$

Theorem (M., 2005)

$\mathrm{NP}_{\mathbb{R}}$ has long, transparent proofs:

$$\mathrm{NP}_{\mathbb{R}} \subseteq \mathrm{PCP}_{\mathbb{R}}(poly, const)$$

Example: Each faulty proof claiming that a polynomial system is solvable can be rewritten such that a fault occurs with high probability in each part of the proof having constant length

Proof: New techniques for self-testing and self-correction of functions on real domains

Main challenge: Are there as well short transparent proofs, i.e. is

$$\mathrm{NP}_{\mathbb{R}} \subseteq \mathrm{PCP}_{\mathbb{R}}(log, const) \ ?$$

Close relation to approximation algorithms for real number optimization problems; a positive answer would yield

Theorem (M., 2006)

If $\mathrm{NP}_{\mathbb{R}}$ has short transparent proofs there is no $\mathrm{FPTAS}_{\mathbb{R}}$ approximation scheme for instances of MAX-QPS with $O(n)$ many non-zero coefficients.

Another open question: Are there any fixed-constant approximation algorithms at all for MAX-QPS? (Flarup & M. '06)

Summary

Analysis of polynomial systems results in interesting problems in many different areas including

- robotics
- combinatorial optimization
- classical and real number complexity theory

References

- Meer, K., Schmitt, B., Schreiber, H.: Dimensional Synthesis of Planar Stephenson-Mechanisms for Motion Generation by Circlepoint Search and Homotopy Methods. Mechanism and Machine Theory, Vol. 37, Nr. 7, 2002, 717-737.
- Malajovich, G., Meer, K.: Computing Multi-Homogeneous Bézout Numbers is Hard. To appear in: Theory of Computing Systems.

  Extended Abstract in: Proc. STACS 2005, LNCS 3404, 244–255.
- Meer, K.: Transparent long proofs: A first PCP theorem for $\mathrm{NP}_{\mathbb{R}}$.

  Foundations of Computational Mathematics, Springer, Vol. 5, Nr. 3, 2005, 231–255.

  Extended Abstract in: Proc. 31st ICALP 2004, LNCS 3142, 959–970.
- Meer, K.: On some relations between approximation and PCPs over the real numbers. To appear in: Theory of Computing Systems.

  Extended Abstract in: Proc. CiE 2005, LNCS 3526, 322–331.
- Flarup, U., Meer, K.: Two logical hierarchies of optimization problems over the real numbers.

  Mathematical Logic Quaterly, Vol. 52, Nr. 1, 2006, 37–50.

2. Definition of multi-hom. Bézout number

Consider $n \in \mathbb{N}$, a finite $A \subset \mathbb{N}^n$ and a polynomial system

$$\begin{cases} f_1(z) = \sum_{\boldsymbol{\alpha} \in A} f_{1\boldsymbol{\alpha}} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \\ \vdots \\ f_n(z) = \sum_{\boldsymbol{\alpha} \in A} f_{n\boldsymbol{\alpha}} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \end{cases}$$

where the $f_{i\alpha}$ are non-zero complex coefficients.

Thus, all f_i have the same support A

A multi-homogeneous structure: partition of $\{1, \ldots, n\}$ into k subsets

$$(I_1, \ldots, I_k) \ , \ I_j \subseteq \{1, \ldots, n\}$$

Define for each partition $(I_1, \ldots, I_k)$:

- block of variables related to I_j : $Z_j = \{z_i | i \in I_j\}$
- corresponding degree of f_i with respect to $\mathbb{Z}_j$: $d_j := \sum_{l \in I_j} \; \alpha_l$ (the same for all polynomials f_i because of same support)

Definition: a) The multi-hom. Bézout number w.r.t. partition $(I_1, \ldots, I_k)$ is the coefficient of $\prod_{j=1}^{k} \zeta_j^{|I_k|}$ in the formal polynomial $(\zeta_1 + \cdots + \zeta_k)^n$ (if each group not yet homogeneous)

$$\text{Béz}(A, I_1, \ldots, I_k) = \begin{pmatrix} & & n & \\ |I_1| & |I_2| & \cdots & |I_k| \end{pmatrix} \prod_{j=1}^{k} d_j^{|I_j|}$$

b) Minimal multi-hom. Bézout number:

$$\min_{\mathbf{I} \text{ partition}} \text{Béz}(A, \mathbf{I})$$