Hardness of the resultant

Bruno Grenet
with Pascal Koiran and Natacha Portier

Laboratoire de l'Informatique du Parallélisme, ÉNS Lyon

http://perso.ens-lyon.fr/bruno.grenet/

Visitors Seminar Series
Thematic Program on the Foundations of Computational Mathematics
Fields Institute, Toronto – September 30, 2009

Introduction

- Resultant: Has a system of polynomials a solution?

Introduction

- Resultant: Has a system of polynomials a solution?
- Here: n homogeneous polynomials in n variables

Introduction

- Resultant: Has a system of polynomials a solution?
- Here: n homogeneous polynomials in n variables
- Canny (1987): Resultant $\in$ PSPACE

Introduction

- Resultant: Has a system of polynomials a solution?
- Here: n homogeneous polynomials in n variables
- Canny (1987): Resultant $\in$ PSPACE
- What is the exact (boolean) complexity of this problem?

Outline

1. Statement of the problem and upper bound

2. Resultant is NP-hard
   - ... under randomized reduction
   - ... under deterministic reduction

Outline

Definitions

- Inputs:

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
- Questions:

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \dots, f_n \in \mathbb{C}[X_1, \dots, X_n]$, homogeneous;
- Questions:
  - Does there exist $(a_1, \dots, a_n) \in \mathbb{C}$ s.t. $f_i(\bar{a}) = 0$ for all i?

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
- Questions:
  - Does there exist $(a_1, \ldots, a_n) \in \mathbb{C}$ s.t. $f_i(\bar{a}) = 0$ for all i?
  - Homogeneous cases: $\bar{a} \neq (0, \ldots, 0)$

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
- Questions:
  - Does there exist $(a_1, \ldots, a_n) \in \mathbb{C}$ s.t. $f_i(\bar{a}) = 0$ for all i?
  - Homogeneous cases: $\bar{a} \neq (0, \ldots, 0)$
- Boolean versions $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
- Questions:
  - Does there exist $(a_1, \ldots, a_n) \in \mathbb{C}$ s.t. $f_i(\bar{a}) = 0$ for all i?
  - Homogeneous cases: $\bar{a} \neq (0, \ldots, 0)$
- Boolean versions $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:
  - Polynomials with integer coefficients

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$;
  - $\mathtt{H}_2\mathtt{N}_{\mathbb{C}}$: $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$, homogeneous;
  - $\mathtt{H}_2\mathtt{N}_{\mathbb{C}}^{\square}$: $f_1, \dots, f_n \in \mathbb{C}[X_1, \dots, X_n]$, homogeneous;
- Questions:
  - Does there exist $(a_1, \dots, a_n) \in \mathbb{C}$ s.t. $f_i(\bar{a}) = 0$ for all i?
  - Homogeneous cases: $\bar{a} \neq (0, \dots, 0)$
- Boolean versions $\mathtt{HN}$, $\mathtt{H}_2\mathtt{N}$, $\mathtt{H}_2\mathtt{N}^{\square}$:
  - Polynomials with integer coefficients
  - Complex roots?

Definitions

- Inputs:
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogeneous;
- Questions:
  - Does there exist $(a_1, \ldots, a_n) \in \mathbb{C}$ s.t. $f_i(\bar{a}) = 0$ for all i?
  - Homogeneous cases: $\bar{a} \neq (0, \ldots, 0)$
- Boolean versions $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:
  - Polynomials with integer coefficients
  - Complex roots?
- Resultant: $\mathtt{H_2N}^{\square}$

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathsf{AM}$.

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathit{H_2N}^{\square} \in \mathsf{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathsf{AM}$.

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathsf{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathsf{AM}$.
- $\mathcal{S}$: instance of $\mathtt{H_2N}^{\square}$ $(f_1, \dots, f_n \in \mathbb{Z}[X_1, \dots, X_n])$.

