The multivariate resultant is NP-hard in any characteristic

Bruno Grenet, Pascal Koiran and Natacha Portier

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

Partly supported by Fields Institute

EJC IM 2010 – March 29, 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

A modern theory!

MODERN ALGEBRA

By B. L. VAN DER WAERDEN, Ph.D.
PROFESSOR OF MATHEMATICS
AT THE UNIVERSITY OF AMSTERDAM

In part a development from lectures
By E. ARTIN and E. NOETHER

VOLUME II

Translated from the second revised German edition
By THEODORE J. BENAC, Ph.D.
ASSOCIATE PROFESSOR, DEPARTMENT OF MATHEMATICS
U.S. NAVAL ACADEMY

CHAPTER XI

ELIMINATION THEORY

In elimination theory we study systems of algebraic equations in several unknowns in order to set up conditions for their solvability as well as formulas for calculating their solutions in various cases. In this chapter the corresponding theory for linear equations, i.e., the theory of determinants, is assumed as known. Furthermore, it shall also be assumed that *one* equation in a *single* unknown of degree higher than one can be solved. or more precisely, if such an equation can not be resolved in a given field. an extension field may be constructed in which it is decomposable. and in fact one in which it may be completely decomposed (Chapter 5). In the following when we refer to the "solutions of an equation" or the "zeros of a polynomial," we shall always assume that the solutions are in a suitably chosen extension field of the fixed commutative field K.

77. THE RESULTANT SYSTEM OF SEVERAL POLYNOMIALS IN A SINGLE VARIABLE

THEOREM. *Let $f_1, \ldots, f_r$ be r polynomials in a single variable of given degrees with indeterminate coefficients. Then there exists a system $D_1, \ldots, D_h$ of integral polynomials in these coefficients with the property that if these coefficients are assigned values from the field K the conditions $D_1 = 0, \ldots, D_h = 0$ are necessary and sufficient in order that either the equations $f_1 = 0, \ldots, f_r = 0$ have a solution in a suitable extension field or that the formal leading coefficients of all polynomials $f_1, \ldots, f_r$ vanish.*

The proof is based on *Kronecker's method of elimination.*

First, we transform the polynomials $f_1, \ldots, f_r$ into polynomials of the same degree by multiplying every polynomial f_i by x^{n-n_i} and $(x-1)^{n-n_i}$ provided that n_i is smaller than n where n is the greatest (formal) degree of the given polynomials. In this way two polynomials of formal degree n arise from f_i such that for any specialization of the coefficients their common zeros and their leading coefficients are the same as those of f_i. This system of polynomials of the same degree may contain more polynomials than are in the system $f_1, \ldots, f_r$ but it has the same common zeros. We designate these polynomials by $g_1, \ldots, g_s$.

1

Most recent book: 1950

General form

- Some polynomials: $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n]$,

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

General form

- Some polynomials: $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n]$,

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

- Condition on the $\gamma_{i,\alpha}$ for the system to have a root?

General form

- Some polynomials: $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n]$,

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

- Condition on the $\gamma_{i,\alpha}$ for the system to have a root?

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

$$R_1(\bar{\gamma}) = \cdots = R_h(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = \cdots = f_s(\bar{X}) = 0$$

Special cases

- If $s = 2$ & $n = 1$ then $h = 1$:

$$R(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = f_2(\bar{X}) = 0$$

Special cases

- If $s = 2$ & $n = 1$ then $h = 1$:

$$R(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = f_2(\bar{X}) = 0$$

$\rightsquigarrow$ Sylvester Resultant

Special cases

- If $s = 2$ & $n = 1$ then $h = 1$:

$$R(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = f_2(\bar{X}) = 0$$

$$\rightsquigarrow \text{Sylvester Resultant}$$

- Homogeneous polynomials: non trivial root?

Special cases

- If $s = 2$ & $n = 1$ then $h = 1$:

$$R(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = f_2(\bar{X}) = 0$$

$$\rightsquigarrow \text{Sylvester Resultant}$$

- Homogeneous polynomials: non trivial root?
- $s = n$: only case with $h = 1$

Special cases

- If $s = 2$ & $n = 1$ then $h = 1$:

$$R(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = f_2(\bar{X}) = 0$$

$$\rightsquigarrow \text{Sylvester Resultant}$$

- Homogeneous polynomials: non trivial root?
- $s = n$: only case with $h = 1$
- In most cases, s polynomials $\rightsquigarrow$ n polynomials is possible

Special cases

- If $s = 2$ & $n = 1$ then $h = 1$:

$$R(\bar{\gamma}) = 0 \implies \exists \bar{X}, f_1(\bar{X}) = f_2(\bar{X}) = 0$$

$\rightsquigarrow$ Sylvester Resultant

- Homogeneous polynomials: non trivial root?
- $s = n$: only case with $h = 1$ $\leftarrow$ our case
- In most cases, s polynomials $\rightsquigarrow$ n polynomials is possible

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: $\exists?\ \bar{a} \in \bar{\mathbb{K}}^{n+1}, f_1(\bar{a}) = \cdots = f_s(\bar{a}) = 0$

