The Multivariate Resultant is NP-hard in any Characteristic

Bruno Grenet, Pascal Koiran and Natacha Portier

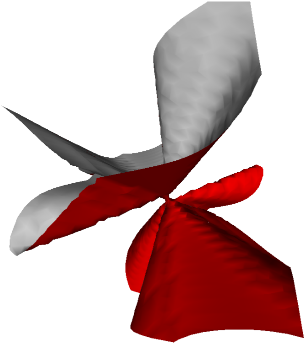
MC2 – LIP, ÉNS Lyon
Theory Group – DCS, U. of Toronto

Partly supported by Fields Institute

Brno – MFCS 2010 – August 23, 2010

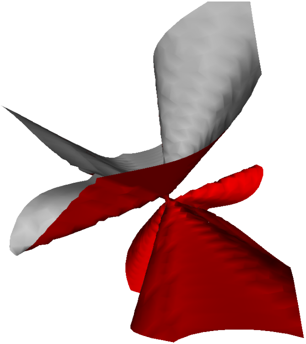
Motivation

- General framework: Resolution of polynomial systems



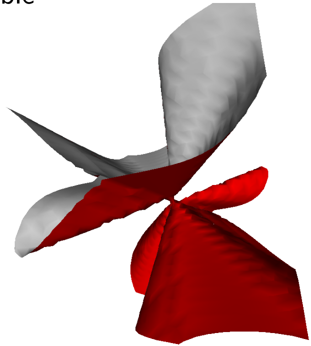
Motivation

- General framework: Resolution of polynomial systems
  - Useful everywhere!



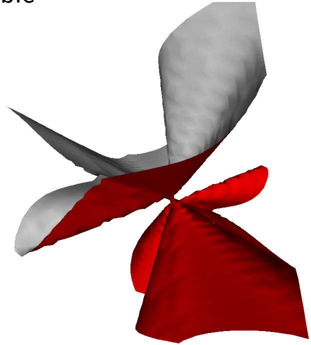
Motivation

- General framework: Resolution of polynomial systems
  - Useful everywhere!
- **Resultant:** condition for a system to be solvable



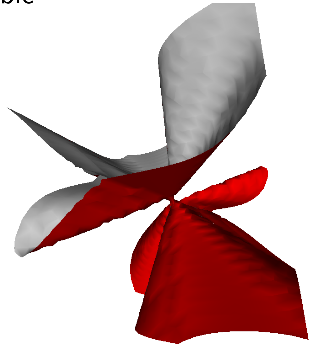
Motivation

- General framework: Resolution of polynomial systems
  - Useful everywhere!
- **Resultant:** condition for a system to be solvable
  - Elimination of quantifiers



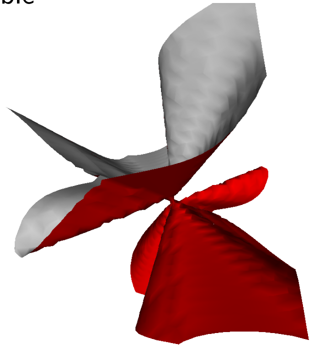
Motivation

- General framework: Resolution of polynomial systems
  - Useful everywhere!
- **Resultant:** condition for a system to be solvable
  - Elimination of quantifiers
  - Robot Motion Planning



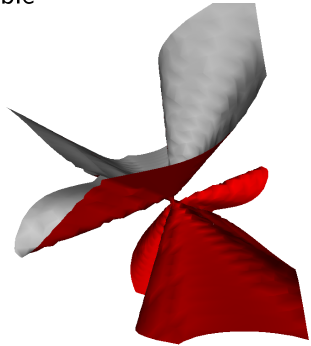
Motivation

- General framework: Resolution of polynomial systems
  - Useful everywhere!
- **Resultant:** condition for a system to be solvable
  - Elimination of quantifiers
  - Robot Motion Planning
  - Real Algebraic Geometry



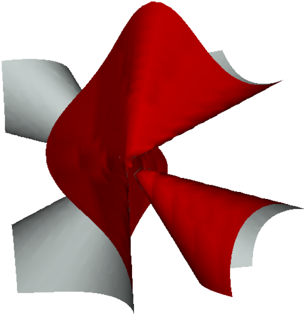
Motivation

- General framework: Resolution of polynomial systems
  - Useful everywhere!
- **Resultant:** condition for a system to be solvable
  - Elimination of quantifiers
  - Robot Motion Planning
  - Real Algebraic Geometry
  - ...



