Problems from Optimization and Computational Algebra Equivalent to Hilbert's Nullstellensatz

Markus Bläser
Saarland University

Sagnik Dutta
MPI for Informatics

Gorav Jindal
University of Warsaw
→ University of Regensburg

Hilbert's Nullstellensatz Problem

HN_R over a ring R

Input: Polynomial equations $f_1 = 0, \cdots, f_m = 0$ with each $f_i \in R[x_1, \cdots, x_n]$.

Output: Does $\exists\ (a_1, \cdots, a_n) \in R^n$ such that $f_i(a_1, \cdots, a_n) = 0$ for all i?

Example:

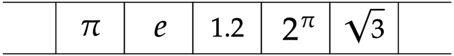
$$xy = 0,$$
$$(x-1)^2 + (y-1)^2 = 0.$$

Over $\mathbb{R} \to$ No solution.

Over $\mathbb{C} \to$ $(0, 1+i)$.

BSS model of computation

Blum-Shub-Smale (BSS) model: RAM model where registers can store arbitrary elements of the ring and each ring operation costs unit time



Memory tape

$\mathsf{P}_{\mathbf{R}}$: Decision problems over R solvable in deterministic polynomial time

$\mathsf{NP}_{\mathbf{R}}$: Decision problems over R solvable in non-deterministic polynomial time

Theorem (Blum, Shub, Smale '89)

HN_R *is* NP_R*-complete when* $R = \mathbb{R}$ *or* $\mathbb{C}$.

Existential Theory of The Reals

ETR language: True sentences of the form $\exists x_1, \cdots, x_n \ \phi(x_1, \cdots, x_n)$ over the reals.

$$\exists (x, y, z) \in \mathbb{R}^3 \ (x + y = 0) \wedge (x \cdot x - y \neq 1) \wedge (y.z + x \geq 5)$$

- $\exists\mathbb{R}$: Class of all languages polynomial-time many-one reducible to ETR.
- $\mathsf{NP} \subseteq \exists\mathbb{R} \subseteq \mathsf{PSPACE}$.
- $\forall\mathbb{R}$: Defined similarly with the $\forall$ quantifier.
- $\mathsf{HN}_{\mathbb{R}}^{\mathbb{Z}}$ is $\exists\mathbb{R}$-complete and its negation is $\forall\mathbb{R}$-complete.

Status of HN over different rings

Ring	Complexity of HN
$\mathbb{Z}$	Undecidable [Matiyasevich '70]
$\mathbb{Q}$	Decidability is open
$\mathbb{F}_2$ (or any finite field)	NP-complete
$\mathbb{C}$	In Π_2^P under GRH [Koiran '96]
$\mathbb{R}$	In PSPACE [Canny '88, Renegar '92]

Goal: Show HN_R-completeness for natural problems from Computational Algebra and Optimization

- Convexity testing
- Hyperbolicity testing
- Real stability testing
- Affine polynomial projection problem
- Sparse shift problem

Goal: Show HN_R-completeness for natural problems from Computational Algebra and Optimization

- Convexity testing
- Hyperbolicity testing
- Real stability testing
- Affine polynomial projection problem [A14, open question]
- Sparse shift problem [A-Open2]

Schaefer, Cardinal, Miltzow: *The Existential Theory of the Reals as a Complexity Class: A Compendium*, 2024

Previous results

- Convexity testing: coNP-hard (Ahmadi, Olshevsky, Parrilo, Tsitsiklis, 2010)
- Hyperbolicity testing: coNP-hard (Saunderson, 2019)
- Real stability testing: coNP-hard (Chin, 2024)
- Affine polynomial projection problem: NP-hard for infinite fields (Kayal 2012)
- Sparse shift problem: HN_R-complete when R is an integral domain that is not a field (Chillara, Grichener, Shpilka, 2023)

Convexity testing is $\forall\mathbb{R}$-complete

- *Hessian* of f:

$$H_f(x) = \begin{bmatrix} \\ \dfrac{\partial^2 f}{\partial x_i \partial x_j} \\ \\ \end{bmatrix}_{n\times n}$$

