Complexity of Integer Quasiconvex Polynomial Optimization

Bernd Bank
Sebastian Heinz
Institut für Mathematik
Humboldt–Universität zu Berlin

TERA 05, October 24 – 28, 2005
In Honor of Joos Heintz's 60 – th Birthday
UBA, Buenos Aires, Argentina

Overview

Objects of interest

- Algebra: integers, polynomials,...
- Geometry: ellipsoids, lattices, ...
- Convex analysis: characteristic cones, supporting hyperplanes,...

Representation

- Computation: Turing machines, dense encoding,...
- Logics: language of ordered rings,...

The theory of integers is not decidable.

The theory of reals allows quantifier elimination.

Gödel (1931), Church (1936), Tarski (1951), Seidenberg (1954)

The story of the optimization problem considered

- **Jeroslow 1973**

  There is no algorithm that solves the integer quadratic optimization problem

  $$(IQP) \qquad \min\{\, c^T x \mid x \in \mathbb{Z}^n \wedge \bigwedge_{i=1}^{s} F_i(x) \geq 0 \,\},$$

  where $c \in \mathbb{Z}^n$ and $F_1, \ldots, F_s \in \mathbb{Z}[X]$ of degree 2 at most.
  By Matiyasevic's 1970 result wrt. Hilbert's 10–th problem.

- **Belousov 1977**

  Properties of convex polynomials.

- **Khachiyan/Tarasov 1980**

  Bounds and algorithmic complexity of convex diophantine inequalities.

- **Khachiyan/Tarasov 1980, Khachiyan 1982**

  There is an algorithm that solves

$$(IPP) \qquad \min\{\, F_0(x) \mid x \in \mathbb{Z}^n \wedge \bigwedge_{i=1}^{s} F_i(x) \geq 0 \,\},$$

  if all polynomials F_i as functions on $\mathbb{R}^n$ are convex ones.

  The complexity bound:

$$\log R = d^{c(\min\{n,s\}+d)} n^{cd} \, \ell,$$

  was given, where

  R radius of a sphere containing a solution if there is one,

  d a degree bound,

  ℓ maximum binary length of the coefficients,

  c a universal constant.

  However, a proof was never seen!

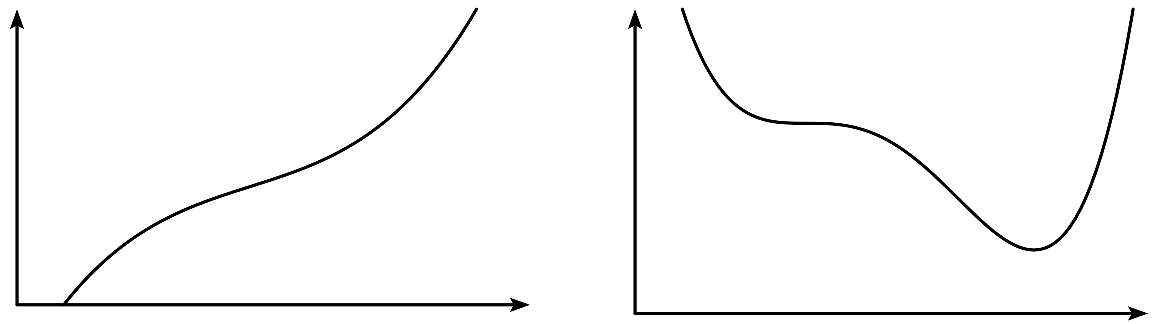
- **Mandel 1986, B/Mandel 1988**

  There is an algorithm that solves

$$(IPP) \qquad \min \{ F_0(x) \mid x \in \mathbb{Z}^n \wedge \bigwedge_{i=1}^{s} F_i(x) \geq 0 \},$$

  if all polynomials F_i as functions on $\mathbb{R}^n$ are quasi–convex ones.

  Examples of quasiconvex (but non-convex) polynomials



  All lower level–sets are convex sets.

- We stucked with the proof of a complexity bound.

- **Joos Heintz/Pablo Solernó 1988**
  Visit in Berlin, ...

- **Pablo Solernó 1989**
  Complejidad de conjuntos semialgebraicos. Tesis UBA

- **Teresa, Joos, Pablo, B 1989 IAM, Bs. As.**
  ...