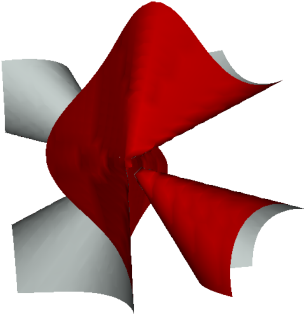
Content of the talk

- A few words about Elimination Theory



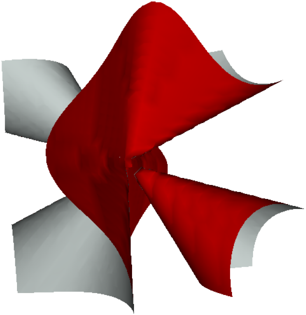
Content of the talk

- A few words about Elimination Theory
- First (simple) results about polynomial system solving



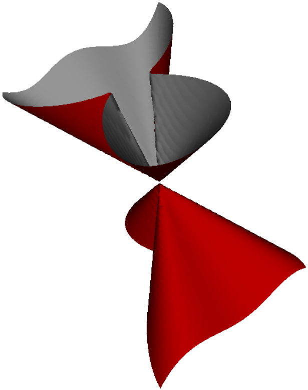
Content of the talk

- A few words about Elimination Theory
- First (simple) results about polynomial system solving
- Two ideas to prove NP-hardness



Outline

1. Elimination Theory
2. First results
3. NP-hardness in any characteristic
   - First idea ⇝ randomized reduction
   - Second idea ⇝ deterministic reduction



General form

$$f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$$

General form

$$f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$$

$$f_i = \sum_{|\alpha|_1 \leq d_i} \gamma_{i,\alpha} \bar{x}^\alpha$$

General form

$$f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$$

$$f_i = \sum_{|\alpha|_1 \leq d_i} \gamma_{i,\alpha} \bar{x}^\alpha$$

For which $\gamma_{i,\alpha}$ is there a root?

General form

$$f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$$

$$f_i = \sum_{|\alpha|_1 \leq d_i} \gamma_{i,\alpha} \bar{x}^\alpha$$

For which $\gamma_{i,\alpha}$ is there a root?

There exist $R_1, \dots, R_h \in \mathbb{K}[\bar{\gamma}]$ s.t.

$$\begin{cases} R_1(\bar{\gamma}) & = & 0 \\ & \vdots & \\ R_h(\bar{\gamma}) & = & 0 \end{cases} \Longrightarrow \exists \bar{a}, \quad \begin{cases} f_1(\bar{a}) & = & 0 \\ & \vdots & \\ f_s(\bar{a}) & = & 0 \end{cases}$$

Two Univariate Polynomials

- $P = \sum_{i=0}^{m} p_i x^i$, $Q = \sum_{j=0}^{n} q_j x^j$:

Two Univariate Polynomials

- $P = \sum_{i=0}^{m} p_i x^i \quad , \quad Q = \sum_{j=0}^{n} q_j x^j \quad :$

$$R = \det \begin{pmatrix} p_m & \cdots\cdots\cdots & p_0 & & \\ & \ddots & & \ddots & \\ & & p_m & \cdots\cdots\cdots & p_0 \\ q_n & \cdots\cdots & q_0 & & \\ & \ddots & & \ddots & \\ & & q_n & \cdots\cdots & q_0 \end{pmatrix}$$

Two Univariate Polynomials

- $P = \sum_{i=0}^{m} p_i x^i \quad , \; Q = \sum_{j=0}^{n} q_j x^j \quad :$

$$R = \det \begin{pmatrix} p_m & \cdots\cdots\cdots & p_0 & & \\ & \ddots & & \ddots & \\ & & p_m & \cdots\cdots\cdots & p_0 \\ q_n & \cdots\cdots & q_0 & & \\ & \ddots & & \ddots & \\ & & q_n & \cdots\cdots & q_0 \end{pmatrix}$$

$\rightsquigarrow$ Sylvester Matrix

Two Bivariate Polynomials

- $P = \sum_{i=0}^{m} p_i x^i y^{m-i}$, $Q = \sum_{j=0}^{n} q_j x^j y^{n-j}$:

$$R = \det \begin{pmatrix} p_m & \cdots\cdots\cdots & p_0 & & \\ & \ddots & & \ddots & \\ & & p_m & \cdots\cdots\cdots & p_0 \\ q_n & \cdots\cdots & q_0 & & \\ & \ddots & & \ddots & \\ & & q_n & \cdots\cdots & q_0 \end{pmatrix}$$

$\rightsquigarrow$ Sylvester Matrix

- Non trivial root?

