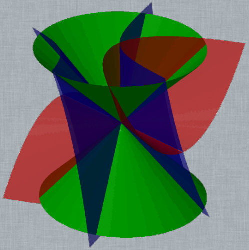
Complexity of the resultant

Bruno Grenet

joint work with Pascal Koiran & Natacha Portier

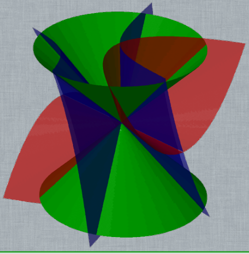
LIX – École Polytechnique

Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

Is there a (nonzero) solution?



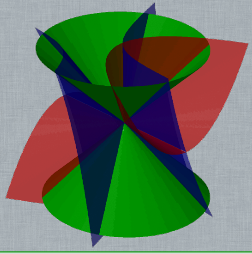
$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

PolSys$(\mathbb{K})$

Input: $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$

Question: Is there $\boldsymbol{a} \in \overline{\mathbb{K}}^n$ s.t. $f(\boldsymbol{a}) = 0$?

Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

PolSys($\mathbb{K}$)

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

Question: Is there $\mathbf{a} \in \overline{\mathbb{K}}^n$ s.t. $f(\mathbf{a}) = 0$?

HomPolSys($\mathbb{K}$)

Input: $f_1, \ldots, f_s \in \mathbb{K}[X_0, \ldots, X_n]$, **homogeneous**

Question: Is there a **nonzero** $\mathbf{a} \in \overline{\mathbb{K}}^{n+1}$ s.t. $f(\mathbf{a}) = 0$?

Glimpse of Elimination Theory

$$f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n], \qquad f_i = \sum_{|\alpha|_1 \leqslant d_i} \gamma_{i,\alpha} \mathbf{X}^\alpha$$

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

Glimpse of Elimination Theory

$$f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n], \qquad f_i = \sum_{|\alpha|_1 \leqslant d_i} \gamma_{i,\alpha} \mathbf{X}^\alpha$$

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

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

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

Two Univariate Polynomials

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

Two Univariate Polynomials

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

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

Two Univariate Polynomials

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

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

$\rightsquigarrow$ 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
- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial

More generally

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \dots, f_{n+1} \in \mathbb{K}[X_0, \dots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial
  - Sylvester Matrix $\rightsquigarrow$ Macaulay Matrix (exponential size)

More generally

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \dots, f_{n+1} \in \mathbb{K}[X_0, \dots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial
  - Sylvester Matrix $\rightsquigarrow$ Macaulay Matrix (exponential size)
- s polynomials $\neq n + 1$ variables $\rightsquigarrow$ several polynomials needed

More generally

- Wlog, homogeneous polynomials, non trivial roots
- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial
  - Sylvester Matrix $\rightsquigarrow$ Macaulay Matrix (exponential size)
- s polynomials $\neq n+1$ variables $\rightsquigarrow$ several polynomials needed

Resultant($\mathbb{K}$)

Input: $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$, homogeneous

Question: Is there a nonzero $\mathbf{a} \in \overline{\mathbb{K}}^{n+1}$ s.t. $f(\mathbf{a}) = 0$?

Macaulay matrices

- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$, homogeneous, of degrees $d_1, \ldots, d_n$
- $D = \sum_i (d_i - 1)$, $\mathcal{M}_D^n = \{X_0^{\alpha_0} \cdots X_n^{\alpha_n} : \alpha_0 + \ldots + \alpha_n = D\}$

Macaulay matrices

- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$, homogeneous, of degrees $d_1, \ldots, d_n$
- $D = \sum_i (d_i - 1)$, $\mathcal{M}_D^n = \{X_0^{\alpha_0} \cdots X_n^{\alpha_n} : \alpha_0 + \ldots + \alpha_n = D\}$

Definition

The first Macaulay matrix is defined as follows:

- Its rows and columns are indexed by $\mathcal{M}_D^n$;
- The row indexed by $\boldsymbol{X^\alpha}$ represents

$$\frac{\boldsymbol{X^\alpha}}{X_i^{d_i}} f_i, \text{ where } i = \min\{j : d_j \leqslant \alpha_j\}.$$

Other Macaulay matrices are defined by reordering the f_i's.