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: $\exists?\ \bar{a} \in \bar{\mathbb{K}}^{n+1}, f_1(\bar{a}) = \cdots = f_s(\bar{a}) = 0$

- $\mathtt{H_2N}(\mathbb{K})$: 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: $\exists?\ \bar{a} \in \bar{\mathbb{K}}^{n+1}, f_1(\bar{a}) = \cdots = f_s(\bar{a}) = 0$

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

Upper bounds

Lemma

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

Upper bounds

Lemma

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

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

Upper bounds

Lemma

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

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

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

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

Corollary

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

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

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

Upper bounds

Lemma

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

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

Corollary

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

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

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

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
  - $X_i = \mathrm{True}$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

□

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 $X_1, \ldots, X_n$
- 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

□

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
  - $x_0 \cdot (x_i + x_0)$

□

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 $X_1, \ldots, X_n$
- 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
  - $x_0 \cdot (x_i + x_0)$
  - $x_0 \cdot (x_i + x_j)$
  - $(x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0)$

□

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

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

□

Summary so far

Upper bounds

	$\mathtt{HN}$	$\mathtt{H_2N}$	$\mathtt{H_2N}^{\square}$
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	???

- Over $\mathbb{Z}$, $\mathtt{HN} \in \mathsf{NP} \implies \mathsf{BPP} = \mathsf{NP}$

Outline

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

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

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

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

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 $\Longrightarrow$ $A(I)$ 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,

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

Reduction

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

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

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

Reduction

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

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

- $\forall j, f_j(\bar{x}) = 0 \iff \forall i, g_i(\bar{x}) = 0$
- α_{ij} algebraically independent: equivalence

Reduction

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

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

- $\forall j, f_j(\bar{x}) = 0 \iff \forall i, g_i(\bar{x}) = 0$
- α_{ij} algebraically independent: equivalence
- Random α_{ij}: equivalence 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

H_2N

- Complex variables x_0 and $x_1, \ldots, x_n$
- 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

H_2N

- Complex variables x_0 and $x_1, \ldots, x_n$
- 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

H_2N

- Complex variables x_0 and $x_1, \ldots, x_n$
- Polynomials $x_0^2 - x_i^2$ for every i $\rightarrow$ $f_1, \ldots, f_n$
  - $x_0 \cdot (x_i + x_0)$
  - $x_0 \cdot (x_i + x_j)$
  - $(x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0)$

  $\rightarrow$ $f_{n+1}, \ldots, f_s$

Reduction

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

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

New system

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

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

New system

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

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

New system

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

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

New system

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

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

New system

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

Reduction

- New variables: $y_1, \ldots, y_{s-n-1}$
- Polynomials $f_i(\bar{x}) = x_0^2 - x_i^2$ unchanged $(1 \leq i \leq n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + \lambda y_{i-n}^2$ $(n+1 \leq i \leq s)$

New system

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

Equivalence?

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

Equivalence?

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

- Either $\bar{a} = 0$ or $a_0 = 1$ and $a_i = \pm 1$

Equivalence?

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

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

Equivalence?

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

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

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

Equivalence?

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

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

- Either $\bar{a} = 0$ or $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$
- $\det = \pm\left(\epsilon_1 + \epsilon_2\lambda + \cdots + \epsilon_{s-n}\lambda^{s-n-1}\right)$

Equivalence?

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

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

- Either $\bar{a} = 0$ or $a_0 = 1$ and $a_i = \pm 1$
- $\epsilon_i = f_{n+i}(\bar{a})$
- $\det = \pm \left(\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_{s-n} \lambda^{s-n-1}\right)$
- Characteristic 0: $\lambda > 2$ is sufficient (unicity of base-λ representation)

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time
- $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^N}$

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time
- $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^N}$
- X is not root of any degree-$(< N)$ polynomial

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time
- $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^N}$
- X is not root of any degree-$(< N)$ polynomial
- Choose $\lambda = X$ in $\mathbb{F}_{p^N}$ is sufficient

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time
- $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^N}$
- X is not root of any degree-$(< N)$ polynomial
- Choose $\lambda = X$ in $\mathbb{F}_{p^N}$ is sufficient

$$\mathrm{H_2N}^{\square}(\mathbb{F}_{p^N}) \text{ is NP-hard}$$

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time
- $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^N}$
- X is not root of any degree-$(< N)$ polynomial
- Choose $\lambda = X$ in $\mathbb{F}_{p^N}$ is sufficient

$$\mathrm{H_2N}^{\square}(\mathbb{F}_{p^N}) \text{ is NP-hard}$$

- Coefficients in $\mathbb{F}_p$: P in the system + technical homogenization

Positive characteristic

- [Shoup, 1990] Find a irreducible degree-N polynomial P in $\mathbb{F}_p[X]$, in polynomial time
- $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^N}$
- X is not root of any degree-$(< N)$ polynomial
- Choose $\lambda = X$ in $\mathbb{F}_{p^N}$ is sufficient

$$\mathrm{H_2N}^{\square}(\mathbb{F}_{p^N}) \text{ is NP-hard}$$

- Coefficients in $\mathbb{F}_p$: P in the system + technical homogenization

$$\mathrm{H_2N}^{\square}(\mathbb{F}_p) \text{ is NP-hard}$$

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!