More generally

- Wlog, homogeneous polynomials, non trivial roots

More generally

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n] \rightsquigarrow$ a unique resultant polynomial

More generally

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n] \rightsquigarrow$ a unique resultant polynomial
- s polynomials $\neq n$ variables $\rightsquigarrow$ several polynomials needed

More generally

Multivariate Resultant

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n] \rightsquigarrow$ a unique resultant polynomial
- s polynomials $\neq$ n variables $\rightsquigarrow$ several polynomials needed

More generally

Multivariate Resultant

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n] \rightsquigarrow$ a unique resultant polynomial
- s polynomials $\neq$ n variables $\rightsquigarrow$ several polynomials needed
- Sylvester Matrix $\rightsquigarrow$ Macaulay Matrix (exponential size)

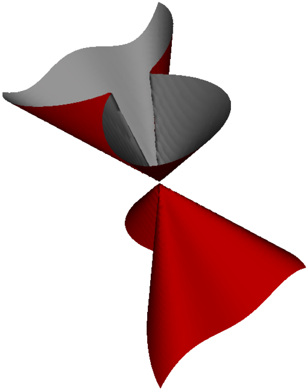
More generally

Multivariate Resultant

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ $\rightsquigarrow$ a unique resultant polynomial
- s polynomials $\neq$ n variables $\rightsquigarrow$ several polynomials needed

- Sylvester Matrix $\rightsquigarrow$ Macaulay Matrix (exponential size)
- Resultant computable in polynomial space

Outline



Definitions

Hilbert's Nullstellensatz over $\mathbb{K}$: $\mathtt{HN}(\mathbb{K})$

Input: $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$

Question: $\exists ?\ \bar{a} \in \bar{\mathbb{K}}^{n+1}, \begin{cases} f_1(\bar{a}) & = & 0 \\ & \vdots & \\ f_s(\bar{a}) & = & 0 \end{cases}$

Definitions

Hilbert's Nullstellensatz over $\mathbb{K}$: $\mathtt{HN}(\mathbb{K})$

Input: $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$

Question: $\exists?\ \bar{a} \in \bar{\mathbb{K}}^{n+1}, \begin{cases} f_1(\bar{a}) & = & 0 \\ & \vdots & \\ f_s(\bar{a}) & = & 0 \end{cases}$

- $\mathtt{H_2N}(\mathbb{K})$: homogeneous polynomials ($\bar{a} \neq \bar{0}$)

Definitions

Hilbert's Nullstellensatz over $\mathbb{K}$: $\mathtt{HN}(\mathbb{K})$

Input: $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$

Question: $\exists?\ \bar{a} \in \bar{\mathbb{K}}^{n+1}, \begin{cases} f_1(\bar{a}) & = & 0 \\ & \vdots & \\ f_s(\bar{a}) & = & 0 \end{cases}$

- $\mathtt{H_2N}(\mathbb{K})$: homogeneous polynomials ($\bar{a} \neq \bar{0}$)
- $\mathtt{H_2N}^{\square}(\mathbb{K})$: $s = n + 1$ homogeneous polynomials

Upper bounds

Lemma

For all $\mathbb{K}$, $\mathtt{H_2N}^{\Box}(\mathbb{K}) \leq_m^p \mathtt{H_2N}(\mathbb{K}) \leq_m^p \mathtt{HN}(\mathbb{K})$

Upper bounds

Lemma

For all $\mathbb{K}$, $\mathtt{H_2N}^{\square}(\mathbb{K}) \leq_m^p \mathtt{H_2N}(\mathbb{K}) \leq_m^p \mathtt{HN}(\mathbb{K})$

Proof. New variables $y_0, \ldots, y_n$ and new polynomial $\sum_i x_i y_i - 1$ □

Upper bounds

Lemma

For all $\mathbb{K}$, $\mathtt{H_2N}^{\square}(\mathbb{K}) \leq_m^p \mathtt{H_2N}(\mathbb{K}) \leq_m^p \mathtt{HN}(\mathbb{K})$

Proof. New variables $y_0, \ldots, y_n$ and new polynomial $\sum_i x_i y_i - 1$ □

Corollary

Under the Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square}(\mathbb{Z}) \in \mathsf{AM}$

Upper bounds

Lemma

For all $\mathbb{K}$, $\mathtt{H_2N}^{\square}(\mathbb{K}) \leq_m^p \mathtt{H_2N}(\mathbb{K}) \leq_m^p \mathtt{HN}(\mathbb{K})$

Proof. New variables $y_0, \ldots, y_n$ and new polynomial $\sum_i x_i y_i - 1$ □

Corollary

Under the Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square}(\mathbb{Z}) \in \mathsf{AM}$