Macaulay matrices

- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$, homogeneous, of degrees $d_1, \ldots, d_n$
- $D = \sum_i (d_i - 1)$, $\mathcal{M}_D^n = \{X_0^{\alpha_0} \cdots X_n^{\alpha_n} : \alpha_0 + \ldots + \alpha_n = D\}$

Definition

The first Macaulay matrix is defined as follows:

- Its rows and columns are indexed by $\mathcal{M}_D^n$;
- The row indexed by $\mathbf{X}^{\boldsymbol{\alpha}}$ represents

$$\frac{\mathbf{X}^{\boldsymbol{\alpha}}}{X_i^{d_i}} f_i, \text{ where } i = \min\{j : d_j \leqslant \alpha_j\}.$$

Other Macaulay matrices are defined by reordering the f_i's.

- Resultant : GCD of the determinants of n Macaulay matrices

Canny's upper bound

Theorem [Canny'87]

The resultant is computable in polynomial space.

Canny's upper bound

Theorem [Canny'87]

The resultant is computable in polynomial space.

Proof idea.

- The resultant can be expressed as $\det(M)/\det(N)$, where M is Macaulay, and N a submatrix of M;
- An entry of M (resp. N) can be computed in polynomial time;
- The determinant can be computed in logarithmic space.

Large determinants

Theorem [G.-Koiran-Portier'10-13]

- Macaulay matrices can be represented by polynomial-size boolean circuits.
- Deciding the nullity of the determinant of a matrix represented by a boolean circuit is PSPACE-complete (over any field).

Large determinants

Theorem [G.-Koiran-Portier'10-13]

- Macaulay matrices can be represented by polynomial-size boolean circuits.
- Deciding the nullity of the determinant of a matrix represented by a boolean circuit is PSPACE-complete (over any field).

Proof idea.

- Let $\mathcal{M}$ be a PSPACE Turing Machine;
- Let $\mathcal{G}_{\mathcal{M}}^{x}$ its *graph of configurations*:
  - initial configuration c_i,
  - accepting configuration c_a;
- $\mathcal{G}_{\mathcal{M}}^{x}$ can be represented by a boolean circuit;
- There exists a path $c_i \rightsquigarrow c_a$ in $\mathcal{G}_{\mathcal{M}}^{x}$ iff $x \in \mathcal{L}(\mathcal{M})$;
- Let $A \simeq$ adjacency matrix of $\mathcal{G}_{\mathcal{M}}^{x}$:

$$\det(A) \neq 0 \iff \exists c_i \rightsquigarrow c_a.$$

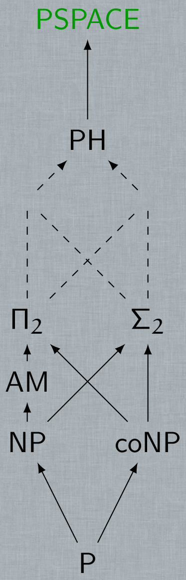
The resultant in Valiant's model of computation

Theorem

In Valiant's algebraic model of computation:

- The resultant belongs to VPSPACE, [Koiran-Perifel'07]
- Determinants of *succinctly represented* matrices is VPSPACE-complete. [Malod'11]