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathsf{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathsf{AM}$.
- $\mathcal{S}$: instance of $\mathtt{H_2N}^{\square}$ ($f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$).
- $\mathcal{T}$: instance of $\mathtt{HN}$ with

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathsf{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathsf{AM}$.
- $\mathcal{S}$: instance of $\mathtt{H_2N}^{\square}$ $(f_1, \dots, f_n \in \mathbb{Z}[X_1, \dots, X_n])$.
- $\mathcal{T}$: instance of $\mathtt{HN}$ with
  - new variables $Y_1, \dots, Y_n$

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathrm{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathrm{AM}$.
- $\mathcal{S}$: instance of $\mathtt{H_2N}^{\square}$ ($f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$).
- $\mathcal{T}$: instance of $\mathtt{HN}$ with
  - new variables $Y_1, \ldots, Y_n$
  - new equation $\sum_{i=1}^{n} X_i Y_i = 1$

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathsf{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathsf{AM}$.
- $\mathcal{S}$: instance of $\mathtt{H_2N}^{\square}$ $(f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n])$.
- $\mathcal{T}$: instance of $\mathtt{HN}$ with
  - new variables $Y_1, \ldots, Y_n$
  - new equation $\displaystyle\sum_{i=1}^{n} X_i Y_i = 1$
- $(a_1, \ldots, a_n) \in \mathcal{S}_{\text{true}} \implies (a_1, \ldots, a_n, 0, \ldots, 0, 1/a_{i_0}, 0, \ldots, 0) \in \mathcal{T}_{\text{true}}$

Upper bound

Theorem

Under Generalized Riemann Hypothesis, $\mathtt{H_2N}^{\square} \in \mathsf{AM}$.

- Koiran (1996): Under GRH, $\mathtt{HN} \in \mathsf{AM}$.
- $\mathcal{S}$: instance of $\mathtt{H_2N}^{\square}$ ($f_1, \dots, f_n \in \mathbb{Z}[X_1, \dots, X_n]$).
- $\mathcal{T}$: instance of $\mathtt{HN}$ with
  - new variables $Y_1, \dots, Y_n$
  - new equation $\sum_{i=1}^{n} X_i Y_i = 1$
- $(a_1, \dots, a_n) \in \mathcal{S}_{\text{true}} \implies (a_1, \dots, a_n, 0, \dots, 0, 1/a_{i_0}, 0, \dots, 0) \in \mathcal{T}_{\text{true}}$
- $(a_1, \dots, a_n, b_1, \dots, b_n) \in \mathcal{T}_{\text{true}} \implies \bar{a} \neq \bar{0} \implies \bar{a} \in \mathcal{S}_{\text{true}}$

Outline

Lower bound

Theorem

$H_2N^{\square}$ *is NP-hard.*

- $\texttt{3-SAT} \leqslant_m \texttt{Boolsys} \leqslant_m \mathtt{H_2N} \leqslant_? \mathtt{H_2N}^{\square}$

Lower bound

Theorem

$H_2N^{\square}$ is NP-hard under randomized reduction.

- $\texttt{3-SAT} \leqslant_m \texttt{Boolsys} \leqslant_m \mathtt{H_2N} \boxed{\leqslant_r} \mathtt{H_2N}^{\square}$
- Randomized reduction: less polynomials ("less rows")

Lower bound

Theorem

$H_2N^{\square}$ is NP-hard under deterministic reduction.

- $\mathtt{3\text{-}SAT} \leqslant_m \mathtt{Boolsys} \leqslant_m \mathtt{H_2N} \boxed{\leqslant_m} \mathtt{H_2N}^{\square}$
- Randomized reduction: less polynomials ("less rows")
- Deterministic reduction: more variables ("more columns")

Lower bound

Theorem

$H_2N^{\square}$ is NP-hard.