$\rightsquigarrow \mathsf{NP} \subseteq \mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$

Upper bounds

Lemma

For all $\mathbb{K}$, $\mathtt{H_2N}^{\square}(\mathbb{K}) \leq_m^p \mathtt{H_2N}(\mathbb{K}) \leq_m^p \mathtt{HN}(\mathbb{K})$

Proof. New variables $y_0, \ldots, y_n$ and new polynomial $\sum_i x_i y_i - 1$ □

Corollary

Under the Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square}(\mathbb{Z}) \in \mathsf{AM}$

Proof. [Koiran, 1996] Under GRH, $\mathtt{HN}(\mathbb{Z}) \in \mathsf{AM}$. □

$\rightsquigarrow \mathsf{NP} \subseteq \mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$

Upper bounds

Lemma

For all $\mathbb{K}$, $\mathtt{H_2N}^{\square}(\mathbb{K}) \leq_m^p \mathtt{H_2N}(\mathbb{K}) \leq_m^p \mathtt{HN}(\mathbb{K})$

Proof. New variables $y_0, \dots, y_n$ and new polynomial $\sum_i x_i y_i - 1$ □

Corollary

Under the Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square}(\mathbb{Z}) \in \mathrm{AM}$

Proof. [Koiran, 1996] Under GRH, $\mathtt{HN}(\mathbb{Z}) \in \mathrm{AM}$. □

$\rightsquigarrow \mathrm{NP} \subseteq \mathrm{AM} \subseteq \Pi_2^{\mathrm{P}}$

Remark. Best known upper bound for $\mathbb{K} = \mathbb{F}_p$ is PSPACE.

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ *and* $\mathtt{H_2N}(\mathbb{K})$ *are* NP-*hard.*

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ *and* $\mathtt{H_2N}(\mathbb{K})$ *are* NP-*hard.*

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ *and* $\mathtt{H_2N}(\mathbb{K})$ *are* NP-*hard.*

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Boolsys

- Boolean variables $X_1, \ldots, X_n$
- Equations
  - $X_i = \text{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

□

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ *and* $\mathtt{H_2N}(\mathbb{K})$ *are* NP-*hard.*

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Boolsys

- Boolean variables $X_1, \ldots, X_n$
- Equations
  - $X_i = \mathrm{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

$\mathtt{H_2N}$

- Variables (over $\mathbb{K}$) x_0 and $x_1, \ldots, x_n$
- Polynomials

□

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ *and* $\mathtt{H_2N}(\mathbb{K})$ *are* NP-*hard.*

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Boolsys

- Boolean variables $X_1, \dots, X_n$
- Equations
  - $X_i = \text{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

$\mathtt{H_2N}$

- Variables (over $\mathbb{K}$) x_0 and $x_1, \dots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every $i > 0$ and

□

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ *and* $\mathtt{H_2N}(\mathbb{K})$ *are* NP-*hard.*

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Boolsys

- Boolean variables $X_1, \dots, X_n$
- Equations
  - $X_i = \mathrm{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

$\mathtt{H_2N}$

- Variables (over $\mathbb{K}$) x_0 and $x_1, \dots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every $i > 0$ and
  - $x_0 \cdot (x_i + x_0)$

□

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ and $\mathtt{H_2N}(\mathbb{K})$ are NP-hard.

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Boolsys

- Boolean variables $X_1, \ldots, X_n$
- Equations
  - $X_i = \mathrm{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

$\mathtt{H_2N}$

- Variables (over $\mathbb{K}$) x_0 and $x_1, \ldots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every $i > 0$ and
  - $x_0 \cdot (x_i + x_0)$
  - $x_0 \cdot (x_i + x_j)$

∎

Lower bounds

Theorem

For all $\mathbb{K}$, $\mathtt{HN}(\mathbb{K})$ and $\mathtt{H_2N}(\mathbb{K})$ are NP-hard.

Proof. Case $\mathtt{H_2N}(\mathbb{K})$, with $\mathrm{char}(\mathbb{K}) \neq 2$:

Boolsys

- Boolean variables $X_1, \dots, X_n$
- Equations
  - $X_i = \text{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

$\mathtt{H_2N}$

- Variables (over $\mathbb{K}$) x_0 and $x_1, \dots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every $i > 0$ and
  - $x_0 \cdot (x_i + x_0)$
  - $x_0 \cdot (x_i + x_j)$
  - $(x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0)$