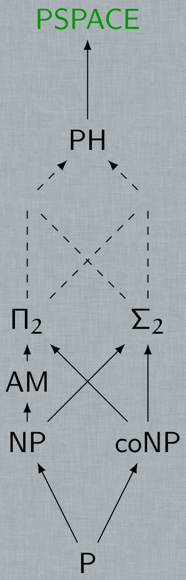
Upper bounds for polynomial systems



Upper bounds

- $\textsc{PolSys}(\mathbb{F}_p) \in \mathsf{PSPACE}$

Upper bounds for polynomial systems



Upper bounds

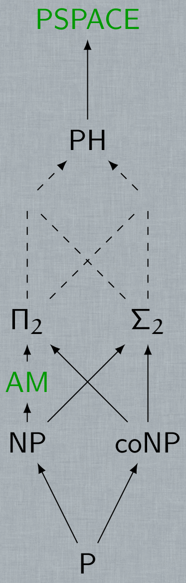
- $\textsc{PolSys}(\mathbb{F}_p) \in \mathsf{PSPACE}$

  $\implies \textsc{HomPolSys}(\mathbb{F}_p), \textsc{Resultant}(\mathbb{F}_p) \in \mathsf{PSPACE}$

Proof. Remove the unwanted zero root:

- New variables $Y_0, \ldots, Y_n$
- New polynomial $\sum_i X_i Y_i - 1$ to the system. $\square$

Upper bounds for polynomial systems

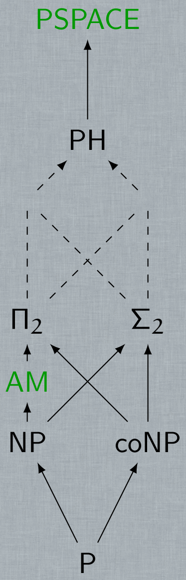


Upper bounds

- PolSys($\mathbb{F}_p$) $\in$ PSPACE

  $\implies$ HomPolSys($\mathbb{F}_p$), Resultant($\mathbb{F}_p$) $\in$ PSPACE
- Under GRH, PolSys($\mathbb{Z}$) $\in$ AM [Koiran'96]

Upper bounds for polynomial systems



Upper bounds

- $\textsc{PolSys}(\mathbb{F}_p) \in \mathsf{PSPACE}$

  $\implies \textsc{HomPolSys}(\mathbb{F}_p), \textsc{Resultant}(\mathbb{F}_p) \in \mathsf{PSPACE}$
- Under GRH, $\textsc{PolSys}(\mathbb{Z}) \in \mathsf{AM}$ [Koiran'96]

  $\implies \textsc{HomPolSys}(\mathbb{Z}), \textsc{Resultant}(\mathbb{Z}) \in \mathsf{AM}$

Proof sketch of Koiran's result

- Let $f = (f_1, \dots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \dots, X_n]$;
- Let $\mathcal{P}(x)$ be the set of prime numbers $\leqslant x$;
- Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leqslant x$, s.t. f has a root mod p.

Proof sketch of Koiran's result

- Let $f = (f_1, \dots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \dots, X_n]$;
- Let $\mathcal{P}(x)$ be the set of prime numbers $\leqslant x$;
- Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leqslant x$, s.t. f has a root mod p.

Theorem [Koiran'96]

There exist polynomial-time computable A and x_0 s.t.

- If f has no root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \leqslant A$;
- If f has a root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \geqslant 8A(\log A + 3)$.

Proof sketch of Koiran's result

- Let $f = (f_1, \dots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \dots, X_n]$;
- Let $\mathcal{P}(x)$ be the set of prime numbers $\leqslant x$;
- Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leqslant x$, s.t. f has a root mod p.

Theorem [Koiran'96]

There exist polynomial-time computable A and x_0 s.t.

- If f has no root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \leqslant A$;
- If f has a root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \geqslant 8A(\log A + 3)$.

Algorithm.

1. Compute A, x_0;
2. Take a random hash function $h : \mathcal{P}(x_0) \to \{0,1\}^{2+\lceil \log A \rceil}$;
3. Check whether there exist $x, y \in \mathcal{P}_f(x_0)$ s.t. $h(x) = h(y)$;

Proof sketch of Koiran's result

- Let $f = (f_1, \dots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \dots, X_n]$;
- Let $\mathcal{P}(x)$ be the set of prime numbers $\leqslant x$;
- Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leqslant x$, s.t. f has a root mod p.