- $\texttt{3-SAT} \leqslant_m \texttt{Boolsys} \leqslant_m \texttt{H}_2\texttt{N} \leqslant_? \texttt{H}_2\texttt{N}^{\square}$
- Randomized reduction: less polynomials ("less rows")
- Deterministic reduction: more variables ("more columns")

$\texttt{Boolsys} \leqslant_m \texttt{H}_2\texttt{N}$

Boolsys

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

$\texttt{Boolsys} \leqslant_m \texttt{H}_2\texttt{N}$

$\texttt{Boolsys}$

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

$\texttt{H}_2\texttt{N}$

- Complex variables x_0 and $x_1, \dots, x_n$
- Equations

$\texttt{Boolsys} \leqslant_m \texttt{H}_2\texttt{N}$

$\texttt{Boolsys}$

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

$\texttt{H}_2\texttt{N}$

- Complex variables x_0 and $x_1, \ldots, x_n$
- Equations $x_0^2 = x_i^2$ for every $i > 0$ and

$\texttt{Boolsys} \leqslant_m \texttt{H}_2\texttt{N}$

$\texttt{Boolsys}$

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

$\texttt{H}_2\texttt{N}$

- Complex variables x_0 and $x_1, \ldots, x_n$
- Equations $x_0^2 = x_i^2$ for every $i > 0$ and
  - $(x_i + x_0)^2 = 0$

Boolsys $\leqslant_m$ $\mathrm{H_2N}$

Boolsys

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

$\mathrm{H_2N}$

- Complex variables x_0 and $x_1, \ldots, x_n$
- Equations $x_0^2 = x_i^2$ for every $i > 0$ and
  - $(x_i + x_0)^2 = 0$
  - $(x_i + x_j)^2 = 0$

$\mathtt{Boolsys} \leqslant_m \mathtt{H_2N}$

Boolsys

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

$\mathtt{H_2N}$

- Complex variables x_0 and $x_1, \dots, x_n$
- Equations $x_0^2 = x_i^2$ for every $i > 0$ and
  - $(x_i + x_0)^2 = 0$
  - $(x_i + x_j)^2 = 0$
  - $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$

$\mathtt{Boolsys} \leqslant_m \mathtt{H_2N}$

Boolsys

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

$\mathtt{H_2N}$

- Complex variables x_0 and $x_1, \dots, x_n$
- Equations $x_0^2 = x_i^2$ for every $i > 0$ and
  - $(x_i + x_0)^2 = 0$
  - $(x_i + x_j)^2 = 0$
  - $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$

Remains to prove $\mathtt{H_2N} \leqslant \mathtt{H_2N}^{\square}$.

Outline

1. Statement of the problem and upper bound

2. Resultant is NP-hard
   - . . . under randomized reduction
   - . . . under deterministic reduction

General idea

- Decrease the number of polynomials

General idea

- Decrease the number of polynomials
- If $f_1, \ldots, f_s$ homogeneous of degree 2,

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

General idea

- Decrease the number of polynomials
- If $f_1, \ldots, f_s$ homogeneous of degree 2,

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

$$\forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \implies \bigwedge_i g_i(\bar{x}) = 0 \right)$$

General idea

- Decrease the number of polynomials
- If $f_1, \ldots, f_s$ homogeneous of degree 2,

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

- If α_{ij} algebraically independent (over $\mathbb{Q}$), then

$$\forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \iff \bigwedge_i g_i(\bar{x}) = 0 \right)$$

General idea

- Decrease the number of polynomials
- If $f_1, \ldots, f_s$ homogeneous of degree 2,

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

- If α_{ij} algebraically independent (over $\mathbb{Q}$), then

$$\forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \impliedby \bigwedge_i g_i(\bar{x}) = 0 \right)$$

- Replace α_{ij} by random integers, and use Schwartz-Lippel Lemma to conclude

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i g_i(\bar{x}) = 0 \right)$$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

$$\Phi(\bar{\alpha}) \iff \bigvee_k \left(\bigwedge_l P_{kl}(\bar{\alpha}) = 0 \wedge \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0 \right)$$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

$$\Phi(\bar{\alpha}) \iff \bigvee_k \left(\bigwedge_l P_{kl}(\bar{\alpha}) = 0 \wedge \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0 \right)$$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

$$\Phi(\bar{\alpha}) \quad \Longleftarrow \qquad\qquad \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0$$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

$$\Phi(\bar{\alpha}) \quad \Longleftarrow \qquad \prod_m Q_{km}(\bar{\alpha}) \neq 0$$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

$$\Phi(\bar{\alpha}) \quad \Longleftarrow \qquad\qquad \prod_m Q_{km}(\bar{\alpha}) \neq 0$$