- **Teresa Krick 1990**
  Complejidad para problemas de geometria elemental, Tesis UBA

- **Joos, Teresa 1990**
  Visit in Berlin, ..., **FOCS, Math. Nach., Crelle**

- **B/Heintz/Krick/Mandel/Solernó 1990, 1991**
  If all polynomials in (IPP) are quasi-convex and if there is a solution then there is a solution in a sphere of radius R satisfying

$$\log R = (sd)^{O(n)}\,\ell.$$

- **Joos** .... **Basu/Pollack/Roy 1996**

- **B/Sporn 1997** $\qquad \log R = d^{O(n)}\,\ell.$

- **Khachiyan/Porkolab 2000**
  showed the existence of an algorithm that solves the problem

$$\min(x_n \mid x \in \mathbb{Z}^n \wedge x \in Y),$$

  where $Y \subseteq \mathbb{R}^n$ is a convex semialgebraic set given by a first order formula over the reals. The algorithm is of time-complexity

$$\ell^{O(1)} \cdot s^{O(n^2)} \cdot d^{O(n^4)}.$$

- **H.W. Lenstra 1983**
  Consider the integer linear optimization problem

$$(LIP) \qquad \min \{ c^T x \mid x \in \mathbb{Z}^n \wedge Ax \geq b \},$$

  where $b, c \in \mathbb{Z}^s$ and $A \in \mathbb{Z}^{s \times n}$ are given such that ℓ is the maximum binary length of all entries. (LIP) can be solved within time–complexity $O(s)\ \ell^{O(1)}\ 2^{O(n^3)}$.

Joos Heintz, 2003

Sebastian Heinz, 2004

The optimization problem

Problem (1)

$$\min_{x\in\mathbb{Z}^n}\left\{\hat{F}(x) \mid \bigwedge_{i=1}^{s} F_i(x) < 0\right\}$$

- $\hat{F}, F_1, \ldots, F_s \in \mathbb{Z}[X]$ **quasi–convex** polynomials
- Problem (1) can be formulated by weak inequalities in the form (IPP) as well, since

$$z < 0 \quad \& \quad z+1 \leq 0 \quad \text{are equivalent if } z \in \mathbb{Z}.$$

Two geometric properties of a quasi–convex polynomial

- $F \in \mathbb{R}[X]$ quasi–convex, $\hat{x} \in \mathbb{R}^n$, $a \in \mathbb{R}^n$, $a \neq 0$

$\Longrightarrow$ If $F(\hat{x} + \lambda \cdot a)$ in $\lambda \in \mathbb{R}$ is strongly decreasing (or constant, resp.), then $F(x + \lambda \cdot a)$ shows the same property for all $x \in \mathbb{R}^n$.

Constancy of $F \in \mathbb{R}[X]$ can easily be checked.

- $F \in \mathbb{R}[X]$ quasi–convex, $\hat{x} \in \mathbb{R}^n$.

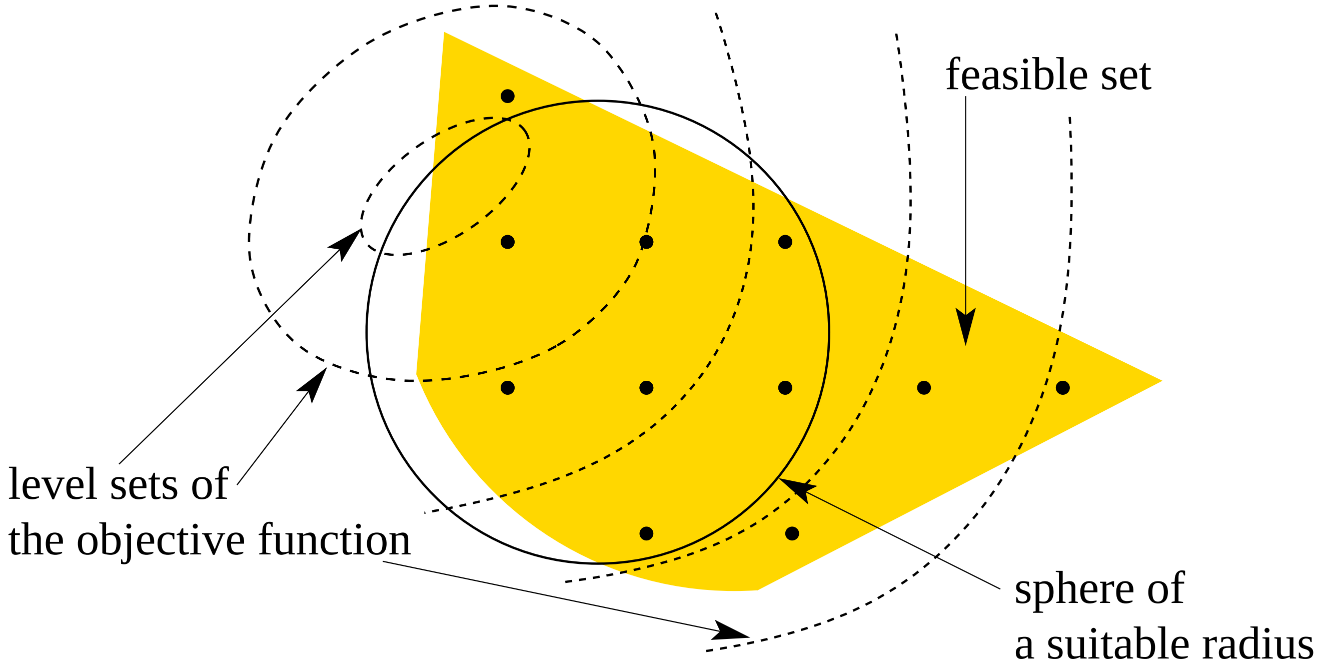
$\Longrightarrow$ If $F(\hat{x}) \geq 0$ and $\mathrm{grad}(F)(\hat{x}) \neq 0$ then for every $x \in \mathbb{R}^n$ holds