Theorem [Koiran'96]

There exist polynomial-time computable A and x_0 s.t.

- If f has no root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \leqslant A$;
- If f has a root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \geqslant 8A(\log A + 3)$.

Algorithm.

1. Compute A, x_0;
2. Take a random hash function $h : \mathcal{P}(x_0) \to \{0,1\}^{2+\lceil \log A \rceil}$;
3. Check whether there exist $x, y \in \mathcal{P}_f(x_0)$ s.t. $h(x) = h(y)$; $\leftarrow$ NP

Proof sketch of Koiran's result

- Let $f = (f_1, \dots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \dots, X_n]$;
- Let $\mathcal{P}(x)$ be the set of prime numbers $\leqslant x$;
- Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leqslant x$, s.t. f has a root mod p.

Theorem [Koiran'96]

There exist polynomial-time computable A and x_0 s.t.

- If f has no root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \leqslant A$;
- If f has a root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \geqslant 8A(\log A + 3)$.

Algorithm.

1. Compute A, x_0;
2. Take a random hash function $h : \mathcal{P}(x_0) \to \{0,1\}^{2+\lceil \log A \rceil}$;
3. Check whether there exist $x, y \in \mathcal{P}_f(x_0)$ s.t. $h(x) = h(y)$; $\leftarrow$ NP
   - proba. 1 if f has a root in $\mathbb{C}$;
   - proba. $\leqslant 1/4$ if f has no root in $\mathbb{C}$.

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition [Folklore]

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are **NP-hard**.

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition **[Folklore]**

For $p = 0$ or prime, $\textsc{PolSys}(\mathbb{F}_p)$ & $\textsc{HomPolSys}(\mathbb{F}_p)$ are **NP-hard**.

Proof. Case $\textsc{HomPolSys}(\mathbb{F}_p)$, with $p \neq 2$:

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition [Folklore]

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proof. Case HomPolSys($\mathbb{F}_p$), with $p \neq 2$:

Boolsys

- Boolean variables $u_1, \ldots, u_n$
- Equations
  - $u_i = \text{True}$
  - $u_i = \neg u_j$
  - $u_i = u_j \vee u_k$

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition [Folklore]

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proof. Case HomPolSys($\mathbb{F}_p$), with $p \neq 2$:

Boolsys

- Boolean variables $u_1, \ldots, u_n$
- Equations
  - $u_i = \text{True}$
  - $u_i = \neg u_j$
  - $u_i = u_j \vee u_k$

HomPolSys

- Variables (over $\mathbb{F}_p$) X_0 and $X_1, \ldots, X_n$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition [Folklore]

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are **NP-hard**.

Proof. Case HomPolSys($\mathbb{F}_p$), with $p \neq 2$:

BoolSys

- Boolean variables $u_1, \dots, u_n$
- Equations
  - $u_i = \text{True}$
  - $u_i = \neg u_j$
  - $u_i = u_j \vee u_k$

HomPolSys

- Variables (over $\mathbb{F}_p$) 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 for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition [Folklore]

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proof. Case HomPolSys($\mathbb{F}_p$), with $p \neq 2$:

BoolSys

- Boolean variables $u_1, \dots, u_n$
- Equations
  - $u_i = \text{True}$
  - $u_i = \neg u_j$
  - $u_i = u_j \vee u_k$

HomPolSys

- Variables (over $\mathbb{F}_p$) X_0 and $X_1, \dots, X_n$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$

Lower bounds for non-square systems

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition [Folklore]

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are **NP-hard**.

Proof. Case HomPolSys($\mathbb{F}_p$), with $p \neq 2$:

BoolSys

- Boolean variables $u_1, \ldots, u_n$
- Equations
  - $u_i = \text{True}$
  - $u_i = \neg u_j$
  - $u_i = u_j \vee u_k$

HomPolSys

- Variables (over $\mathbb{F}_p$) 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 for the resultant in char. 0

Proposition [Heintz-Morgenstern'93]

Resultant($\mathbb{Z}$) is NP-hard.