- [FGM90] Simply exponential bound on the degree of $\prod_m Q_{km}$

Random integers are sufficient

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Quantifier Elimination in $\Phi(\bar{\alpha})$:

$$\Phi(\bar{\alpha}) \quad \Longleftarrow \qquad\qquad \prod_m Q_{km}(\bar{\alpha}) \neq 0$$

- [FGM90] Simply exponential bound on the degree of $\prod_m Q_{km}$
- Schwartz-Zippel Lemma: Random α_{ij} of polynomial length work

Summary of the randomized reduction

- Instance of $\mathtt{H_2N}$: more polynomials than variables, *i.e.* too many polynomials

Summary of the randomized reduction

- Instance of $\mathtt{H_2N}$: more polynomials than variables, *i.e.* too many polynomials
- New system: linear combinations of the polynomials

Summary of the randomized reduction

- Instance of $\mathtt{H_2N}$: more polynomials than variables, *i.e.* too many polynomials
- New system: linear combinations of the polynomials
- If combinations with algebraically independent coefficients, then equivalence

Summary of the randomized reduction

- Instance of $\mathtt{H_2N}$: more polynomials than variables, *i.e.* too many polynomials
- New system: linear combinations of the polynomials
- If combinations with algebraically independent coefficients, then equivalence
- Algebraically independent coefficients can be replaced by random integers

Outline

1. Statement of the problem and upper bound
2. Resultant is NP-hard
   - . . . under randomized reduction
   - . . . under deterministic reduction

Introduction

- Instead of decreasing the number of polynomials, new variables are added

Introduction

- Instead of decreasing the number of polynomials, new variables are added
- Careful look to the equations is needed

Introduction

- Instead of decreasing the number of polynomials, new variables are added
- Careful look to the equations is needed
- Key point: translation in terms of the rank of the Jacobian matrix

Introduction

- Instead of decreasing the number of polynomials, new variables are added
- Careful look to the equations is needed
- Key point: translation in terms of the rank of the Jacobian matrix

H_2N

- Complex variables x_0 and $x_1, \dots, x_n$
- Equations $x_0^2 - x_i^2 = 0$ for every i
  - $(x_i + x_0)^2 = 0$
  - $(x_i + x_j)^2 = 0$
  - $(x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0) = 0$

Introduction

- Instead of decreasing the number of polynomials, new variables are added
- Careful look to the equations is needed
- Key point: translation in terms of the rank of the Jacobian matrix

$\mathtt{H_2N}$

- Complex variables x_0 and $x_1, \ldots, x_n$
- Equations $x_0^2 - x_i^2 = 0$ for every i $\longrightarrow f_1, \ldots, f_n$

$$\left.\begin{array}{l} \blacktriangleright\ (x_i + x_0)^2 = 0 \\ \blacktriangleright\ (x_i + x_j)^2 = 0 \\ \blacktriangleright\ (x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0) = 0 \end{array}\right\} \longrightarrow f_{n+1}, \ldots, f_s$$

Reduction

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

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ \\ \\ \\ \\ \end{cases}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ f_{n+1}(\bar{x}) + 13y_1^2 = 0 \\ \\ \\ \\ \\ \end{cases}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ f_{n+1}(\bar{x}) + 13y_1^2 = 0 \\ f_{n+2}(\bar{x}) - y_1^2 + 13y_2^2 = 0 \end{cases}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ f_{n+1}(\bar{x}) + 13y_1^2 = 0 \\ f_{n+2}(\bar{x}) - y_1^2 + 13y_2^2 = 0 \\ f_{n+3}(\bar{x}) - y_2^2 + 13y_3^2 = 0 \\ \\ \\ \\ \end{cases}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ f_{n+1}(\bar{x}) + 13y_1^2 = 0 \\ f_{n+2}(\bar{x}) - y_1^2 + 13y_2^2 = 0 \\ f_{n+3}(\bar{x}) - y_2^2 + 13y_3^2 = 0 \\ \qquad\qquad\vdots \\ f_{s-1}(\bar{x}) - y_{s-n-2}^2 + 13y_{s-n-1}^2 = 0 \end{cases}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ f_{n+1}(\bar{x}) + 13y_1^2 = 0 \\ f_{n+2}(\bar{x}) - y_1^2 + 13y_2^2 = 0 \\ f_{n+3}(\bar{x}) - y_2^2 + 13y_3^2 = 0 \\ \qquad\qquad\vdots \\ f_{s-1}(\bar{x}) - y_{s-n-2}^2 + 13y_{s-n-1}^2 = 0 \\ f_s(\bar{x}) - y_{s-n-1}^2 = 0 \end{cases}$$