□

Lower bound over $\mathbb{Z}$

Theorem

$\mathtt{H_2N}^{\square}(\mathbb{Z})$ *is* NP*-hard.*

Lower bound over $\mathbb{Z}$

Theorem

$\mathtt{H_2N}^{\square}(\mathbb{Z})$ *is* NP-*hard.*

Proof. Partition: $S = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}$, $\exists ?\ S' \subseteq S$, $\sum_{i \in S'} u_i = \sum_{j \notin S'} u_j$

Lower bound over $\mathbb{Z}$

Theorem

$\mathtt{H_2N}^{\square}(\mathbb{Z})$ *is* NP*-hard.*

Proof. $\texttt{Partition}$: $S = \{u_1, \dots, u_n\} \subseteq \mathbb{Z}$, $\exists ?\ S' \subseteq S$, $\sum_{i \in S'} u_i = \sum_{j \notin S'} u_j$

$$\rightsquigarrow \begin{cases} x_1^2 - x_0^2 & = & 0 \\ & \vdots & \\ x_n^2 - x_0^2 & = & 0 \\ u_1 x_1 + \cdots + u_n x_n & = & 0 \end{cases}$$

$\square$

Summary so far

Upper bounds

	HN	H_2N	$H_2N^{\square}$
Over $\mathbb{Z}$	AM		
Over $\mathbb{F}_p$	PSPACE		

Summary so far

Upper bounds

	HN	H_2N	$H_2N^{\square}$
Over $\mathbb{Z}$	AM		
Over $\mathbb{F}_p$	PSPACE		

Lower bounds

	HN	H_2N	$H_2N^{\square}$
Over $\mathbb{Z}$	NP	NP	NP
Over $\mathbb{F}_p$	NP	NP	???

Summary so far

Upper bounds

	HN	H_2N	$H_2N^{\square}$
Over $\mathbb{Z}$	AM		
Over $\mathbb{F}_p$	PSPACE		

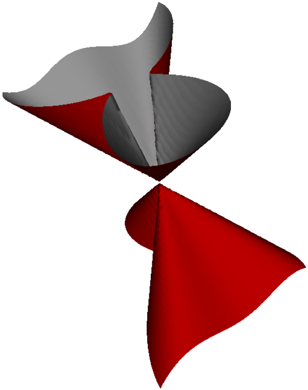
Lower bounds

	HN	H_2N	$H_2N^{\square}$
Over $\mathbb{Z}$	NP	NP	NP
Over $\mathbb{F}_p$	NP	NP	???

- NP = AM "under plausible complexity conjectures"

Outline

1. Elimination Theory
2. First results
3. NP-hardness in any characteristic
   - First idea $\rightsquigarrow$ randomized reduction
   - Second idea $\rightsquigarrow$ deterministic reduction



Two ideas, two reductions

- $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$

Two ideas, two reductions

- $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$
  - $s \leq n$: always a root

Two ideas, two reductions

- $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$
  - $s \leq n$: always a root
  - $s > n + 1$: NP-hard

Two ideas, two reductions

- $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$
  - $s \leq n$: always a root
  - $s > n + 1$: NP-hard
  - $s = n + 1$: ?

Two ideas, two reductions

- $f_1, \dots, f_s \in \mathbb{K}[x_0, \dots, x_n]$
  - $s \leq n$: always a root
  - $s > n+1$: NP-hard
  - $s = n+1$: ?
- Reduction from the case $s > n+1$

Two ideas, two reductions

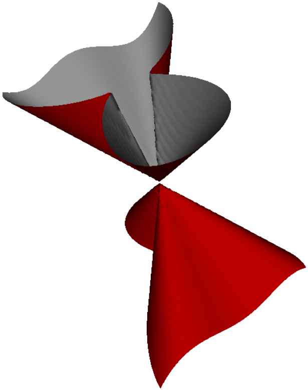
- $f_1, \dots, f_s \in \mathbb{K}[x_0, \dots, x_n]$
  - $s \leq n$: always a root
  - $s > n + 1$: NP-hard
  - $s = n + 1$: ?
- Reduction from the case $s > n + 1$
  - First idea: decrease the number of polynomials

Two ideas, two reductions

- $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$
  - $s \leq n$: always a root
  - $s > n+1$: NP-hard
  - $s = n+1$: ?
- Reduction from the case $s > n+1$
  - First idea: decrease the number of polynomials
  - Second idea: increase the number of variables

Outline

1. Elimination Theory
2. First results
3. NP-hardness in any characteristic
   - First idea ⇝ randomized reduction
   - Second idea ⇝ deterministic reduction



Randomized reduction?

- An instance I of P_1

Randomized reduction?

- An instance I of P_1
- A randomized polynomial time algorithm A

Randomized reduction?