Lower bound for the resultant in char. 0

Proposition [Heintz-Morgenstern'93]

RESULTANT($\mathbb{Z}$) 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 for the resultant in char. 0

Proposition [Heintz-Morgenstern'93]

Resultant$(\mathbb{Z})$ is **NP-hard**.

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

$$\rightsquigarrow \begin{cases} X_1^2 - X_0^2 & = & 0 \\ & \vdots & \\ X_n^2 - X_0^2 & = & 0 \\ u_1 X_1 + \cdots + u_n X_n & = & 0 \end{cases}$$

$\square$

Lower bound for the resultant in char. 0

Proposition [Heintz-Morgenstern'93]

$\textsc{Resultant}(\mathbb{Z})$ is **NP-hard**.

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

$$\rightsquigarrow \begin{cases} X_1^2 - X_0^2 & = & 0 \\ & \vdots & \\ X_n^2 - X_0^2 & = & 0 \\ u_1 X_1 + \cdots + u_n X_n & = & 0 \end{cases}$$

$\square$

	$\textsc{PolSys}$	$\textsc{HomPolSys}$	$\textsc{Resultant}$
$\mathbb{Z}$	NP-hard	NP-hard	NP-hard
$\mathbb{F}_p$	NP-hard	NP-hard	**Open**

Hardness in positive characteristics

- HomPolSys($\mathbb{F}_p$) is NP-hard:

  \# homogeneous polynomials $\geqslant$ # variables

HomPolSys

- Variables X_0 and $X_1, \ldots, X_n$ over $\mathbb{F}_p$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

Hardness in positive characteristics

- HomPolSys($\mathbb{F}_p$) is NP-hard:
  # homogeneous polynomials $\geqslant$ # variables
- Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

HomPolSys

- Variables X_0 and $X_1, \ldots, X_n$ over $\mathbb{F}_p$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

Hardness in positive characteristics

- HomPolSys($\mathbb{F}_p$) is NP-hard:

  \# homogeneous polynomials $\geqslant$ # variables

- Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

HomPolSys

- Variables X_0 and $X_1, \dots, X_n$ over $\mathbb{F}_p$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

Idea of the reduction

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

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

Idea of the reduction

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

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

- $\forall \mathbf{a} \in \overline{\mathbb{F}_p}^{n+1} \Big(\forall j, f_j(\mathbf{a}) = 0 \implies \forall i, g_i(\mathbf{a}) = 0 \Big)$

Idea of the reduction

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

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

- $\forall \mathbf{a} \in \overline{\mathbb{F}_p}^{n+1} \Big(\forall j, f_j(\mathbf{a}) = 0 \boxed{\iff} \forall i, g_i(\mathbf{a}) = 0 \Big)$

if α_{ij} algebraically independent

Idea of the reduction

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

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

- $\forall a \in \overline{\mathbb{F}_p}^{n+1} \left(\forall j, f_j(a) = 0 \boxed{\iff} \forall i, g_i(a) = 0 \right)$

if α_{ij} algebraically independent

- Replace algebraic independence by random choice

Two useful results

Effective Bertini Theorem

Let $f_1, \dots, f_s$ and $g_0, \dots, g_n$ be as on previous slide. Then there exists a polynomial F of degree at most 3^{n+1} s.t.

$$F(\boldsymbol{\alpha}) \neq 0 \implies \forall \boldsymbol{a} \big(\forall i, f_i(\boldsymbol{a}) = 0 \iff \forall j, g_j(\boldsymbol{a}) = 0\big).$$

Two useful results

Effective Bertini Theorem

Let $f_1, \dots, f_s$ and $g_0, \dots, g_n$ be as on previous slide. Then there exists a polynomial F of degree at most 3^{n+1} s.t.

$$F(\alpha) \neq 0 \implies \forall a \big(\forall i, f_i(a) = 0 \iff \forall j, g_j(a) = 0\big).$$