Reduction

- New variables: $y_1, \dots, y_{s-n-1}$
- Equations $f_i(\bar{x}) = x_0^2 - x_i^2 = 0$ unchanged $(1 \leqslant i \leqslant n)$
- $f_i(\bar{x}) \rightsquigarrow f_i(\bar{x}) - y_{i-n-1}^2 + 13y_{i-n}^2$ $(n+1 \leqslant i \leqslant s)$

New system

$$\mathcal{S}_G = \begin{cases} f_1(\bar{x}) = 0 \\ \quad\vdots \\ f_n(\bar{x}) = 0 \\ f_{n+1}(\bar{x}) + 13y_1^2 = 0 \\ f_{n+2}(\bar{x}) - y_1^2 + 13y_2^2 = 0 \\ f_{n+3}(\bar{x}) - y_2^2 + 13y_3^2 = 0 \\ \qquad\qquad\vdots \\ f_{s-1}(\bar{x}) - y_{s-n-2}^2 + 13y_{s-n-1}^2 = 0 \\ f_s(\bar{x}) - y_{s-n-1}^2 = 0 \end{cases} \quad \rightsquigarrow \quad \begin{array}{c} \bar{a} \text{ solution of } \mathcal{S}_F \\ \Downarrow \\ (\bar{a}, \bar{0}) \text{ solution of } \mathcal{S}_G \end{array}$$

Translation in terms of Jacobian matrices

Jacobian matrix

Let $F:\mathbb{C}^{n+1}\to\mathbb{C}^s$ s.t. $F(\bar{x})=(f_1(\bar{x}),\ldots,f_s(\bar{x}))^t$. Then J_F is defined by

$$(J_F)_{ij}=\frac{\partial f_i}{\partial x_j}.$$

Translation in terms of Jacobian matrices

Jacobian matrix

Let $F : \mathbb{C}^{n+1} \to \mathbb{C}^s$ s.t. $F(\bar{x}) = (f_1(\bar{x}), \ldots, f_s(\bar{x}))^t$. Then J_F is defined by

$$(J_F)_{ij} = \frac{\partial f_i}{\partial x_j}.$$

Lemma

Let $\mathcal{S}_F$ be a homogeneous polynomial system of s equations in $n+1$ variables. If $\bar{a}$ is a non trivial solution of $\mathcal{S}_F$, then $J_F(\bar{a})$ has rank at most n.

Translation in terms of Jacobian matrices

Jacobian matrix

Let $F : \mathbb{C}^{n+1} \to \mathbb{C}^s$ s.t. $F(\bar{x}) = (f_1(\bar{x}), \dots, f_s(\bar{x}))^t$. Then J_F is defined by

$$(J_F)_{ij} = \frac{\partial f_i}{\partial x_j}.$$

Lemma

Let $\mathcal{S}_F$ be a homogeneous polynomial system of s equations in $n+1$ variables. If $\bar{a}$ is a non trivial solution of $\mathcal{S}_F$, then $J_F(\bar{a})$ has rank at most n.

Proof. $\mathcal{S}_F$ is homogeneous $\implies$ if $\mathcal{S}_F$ has a non trivial solution, then there is a line of solutions. $\square$

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Lemma

Let $\bar{a}$ be a $(n+1)$-tuple such that $a_0^2 = \cdots = a_n^2 \neq 0$.