- f is *convex*
  $\iff \forall x \in \mathbb{R}^n \quad H_f(x)$ is positive semidefinite
  $\iff \forall x, z \in \mathbb{R}^n \quad z^T H_f(x) z \geq 0.$
- Convexity testing $\in \forall\mathbb{R}$.

f is homogeneous of degree 4 $\implies$ $z^T H_f(x) z$ is a **biquadratic polynomial**

$$f = x_1^3 x_2 + x_1 x_3 x_4^2$$

$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 \end{bmatrix} \begin{bmatrix} 6x_1x_2 & 3x_1^2 & x_4^2 & 2x_1x_3 \\ 3x_1^2 & 0 & 0 & 0 \\ x_4^2 & 0 & 0 & 2x_1x_4 \\ 2x_1x_3 & 0 & 2x_1x_4 & 2x_1x_3 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix}$$

$$= 6x_1x_2z_1^2 + 6x_1^2z_1z_2 + 2x_4^2z_1z_3 + 4x_1x_3z_1z_4 + 4x_1x_4z_3z_4 + 2x_1x_3z_4^2$$

f is homogeneous of degree 4 $\implies$ $z^T H_f(x) z$ is a **biquadratic polynomial**

$$f = x_1^3 x_2 + x_1 x_3 x_4^2$$

$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 \end{bmatrix} \begin{bmatrix} 6x_1x_2 & 3x_1^2 & x_4^2 & 2x_1x_3 \\ 3x_1^2 & 0 & 0 & 0 \\ x_4^2 & 0 & 0 & 2x_1x_4 \\ 2x_1x_3 & 0 & 2x_1x_4 & 2x_1x_3 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix}$$

$$= 6x_1x_2z_1^2 + 6x_1^2z_1z_2 + 2x_4^2z_1z_3 + 4x_1x_3z_1z_4 + 4x_1x_4z_3z_4 + 2x_1x_3z_4^2$$

Convexity testing for degree-4 homogeneous

$\leq_p$ Non-negativity testing for biquadratic polynomials

$\leq_p$ Universal theory of the reals

Convexity testing

$\geq$

Biquadratic non-negativity testing

$\geq$

Universal theory of the reals

[Ahmadi, Olshevsky, Parrilo, Tsitsiklis ’10]
(Used for showing coNP-hardness)

[Our contribution]

Convexity testing

$\geq$

Biquadratic non-negativity testing

$\geq$

Universal theory of the reals

[Ahmadi, Olshevsky, Parrilo, Tsitsiklis '10]

(Used for showing coNP-hardness)

[Our contribution]

$\forall\mathbb{R}$-complete problems

Easy:

$$\forall \boldsymbol{x} \in [-1,1]^n \quad f(\boldsymbol{x}) > 0 \qquad \left(\deg f = 4\right)$$

[Schaefer, Stefankovic '24]:

$$\forall \boldsymbol{x} \quad f(\boldsymbol{x}) \geq 0 \qquad \left(\deg f = 4\right)$$

Our mini-goal:

$$\forall \boldsymbol{x} \quad f(\boldsymbol{x}) \geq 0 \qquad \left(\text{semi-biquadratic } f\right)$$

Our final goal:

$$\forall \boldsymbol{x} \quad f(\boldsymbol{x}) \geq 0 \qquad \left(\text{biquadratic } f\right)$$

$$\forall \boldsymbol{x} \in [-1,1]^n \; f(\boldsymbol{x}) > 0 \qquad \longrightarrow \qquad \forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \; P(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \geq 0$$

Construction in [Schaefer, Stefankovic '24]:

$$P(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = f(\boldsymbol{x}) + 400\left((y_1 - 1/16)^2 + \sum_{i=2}^{m}(y_i - y_{i-1}^2)^2\right) - y_m^2 + y_m^4$$

$$+ \sum_{i=1}^{n}\left((x_i z_{i+n} - 2z_i)^2 + (z_{i+n} - z_i^2 - 1)^2\right)$$

$$\forall \boldsymbol{x} \in [-1,1]^n \; f(\boldsymbol{x}) > 0 \qquad \longrightarrow \qquad \forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \; P(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \geq 0$$

Construction in [Schaefer, Stefankovic '24]:

$$P(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = f(\boldsymbol{x}) + 400\left((y_1 - 1/16)^2 + \sum_{i=2}^{m} (y_i - y_{i-1}^2)^2\right) - y_m^2 + y_m^4$$
$$+ \sum_{i=1}^{n} \left((x_i z_{i+n} - 2z_i)^2 + (z_{i+n} - z_i^2 - 1)^2\right)$$

Strategy to semi-biquadratize:

- Fix problematic monomials by creating duplicate variables, e.g., replace y_m^4 with $y_m^2 w_m^2$ for a new variable w_m.
- Add the term $(y_m - w_m)^2$ to P.