- An instance I of P_1
- A randomized polynomial time algorithm A
- $A(I)$ is an instance of P_2

Randomized reduction?

- An instance I of P_1
- A randomized polynomial time algorithm A
- $A(I)$ is an instance of P_2
- I is a positive instance $\implies$ $A(I)$ is a positive instance

Randomized reduction?

- An instance I of P_1
- A randomized polynomial time algorithm A
- $A(I)$ is an instance of P_2
- I is a positive instance $\implies$ $A(I)$ is a positive instance
- I is a negative instance $\implies$ $\mathbb{P}[A(I) \text{ is a positive instance}] \leq 1/3$

Reduction

- If $f_1, \ldots, f_s$ homogeneous of degree 2,

$$g_i := \sum_{j=1}^{s} \alpha_{ij} f_j, 0 \leq i \leq n$$

Reduction

- If $f_1, \ldots, f_s$ homogeneous of degree 2,

$$g_i := \sum_{j=1}^{s} \alpha_{ij} f_j, 0 \leq i \leq n$$

- $\forall j, f_j(\bar{x}) = 0 \implies \forall i, g_i(\bar{x}) = 0$

Reduction

- If $f_1, \ldots, f_s$ homogeneous of degree 2,

$$g_i := \sum_{j=1}^{s} \alpha_{ij} f_j, 0 \leq i \leq n$$

- $\forall j, f_j(\bar{x}) = 0 \iff \forall i, g_i(\bar{x}) = 0$

if α_{ij} algebraically independent

Reduction

- If $f_1, \ldots, f_s$ homogeneous of degree 2,

$$g_i := \sum_{j=1}^{s} \alpha_{ij} f_j, 0 \leq i \leq n$$

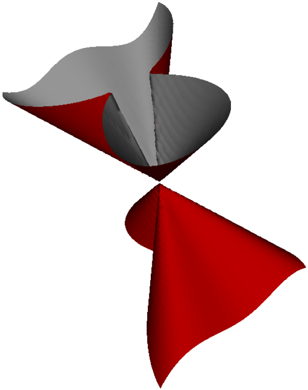
- $\forall j, f_j(\bar{x}) = 0 \iff \forall i, g_i(\bar{x}) = 0$

if α_{ij} algebraically independent

if random α_{ij}: with high probability

(Quantifier Elimination + Schwartz-Zippel Lemma)

Outline



Introduction

- Randomized reduction: fewer polynomials

Introduction

- Randomized reduction: fewer polynomials

  $\neq$ Deterministic reduction: more variables

Introduction

- Randomized reduction: fewer polynomials

  $\neq$ Deterministic reduction: more variables

$\mathtt{H_2N}$

- Variables over $\mathbb{K}$ x_0 and $x_1, \dots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every i
  - $x_0 \cdot (x_i + x_0)$
  - $x_0 \cdot (x_i + x_j)$
  - $(x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0)$

Introduction

- Randomized reduction: fewer polynomials

  $\neq$ Deterministic reduction: more variables

$\mathtt{H_2N}$

- Variables over $\mathbb{K}$ x_0 and $x_1, \ldots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every i $\quad \to \quad f_1, \ldots, f_n$

$$\left.\begin{array}{l} \blacktriangleright\ x_0 \cdot (x_i + x_0) \\ \blacktriangleright\ x_0 \cdot (x_i + x_j) \\ \blacktriangleright\ (x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0) \end{array}\right\} \quad \to \quad f_{n+1}, \ldots, f_s$$

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$

New system

$$g(\bar{x}, \bar{y}) = \left(\quad \right)$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$

New system

$$g(\bar{x}, \bar{y}) = \begin{pmatrix} f_1(\bar{x}) & \\ \vdots & \text{(unchanged)} \\ f_n(\bar{x}) & \\ & \\ & \\ & \end{pmatrix}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$

New system

$$g(\bar{x}, \bar{y}) = \begin{pmatrix} f_1(\bar{x}) & \\ \vdots & \text{(unchanged)} \\ f_n(\bar{x}) & \\ f_{n+1}(\bar{x}) & + \lambda y_1^2 \\ & \\ & \\ & \end{pmatrix}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$

New system

$$g(\bar{x}, \bar{y}) = \begin{pmatrix} f_1(\bar{x}) & & \\ \vdots & & \text{(unchanged)} \\ f_n(\bar{x}) & & \\ f_{n+1}(\bar{x}) & & + \lambda y_1^2 \\ f_{n+2}(\bar{x}) & - y_1^2 & + \lambda y_2^2 \\ & & \\ & & \end{pmatrix}$$