$$F(x) < 0 \quad \Rightarrow \quad \mathrm{grad}(F)(\hat{x}) \cdot x \leq \mathrm{grad}(F)(\hat{x}) \cdot \hat{x}.$$

- simply exponential time–complexity & polynomial output–complexity

B/Mandel (1988), Krick (1990)

Two additional polynomials



- $F_0(x) \;:= -\hat{R}^2 + x^T x$ radius $\hat{R} \in \mathbb{Z}$ explicitly given
- $F_{s+1}(x) := \hat{F}(x) - z$ compute $z \in \mathbb{Z}$ using binary search

B/Heintz/Krick/Mandel/Solernó (1991), B (1997)

Reduction to a second problem

Problem (2)

$$\textbf{Find} \quad x^* \in Y \cap \mathbb{Z}^n \ \textbf{ or show } \ Y \cap \mathbb{Z}^n = \emptyset.$$

- $F_0, \ldots, F_{s+1} \in \mathbb{Z}[X]$ quasi–convex polynomials
- $A_0 \in \mathbb{Z}^{n \times n}$ positive definite matrix, $R_0 \in \mathbb{Z}$ integer number
- $F_0(x) := -R_0 + x^T A_0 x$
- $Y := \left\{ x \in \mathbb{R}^n \mid \bigwedge_{i=0}^{s+1} F_i(x) < 0 \right\}$ bounded open convex set

Strategy to solve Problem (2)

- generalize Lenstra's algorithm efficiently

B/Mandel (1988), Khachiyan/Porkolab (2000)

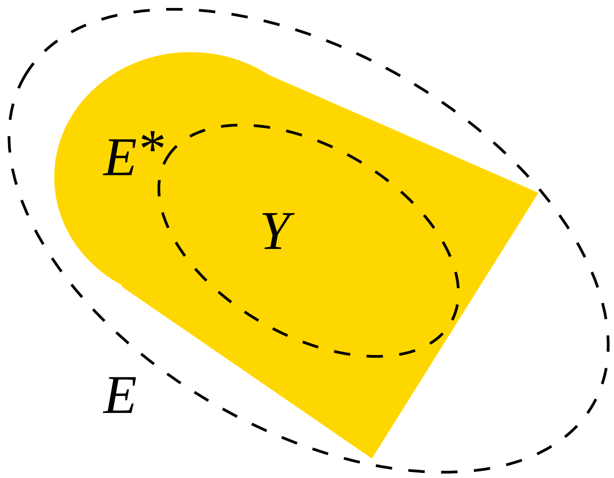
Solution of Problem (2)

Following Schrijver's method

- compute an ellipsoid E being tough on the set Y
- apply the basis reduction algorithm
- linear transformation of coordinates
- solve $2^{O(n^2)}$ problems of dimension $n-1$

E* is tough on *Y $:=$

- E, E^* concentric ellipsoids
- E^* is equal to E shrunk by the factor $\sqrt{(n+1)^3}$
- $E^* \subseteq Y \subseteq E$



John (1948), Lenstra/Lenstra/Lovász (1982), Schrijver (1994)

The main result

Parameters of the representation of the set *Y*

- n number of variables
- $s+2$ number of polynomials
- $d \geq 2$ degree bound of the polynomials
- ℓ maximum binary length of the coefficients