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Lemma

Let $\bar{a}$ be a $(n+1)$-tuple such that $a_0^2 = \cdots = a_n^2 \neq 0$. Then for our system

(i) *$\bar{a}$ is solution $\implies$ $rk(J_F(\bar{a})) = n$;*

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Lemma

Let $\bar{a}$ be a $(n+1)$-tuple such that $a_0^2 = \cdots = a_n^2 \neq 0$. Then for our system

(i) *$\bar{a}$ is solution $\implies rk(J_F(\bar{a})) = n$;*

(ii) *$\bar{a}$ is not solution $\implies rk(J_F(\bar{a})) = n + 1$.*

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Lemma

Let $\bar{a}$ be a $(n+1)$-tuple such that $a_0^2 = \cdots = a_n^2 \neq 0$. Then for our system

(i) *$\bar{a}$ is solution $\implies rk(J_F(\bar{a})) = n$;*

(ii) *$\bar{a}$ is not solution $\implies rk(J_F(\bar{a})) = n + 1$.*

Proof.

- The first n rows are *almost* diagonal.

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Lemma

Let $\bar{a}$ be a $(n+1)$-tuple such that $a_0^2 = \cdots = a_n^2 \neq 0$. Then for our system

(i) *$\bar{a}$ is solution $\implies$ $rk(J_F(\bar{a})) = n$;*

(ii) *$\bar{a}$ is not solution $\implies$ $rk(J_F(\bar{a})) = n + 1$.*

Proof.

- The first n rows are *almost* diagonal.
- Exhaustive study of the Jacobian matrix: each equation is satisfied by $\bar{a}$ iff the corresponding row is linearly dependent from the first n ones.

Particular case of our system

Our system $\mathcal{S}_F$: $x_0^2 = x_i^2$, $(x_i + x_0)^2 = 0$, $(x_i + x_j)^2 = 0$ and $(x_i + x_0)^2 = (x_j + x_0) \cdot (x_k + x_0)$.

Lemma

Let $\bar{a}$ be a $(n+1)$-tuple such that $a_0^2 = \cdots = a_n^2 \neq 0$. Then for our system

(i) *$\bar{a}$ is solution $\implies$ $rk(J_F(\bar{a})) = n$;*

(ii) *$\bar{a}$ is not solution $\implies$ $rk(J_F(\bar{a})) = n + 1$.*

Proof.

- The first n rows are *almost* diagonal.
- Exhaustive study of the Jacobian matrix: each equation is satisfied by $\bar{a}$ iff the corresponding row is linearly dependent from the first n ones. $\rightsquigarrow$ Why is this true?

$\square$

Equivalence of the old and new systems

$$\mathcal{S}_F \text{ infeasible} \implies \text{rk } J_F(\bar{a})) = n+1 \overset{?}{\implies} \text{rk } J_G(\bar{a},\bar{b})) = s \implies \mathcal{S}_G \text{ infeasible}$$

Equivalence of the old and new systems

$\mathcal{S}_F$ infeasible $\Longrightarrow$ rk $J_F(\bar{a})) = n+1 \overset{?}{\Longrightarrow}$ rk $J_G(\bar{a},\bar{b})) = s \Longrightarrow \mathcal{S}_G$ infeasible

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2}J_G(\bar{a},\bar{b})\right) = \det\left(\begin{array}{ccc|ccc} 1 & \pm 1 & & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots & & \vdots \\ 1 & & \pm 1 & 0 & \cdots & 0 \\ \hline & & & 13b_1 & & \\ & \|\cdot\|_1 \leqslant 12 & & -b_1 & \ddots & \\ & & & & \ddots & 13b_{s-n-1} \\ & & & & & -b_{s-n-1} \end{array}\right)$$

Equivalence of the old and new systems

$\mathcal{S}_F$ infeasible $\implies$ rk $J_F(\bar{a})) = n+1 \overset{?}{\implies}$ rk $J_G(\bar{a},\bar{b})) = s \implies \mathcal{S}_G$ infeasible