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$

New system

$$g(\bar{x}, \bar{y}) = \begin{pmatrix} f_1(\bar{x}) & & \\ \vdots & \text{(unchanged)} & \\ f_n(\bar{x}) & & \\ f_{n+1}(\bar{x}) & & + \lambda y_1^2 \\ f_{n+2}(\bar{x}) & - y_1^2 & + \lambda y_2^2 \\ \vdots & & \\ f_{s-1}(\bar{x}) & - y_{s-n-2}^2 & + \lambda y_{s-n-1}^2 \end{pmatrix}$$

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$

New system

$$g(\bar{x}, \bar{y}) = \begin{pmatrix} f_1(\bar{x}) & & \\ \vdots & & \text{(unchanged)} \\ f_n(\bar{x}) & & \\ f_{n+1}(\bar{x}) & & + \lambda y_1^2 \\ f_{n+2}(\bar{x}) & - y_1^2 & + \lambda y_2^2 \\ \vdots & & \\ f_{s-1}(\bar{x}) & - y_{s-n-2}^2 & + \lambda y_{s-n-1}^2 \\ f_s(\bar{x}) & - y_{s-n-1}^2 & \end{pmatrix}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$

New system

$$g(\bar{x},\bar{y}) = \begin{pmatrix} f_1(\bar{x}) & & \\ \vdots & \text{(unchanged)} & \\ f_n(\bar{x}) & & \\ f_{n+1}(\bar{x}) & & + \lambda y_1^2 \\ f_{n+2}(\bar{x}) & - y_1^2 & + \lambda y_2^2 \\ \vdots & & \\ f_{s-1}(\bar{x}) & - y_{s-n-2}^2 & + \lambda y_{s-n-1}^2 \\ f_s(\bar{x}) & - y_{s-n-1}^2 & \end{pmatrix} \leadsto \begin{array}{c} \bar{a} \text{ root of } f \\ \Downarrow \\ (\bar{a},\bar{0}) \text{ root of } g \end{array}$$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} f_1(\bar{a}) & & \\ \vdots & & \\ f_n(\bar{a}) & & \\ f_{n+1}(\bar{a}) & & +\lambda b_1^2 \\ f_{n+2}(\bar{a}) & -b_1^2 & +\lambda b_2^2 \\ \vdots & & \\ f_{s-1}(\bar{a}) & -b_{s-n-2}^2 & +\lambda b_{s-n-1}^2 \\ f_s(\bar{a}) & -b_{s-n-1}^2 & \end{pmatrix}$$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} f_1(\bar{a}) \\ \vdots \\ f_n(\bar{a}) \\ f_{n+1}(\bar{a} & & +\lambda b_1^2 \\ f_{n+2}(\bar{a} & -b_1^2 & +\lambda b_2^2 \\ \vdots \\ f_{s-1}(\bar{a} & -b_{s-n-2}^2 & +\lambda b_{s-n-1}^2 \\ f_s(\bar{a}) & -b_{s-n-1}^2 \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} f_1(\bar{a}) & & \\ \vdots & & \\ f_n(\bar{a}) & & \\ f_{n+1}(\bar{a}) & & +\lambda b_1^2 \\ f_{n+2}(\bar{a}) & -b_1^2 & +\lambda b_2^2 \\ \vdots & & \\ f_{s-1}(\bar{a}) & -b_{s-n-2}^2 & +\lambda b_{s-n-1}^2 \\ f_s(\bar{a}) & -b_{s-n-1}^2 & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} f_1(\bar{a}) & & \\ \vdots & & \\ f_n(\bar{a}) & & \\ f_{n+1}(\bar{a}) & & +\lambda b_1^2 \\ f_{n+2}(\bar{a}) & -b_1^2 & +\lambda b_2^2 \\ \vdots & & \\ f_{s-1}(\bar{a}) & -b_{s-n-2}^2 & +\lambda b_{s-n-1}^2 \\ f_s(\bar{a}) & -b_{s-n-1}^2 & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} \epsilon_1 & & +\lambda b_1^2 \\ \epsilon_2 & -b_1^2 & +\lambda b_2^2 \\ \vdots & & \\ \epsilon_{s-n-1} & -b_{s-n-2}^2 & +\lambda b_{s-n-1}^2 \\ \epsilon_{s-n} & -b_{s-n-1}^2 & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} \epsilon_1 & & +\lambda b_1^2 \\ \epsilon_2 & -b_1^2 & +\lambda b_2^2 \\ \vdots & & \\ \epsilon_{s-n-1} & -b_{s-n-2}^2 & +\lambda b_{s-n-1}^2 \\ \epsilon_{s-n} & -b_{s-n-1}^2 & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$
- $Y_i = b_i^2$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} \epsilon_1 & & +\lambda Y_1 \\ \epsilon_2 & -Y_1 & +\lambda Y_2 \\ \vdots & & \\ \epsilon_{s-n-1} & -Y_{s-n-2} & +\lambda Y_{s-n-1} \\ \epsilon_{s-n} & -Y_{s-n-1} & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$
- $Y_i = b_i^2$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} \epsilon_1 & & +\lambda Y_1 & \\ \epsilon_2 & -Y_1 & +\lambda Y_2 & \\ \vdots & & & \\ \epsilon_{s-n-1} & -Y_{s-n-2} & +\lambda Y_{s-n-1} & \\ \epsilon_{s-n} & -Y_{s-n-1} & & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$
- $Y_i = b_i^2$