Lemma [DeMillo-Lipton, Zippel, Schwartz (1978-80)]

Let $F \in \mathbb{F}_q[X_0, \dots, X_n]$ be nonzero, of degree d. If $A_0, \dots, A_n$ are chosen independently at random in $\mathbb{F}_q$, then

$$\mathbb{P}[F(A_0, \dots, A_n) = 0] \leqslant \frac{d}{q}$$

The randomized reduction

1. Build an extension $\mathbb{L}/\mathbb{F}_p$ with at least 3^{n+2} elements; [Shoup'90]

The randomized reduction

1. Build an extension $\mathbb{L}/\mathbb{F}_p$ with at least 3^{n+2} elements; [Shoup'90]
2. Choose the α_{ij}'s independently at random in $\mathbb{L}$;

The randomized reduction

1. Build an extension $\mathbb{L}/\mathbb{F}_p$ with at least 3^{n+2} elements; [Shoup'90]
2. Choose the α_{ij}'s independently at random in $\mathbb{L}$;
3. Define, for $0 \leqslant i \leqslant n$, $g_i = \sum_j \alpha_{ij} f_j$.

The randomized reduction

1. Build an extension $\mathbb{L}/\mathbb{F}_p$ with at least 3^{n+2} elements; [Shoup'90]
2. Choose the α_{ij}'s independently at random in $\mathbb{L}$;
3. Define, for $0 \leqslant i \leqslant n$, $g_i = \sum_j \alpha_{ij} f_j$.

- $f_j(\mathbf{a}) = 0 \implies g_i(\mathbf{a}) = 0$

The randomized reduction

1. Build an extension $\mathbb{L}/\mathbb{F}_p$ with at least 3^{n+2} elements; [Shoup'90]
2. Choose the α_{ij}'s independently at random in $\mathbb{L}$;
3. Define, for $0 \leqslant i \leqslant n$, $g_i = \sum_j \alpha_{ij} f_j$.

- $f_j(\mathbf{a}) = 0 \implies g_i(\mathbf{a}) = 0$
- If the f_j have no common root,

$$\mathbb{P}\left[\text{the } g_i \text{ have a common root}\right] = \mathbb{P}\left[F(\boldsymbol{\alpha}) = 0\right] \leqslant \frac{1}{3}$$

The randomized reduction

1. Build an extension $\mathbb{L}/\mathbb{F}_p$ with at least 3^{n+2} elements; [Shoup'90]
2. Choose the α_{ij}'s independently at random in $\mathbb{L}$;
3. Define, for $0 \leqslant i \leqslant n$, $g_i = \sum_j \alpha_{ij} f_j$.

- $f_j(\boldsymbol{a}) = 0 \implies g_i(\boldsymbol{a}) = 0$
- If the f_j have no common root,

$$\mathbb{P}\left[\text{the } g_i \text{ have a common root}\right] = \mathbb{P}\left[F(\boldsymbol{\alpha}) = 0\right] \leqslant \frac{1}{3}$$

Theorem [G.-Koiran-Portier'10-13]

Let p be a prime number. Resultant($\mathbb{F}_q$) is NP-hard for **degree-2** polynomials for some $q = p^s$, under **randomized reductions**.

Hardness in positive characteristics

- HomPolSys($\mathbb{F}_p$) is NP-hard:

  # homogeneous polynomials $\geqslant$ # variables

- Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

HomPolSys

- Variables X_0 and $X_1, \ldots, X_n$ over $\mathbb{F}_p$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

Hardness in positive characteristics

- HomPolSys($\mathbb{F}_p$) is NP-hard:

  \# homogeneous polynomials $\geqslant$ \# variables

- Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

HomPolSys

- Variables X_0 and $X_1, \ldots, X_n$ over $\mathbb{F}_p$
- Polynomials $X_0^2 - X_i^2$ for every $i > 0$ and — $f_1, \ldots, f_n$
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$ — $f_{n+1}, \ldots, f_s$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