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2}J_G(\bar{a},\bar{b})\right) = \det\left(\begin{array}{ccc|ccc}
1 & \pm 1 & & 0 & \cdots & 0 \\
\vdots & & \ddots & \vdots & & \vdots \\
1 & & \pm 1 & 0 & \cdots & 0 \\
\hline
 & & & 13b_1 & & \\
\|\cdot\|_1 & \leqslant & 12 & -b_1 & \ddots & \\
 & & & & \ddots & 13b_{s-n-1} \\
 & & & & & -b_{s-n-1}
\end{array}\right)$$

Equivalence of the old and new systems

$$\mathcal{S}_F \text{ infeasible} \implies \text{rk } J_F(\bar{a})) = n+1 \overset{?}{\implies} \text{rk } J_G(\bar{a},\bar{b})) = s \implies \mathcal{S}_G \text{ infeasible}$$

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2}J_G(\bar{a},\bar{b})\right) = \det\left(\begin{array}{cccc|ccc} 1 & \pm 1 & & & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 1 & & & \pm 1 & 0 & \cdots & 0 \\ \hline & & & & 13 & & \\ & \|\cdot\|_1 & \leqslant & 12 & -1 & \ddots & \\ & & & & & \ddots & 13 \\ & & & & & & -1 \end{array}\right)$$

Equivalence of the old and new systems

$$\mathcal{S}_F \text{ infeasible} \implies \text{rk } J_F(\bar{a})) = n+1 \overset{?}{\implies} \text{rk } J_G(\bar{a}, \bar{b})) = s \implies \mathcal{S}_G \text{ infeasible}$$

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2} J_G(\bar{a}, \bar{b})\right) = \det \left(\begin{array}{ccc|ccc} 1 & \pm 1 & & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots & & \vdots \\ 1 & & \pm 1 & 0 & \cdots & 0 \\ \hline & & & 13 & & \\ \|\cdot\|_1 & \leqslant & 12 & -1 & \ddots & \\ & & & & \ddots & 13 \\ & & & & & -1 \end{array}\right)$$

Equivalence of the old and new systems

$\mathcal{S}_F$ infeasible $\implies$ rk $J_F(\bar{a})) = n+1 \overset{?}{\implies}$ rk $J_G(\bar{a},\bar{b})) = s \implies \mathcal{S}_G$ infeasible

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2}J_G(\bar{a},\bar{b})\right) = \det\left(\begin{array}{cccc|ccc} 0 & \pm 1 & & & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & & & \pm 1 & 0 & \cdots & 0 \\ \hline * & & & & 13 & & \\ \vdots & |*| & \leqslant & 12 & -1 & \ddots & \\ \vdots & & & & & \ddots & 13 \\ * & & & & & & -1 \end{array}\right)$$

Equivalence of the old and new systems

$\mathcal{S}_F$ infeasible $\implies$ rk $J_F(\bar{a})) = n+1 \overset{?}{\implies}$ rk $J_G(\bar{a},\bar{b})) = s \implies \mathcal{S}_G$ infeasible

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2}J_G(\bar{a},\bar{b})\right) = \pm\det\begin{pmatrix} c_1 & 13 & & \\ \vdots & -1 & \ddots & \\ \vdots & & \ddots & 13 \\ c_{s-n} & & & -1 \end{pmatrix}$$

where $|c_i| \leqslant 12$. NB: $(c_1,\ldots,c_n) = \bar{0} \iff$ rk $J_F(\bar{a})) = n$.

Equivalence of the old and new systems

$\mathcal{S}_F$ infeasible $\implies$ rk $J_F(\bar{a})) = n+1 \overset{?}{\implies}$ rk $J_G(\bar{a},\bar{b})) = s \implies \mathcal{S}_G$ infeasible

Let $a_0 = 1$. Then for every i, $a_i = \pm 1$.

$$\det\left(\frac{1}{2}J_G(\bar{a},\bar{b})\right) = \pm\det\begin{pmatrix} c_1 & 13 & & \\ \vdots & -1 & \ddots & \\ \vdots & & \ddots & 13 \\ c_{s-n} & & & -1 \end{pmatrix}$$

where $|c_i| \leqslant 12$. NB: $(c_1,\ldots,c_n) = \bar{0} \iff$ rk $J_F(\bar{a})) = n$.
The determinant is non zero, *via* the unicity of base-13 representation.