<u>Theorem</u>

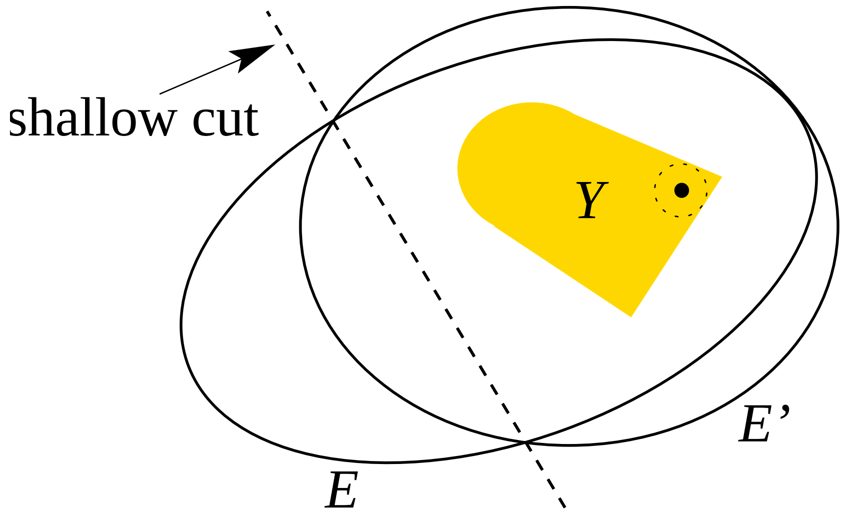
An ellipsoid E can be computed with time-complexity

$$O(s)\, \ell^{O(1)}\, d^{O(n)}$$

such that

E is tough on Y, if $Y \cap \mathbb{Z}^n \neq \emptyset$ holds.

The shallow-cut ellipsoid method



- ellipsoid E is replaced by E' having smaller volume
- until a tough ellipsoid is computed

Grötschel/Lovász/Schrijver (1993)

Finding shallow cuts

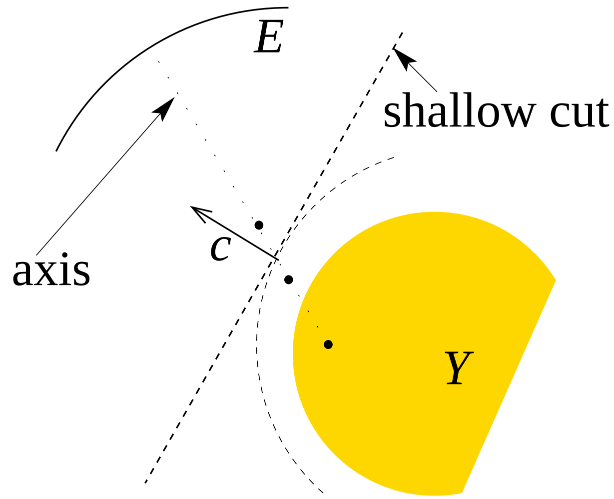
Lemma (Shallow cut)

- E ellipsoid such that $Y \subseteq E$ and E not tough

$\Longrightarrow$ $\exists$ an algorithm which outputs a shallow cut

Proof. (sketch)

- use every axis of E
- find points outside Y
- compute gradients $c \neq 0$
- c defines a shallow cut $\square$



Stoer/Witzgall (1970), von zur Gathen/Gerhard (1999)

Spheres around integer points

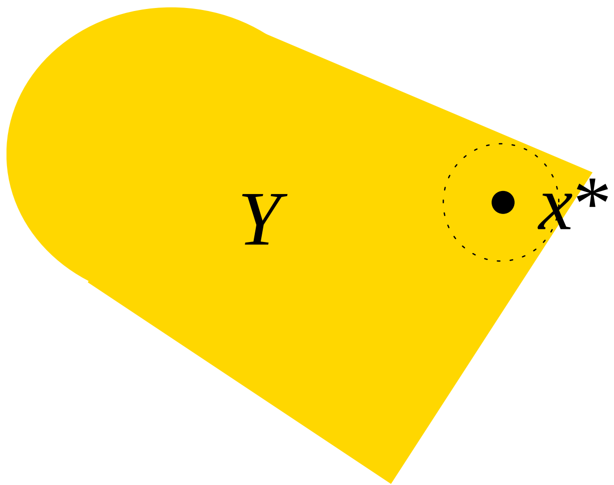
Lemma (Volume)

- $Y \cap \mathbb{Z}^n$ not empty

$\Longrightarrow$ $\exists$ a rational number $\varepsilon > 0$ such that $\varepsilon < \mathrm{vol}(Y)$

- of binary length $O(\ell)(d \cdot n)^{O(1)}$

Proof. (sketch)



- fix $x^* \in Y \cap \mathbb{Z}^n$
- $F_i(x^*) \leq -1, i = 0, \ldots, s+1$
- gradients are bounded
- distance to the border of Y $\square$

The proof of the **Theorem** is finished.