Semi-biquadratic to Biquadratic

How do we biquadratize the polynomial $f(y_1, y_2, w_1, w_2) = y_1 y_2 w_1 w_2 + y_1 w_2 + w_1$?

- Homogenizing w.r.t. a variable?
  $t^4 f(y_1/t, y_2/t, w_1/t, w_2/t) = y_1 y_2 w_1 w_2 + y_1 w_2 t^2 + w_1 t^3 \quad \longrightarrow$ can't be biquadratic.

Semi-biquadratic to Biquadratic

How do we biquadratize the polynomial $f(y_1, y_2, w_1, w_2) = y_1 y_2 w_1 w_2 + y_1 w_2 + w_1$?

- Homogenizing w.r.t. a variable?
  $t^4 f(y_1/t, y_2/t, w_1/t, w_2/t) = y_1 y_2 w_1 w_2 + y_1 w_2 t^2 + w_1 t^3 \longrightarrow$ can't be biquadratic.
- Homogenize w.r.t. two variables.
  $s^2 t^2 f(y_1/s, y_2/s, w_1/t, w_2/t) = y_1 y_2 w_1 w_2 + y_1 s w_2 t + s^2 w_1 t.$

Affine Polynomial Projection Problem

$\mathsf{PolyProj}_F$ over a field F

Input: Polynomials $f \in \mathbb{F}[y_1, \cdots, y_m]$, $g \in \mathbb{F}[x_1, \cdots, x_n]$

Output: Does $\exists$ $m \times n$ matrix A and vector $b \in \mathbb{F}^m$ such that $f(A\mathbf{x} + b) = g(\mathbf{x})$

Importance:

- $\mathsf{VP} = \mathsf{VNP} \implies$ The Permanent Polynomial is an affine projection of the Determinant Polynomial with only quasi-poly blowup in size.
- Matrix multiplication has an $\tilde{O}(n^2)$ algorithm if $\mathsf{Mat}_n = \sum_{1 \le i,j,k \le n} x_{ij} y_{jk} z_{ki}$ is an affine projection of $\mathsf{SP}_m = \sum_{i=1}^{m} x_{i1} x_{i2} x_{i3}$ for $m = \tilde{O}(n^2)$.

Prior result

Theorem (Kayal '12)

$\mathsf{PolyProj}_F$ *is* NP*-hard for all infinite fields* F*.*

Our result

Theorem

$\mathsf{PolyProj}_F$ *is* HN_F*-hard for all fields* F*.*

Sparse Shift Problem

$\mathsf{SparseShift}_R$ over a ring R

Input: Polynomial $f \in R[x_1, \cdots, x_n]$
Output: Does $\exists\ (a_1, \cdots, a_n) \in R^n$ such that $f(x_1 + a_1, \cdots, x_n + a_n)$ has fewer monomials than $f(x_1, \cdots, x_n)$?

Prior result

Theorem (Chillara, Grichener, Shpilka '23)

$\mathsf{SparseShift}_R$ *is* HN_R*-hard for integral domains* R *which are not fields.*

Our result

Theorem

$\mathsf{SparseShift}_F$ *is* HN_F*-hard for all infinite fields* F*.*

$\implies$ $\mathsf{SparseShift}_F$ is HN_F-complete when $F = \mathbb{R}$ or $\mathbb{C}$.

Advertisement

Saarland University is inviting applications for a

- tenure track professorship (W2 tt W3) in
- quantum algorithms, complexity, and quantum information
- position within the CS department
- associated with the new center for quantum technologies

More infos: www.uni-saarland.de $\rightarrow$ job vacancies

Thank you!