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.
- If $\bar{a}$ is solution of $\mathcal{S}_F$, then $(\bar{a}, \bar{0})$ is solution of $\mathcal{S}_G$.

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.
- If $\bar{a}$ is solution of $\mathcal{S}_F$, then $(\bar{a}, \bar{0})$ is solution of $\mathcal{S}_G$.
- If $\mathcal{S}_F$ has no solution, let $(\bar{a}, \bar{b}) \neq \bar{0}$:

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.
- If $\bar{a}$ is solution of $\mathcal{S}_F$, then $(\bar{a}, \bar{0})$ is solution of $\mathcal{S}_G$.
- If $\mathcal{S}_F$ has no solution, let $(\bar{a}, \bar{b}) \neq \bar{0}$:
  - The Jacobian matrix $J_F(\bar{a})$ has maximal rank (as soon as $\bar{a} \neq \bar{0}$).

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.
- If $\bar{a}$ is solution of $\mathcal{S}_F$, then $(\bar{a}, \bar{0})$ is solution of $\mathcal{S}_G$.
- If $\mathcal{S}_F$ has no solution, let $(\bar{a}, \bar{b}) \neq \bar{0}$:
  - The Jacobian matrix $J_F(\bar{a})$ has maximal rank (as soon as $\bar{a} \neq \bar{0}$).
  - Then $J_G(\bar{a}, \bar{b})$ has maximal rank (with a slight modification if some b_i vanishes).

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.
- If $\bar{a}$ is solution of $\mathcal{S}_F$, then $(\bar{a}, \bar{0})$ is solution of $\mathcal{S}_G$.
- If $\mathcal{S}_F$ has no solution, let $(\bar{a}, \bar{b}) \neq \bar{0}$:
  - The Jacobian matrix $J_F(\bar{a})$ has maximal rank (as soon as $\bar{a} \neq \bar{0}$).
  - Then $J_G(\bar{a}, \bar{b})$ has maximal rank (with a slight modification if some b_i vanishes).
  - So $\mathcal{S}_G$ cannot have non trivial solution.

Summary of the deterministic reduction

- New variables are added, and last equations are modified $\rightsquigarrow \mathcal{S}_G$.
- If $\bar{a}$ is solution of $\mathcal{S}_F$, then $(\bar{a}, \bar{0})$ is solution of $\mathcal{S}_G$.
- If $\mathcal{S}_F$ has no solution, let $(\bar{a}, \bar{b}) \neq \bar{0}$:
  - The Jacobian matrix $J_F(\bar{a})$ has maximal rank (as soon as $\bar{a} \neq \bar{0}$).
  - Then $J_G(\bar{a}, \bar{b})$ has maximal rank (with a slight modification if some b_i vanishes).
  - So $\mathcal{S}_G$ cannot have non trivial solution.

$\mathtt{H_2N}^{\square}$ is NP-hard.

Conclusion

- 🙂 Answer to Canny's question.

Conclusion

- Answer to Canny's question.
- Upper (AM) and lower (NP) bounds are "almost equal".

Conclusion

- ☺ Answer to Canny's question.
- ☺ Upper (AM) and lower (NP) bounds are "almost equal".
- ☹ Why does it work?

Conclusion

- 🙂 Answer to Canny's question.
- 🙂 Upper (AM) and lower (NP) bounds are "almost equal".
- ☹ Why does it work?
- ☹ The method seems unable to prove results in algebraic complexity.

Conclusion

- 🙂 Answer to Canny's question.
- 🙂 Upper (AM) and lower (NP) bounds are "almost equal".
- ☹ Why does it work?
- ☹ The method seems unable to prove results in algebraic complexity.

Thank you!