Complexity bounds

- **Problem (2)** is of time-complexity $O(s)\ell^{O(1)}d^{O(n)}2^{O(n^3)}$.
- A suitable radius is of binary length $O(\ell)d^{O(n)}$.

S. Heinz's results

- **Problem (1)** is of time-complexity $\boxed{O(s)\ell^{O(1)}d^{O(n)}2^{O(n^3)}}$.
- This is the best one can expect, if Lenstra's idea is applied.
- If n is fixed **Problem (1)** can be solved in **polynomial time**.

Khachiyan/Porkolab result (applied to **Problem (1)**)

- **Problem (1)** is of time-complexity $\boxed{\ell^{O(1)}s^{O(n^2)}d^{O(n^4)}}$.

Schrijver (1994),B/Heintz/Krick/Mandel/Solernó (1991), B (1997),

von zur Gathen/Gerhard (1999), Khachiyan/Porkolab (2000), Heinz (2005)

References

M. Aigner. *Diskrete Mathematik*. *Vieweg Studium*. Friedr. Vieweg & Sohn, 1993.

B. Bank, R. Mandel. *Parametric integer optimization*. Akademie-Verlag, Berlin, 1988.

B. Bank, J. Heintz, T. Krick, R. Mandel, P. Solernó. *Computability and complexity of polynomial optimization problems*. Preprint; 91-20. Fachbereich Mathematik der Humboldt-Universität zu Berlin, 1991.

B. Bank, J. Heintz, M. Giusti, G. Mbakop. *Equations for polar varieties and efficient real elimination*. Preprint; 99-15. Institut für Mathematik an der Mathematisch-Naturwissenschaftlichen Fakultät II der Humboldt-Universität zu Berlin, 1999.

B. Bank. *Optimization and real equation solving*, in *II Escuela de Matemática Aplicada (25 al 29 de agosto de 1997): Notas de los Cursos*. Universidad de Buenos Aires, 1997.

P. Bürgisser, M. Clausen, M. A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1997. With the Collaboration of Thomas Lickteig.

M. R. Garey, D. S. Johnson. *Computers and intractability*. W. H. Freeman and Company, 1979.

M. Grötschel, L. Lovász, A. Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag, second, corrected edition, 1993.

J. Heintz, M.-F. Roy, P. Solernó. *Sur la complexité du principe de Tarski-Seidenberg*, au *Bulletin de la Société Mathématique de France*, 118:101-126, 1990.

R. G. Jeroslow. *There cannot be any algorithm for integer programming with quadratic constraints*, in *Operations Research*, 21:221-224, 1973.

F. John. *Extremum problems with inequalities as subsidiary conditions*, in *Studies and Essays, presented to R. Courant on his 60th Birthday, January 8th*, pp. 187-204. Interscience Publishers, 1948.

L. Khachiyan. *Convexity and complexity in polynomial programming*, in *Proceedings of the International Congress of Mathematicians*, August 16-24, Warsaw, 1983.

L. Khachiyan, L. Porkolab. *Integer optimization on convex semialgebraic sets*, in *Discrete & Computational Geometry*, 23:207-224. Springer-Verlag, 2000.

D. E. Knuth. *The art of computer programming II*. Addison-Wesley Publishing Company, second edition, 1981.

L. Lehmann. *Effektives reelles Lösen einer multivariaten polynomialen Gleichung*. Diploma thesis, Humboldt-Universität zu Berlin, 1999.

A. K. Lenstra, H. W. Lenstra, L. Lovász. *Factoring polynomials with rational coefficients*, in *Mathematische Annalen*, 261:515-534. Springer-Verlag, 1982.

H. W. Lenstra. *Integer programming with a fixed number of variables*, in *Mathematics of Operations Research*, 8:538-548, 1983.

J. Renegar. *On the computational complexity of approximating solutions for real algebraic formulae*, in *SIAM Journal on Computing*, 21:1008-1025, 1992.

A. Schrijver. *Theory of linear and integer programming*. *Wiley-Interscience Series in Discrete Mathematics and Optimization*. John Wiley & Sons, 1994.

J. Stoer, C. Witzgall. *Convexity and optimization in finite dimension I*, volume 163 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1970.

J. von zur Gathen, J. Gerhard. *Modern computer algebra*. Cambridge University Press, 1999.