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_{s-n}\lambda^{s-n-1}\right)$$

Equivalence?

$(\bar{a}, \bar{b})$: a non trivial root

$$\begin{pmatrix} \epsilon_1 & & +\lambda Y_1 \\ \epsilon_2 & -Y_1 & +\lambda Y_2 \\ \vdots & & \\ \epsilon_{s-n-1} & -Y_{s-n-2} & +\lambda Y_{s-n-1} \\ \epsilon_{s-n} & -Y_{s-n-1} & \end{pmatrix}$$

- $\bar{a} = 0 \implies \bar{b} = 0$
- $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$
- $Y_i = b_i^2$

$$\det = \pm \left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_{s-n}\lambda^{s-n-1}\right)$$

$$\det = 0 \overset{?}{\implies} \forall i,\ \epsilon_i = 0 \implies f_1(\bar{a}) = \cdots = f_s(\bar{a}) = 0$$

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:
  - P: irreducible degree-N polynomial of $\mathbb{K}[X]$

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:
  - P: irreducible degree-N polynomial of $\mathbb{K}[X]$
  - $\mathbb{L} = \mathbb{K}[X]/(P)$

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:
  - P: irreducible degree-N polynomial of $\mathbb{K}[X]$
  - $\mathbb{L} = \mathbb{K}[X]/(P)$
  - $\lambda = X \in \mathbb{L}$ is sufficient

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:
  - P: irreducible degree-N polynomial of $\mathbb{K}[X]$ ← [Shoup 1990] Polynomial time algorithm
  - $\mathbb{L} = \mathbb{K}[X]/(P)$
  - $\lambda = X \in \mathbb{L}$ is sufficient

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:
  - P: irreducible degree-N polynomial of $\mathbb{K}[X]$ ← [Shoup 1990] Polynomial time algorithm
  - $\mathbb{L} = \mathbb{K}[X]/(P)$
  - $\lambda = X \in \mathbb{L}$ is sufficient
- Coefficients in $\mathbb{K}$ instead of $\mathbb{L}$: "put P inside the system"

Last step

$$\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_N\lambda^{N-1}\right)$$

- Characteristic 0:
  - $\epsilon_i \in \mathbb{Z}$, bounded
  - $\lambda > \max_i \epsilon_i$
  - Unicity of base-λ decomposition
- Positive Characteristic:
  - P: irreducible degree-N polynomial of $\mathbb{K}[X]$ ← [Shoup 1990] Polynomial time algorithm
  - $\mathbb{L} = \mathbb{K}[X]/(P)$
  - $\lambda = X \in \mathbb{L}$ is sufficient
- Coefficients in $\mathbb{K}$ instead of $\mathbb{L}$: "put P inside the system"

$$\mathtt{H_2N}^{\square}(\mathbb{K}) \text{ is NP-hard}$$

Conclusion

- This answers a question of Canny (1987)

Conclusion

- This answers a question of Canny (1987)
- Upper (AM) and lower (NP) bounds are "almost equal" for characteristic 0

Conclusion

- 🙂 This answers a question of Canny (1987)
- 🙂 Upper (AM) and lower (NP) bounds are "almost equal" for characteristic 0

- 🙁 Huge gap for positive characteristic

Conclusion

- 🙂 This answers a question of Canny (1987)
- 🙂 Upper (AM) and lower (NP) bounds are “almost equal” for characteristic 0

- 🙁 Huge gap for positive characteristic
- 🙁 The method seems unable to prove results in algebraic complexity

Conclusion

- 🙂 This answers a question of Canny (1987)
- 🙂 Upper (AM) and lower (NP) bounds are "almost equal" for characteristic 0

- ☹ Huge gap for positive characteristic
- ☹ The method seems unable to prove results in algebraic complexity

Thank you!