Reduction

- New variables: $Y_1, \dots, Y_{s-n-1}$

New system

$$g(\mathbf{X}, \mathbf{Y}) = \left(\quad \right)$$

Reduction

- New variables: $Y_1, \dots, Y_{s-n-1}$

New system

$$g(\mathbf{X}, \mathbf{Y}) = \begin{pmatrix} f_1(\mathbf{X}) & \\ \vdots & \text{(unchanged)} \\ f_n(\mathbf{X}) & \\ & \\ & \\ & \\ & \end{pmatrix}$$

Reduction

- New variables: $Y_1, \ldots, Y_{s-n-1}$

New system

$$g(\mathbf{X},\mathbf{Y}) = \begin{pmatrix} f_1(\mathbf{X}) & \\ \vdots & \text{(unchanged)} \\ f_n(\mathbf{X}) & \\ f_{n+1}(\mathbf{X}) & + \lambda Y_1^2 \\ & \\ & \\ & \end{pmatrix}$$

Reduction

- New variables: $Y_1, \dots, Y_{s-n-1}$

New system

$$g(\mathbf{X}, \mathbf{Y}) = \begin{pmatrix} f_1(\mathbf{X}) & & \\ \vdots & & \text{(unchanged)} \\ f_n(\mathbf{X}) & & \\ f_{n+1}(\mathbf{X}) & & +\lambda Y_1^2 \\ f_{n+2}(\mathbf{X}) & -Y_1^2 & +\lambda Y_2^2 \\ & & \\ & & \end{pmatrix}$$

Reduction

- New variables: $Y_1, \dots, Y_{s-n-1}$

New system

$$g(\mathbf{X}, \mathbf{Y}) = \begin{pmatrix} f_1(\mathbf{X}) & & \\ \vdots & \text{(unchanged)} & \\ f_n(\mathbf{X}) & & \\ f_{n+1}(\mathbf{X}) & & +\lambda Y_1^2 \\ f_{n+2}(\mathbf{X}) & -Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(\mathbf{X}) & -Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \end{pmatrix}$$

Reduction

- New variables: $Y_1, \dots, Y_{s-n-1}$

New system

$$g(\mathbf{X}, \mathbf{Y}) = \begin{pmatrix} f_1(\mathbf{X}) & & \\ \vdots & & \text{(unchanged)} \\ f_n(\mathbf{X}) & & \\ f_{n+1}(\mathbf{X}) & & +\lambda Y_1^2 \\ f_{n+2}(\mathbf{X}) & -Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(\mathbf{X}) & -Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \\ f_s(\mathbf{X}) & -Y_{s-n-1}^2 & \end{pmatrix}$$

Reduction

- New variables: $Y_1, \dots, Y_{s-n-1}$

New system

$$g(\mathbf{X},\mathbf{Y}) = \begin{pmatrix} f_1(\mathbf{X}) & & \\ \vdots & \text{(unchanged)} & \\ f_n(\mathbf{X}) & & \\ f_{n+1}(\mathbf{X}) & & +\lambda Y_1^2 \\ f_{n+2}(\mathbf{X}) & -Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(\mathbf{X}) & -Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \\ f_s(\mathbf{X}) & -Y_{s-n-1}^2 & \end{pmatrix}$$

$$\alpha \text{ root of } f \implies (\alpha, 0) \text{ root of } g$$

Equivalence?

$(\mathbf{a}, \mathbf{b})$ non trivial root of $g \overset{?}{\Longrightarrow}$ $\mathbf{a}$ non trivial root of f

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

Equivalence?

$$(\mathbf{a}, \mathbf{b}) \text{ non trivial root of } g \overset{?}{\Longrightarrow} \mathbf{a} \text{ non trivial root of } f$$

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

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

Equivalence?

$(\mathbf{a}, \mathbf{b})$ non trivial root of $g \overset{?}{\Longrightarrow}$ $\mathbf{a}$ non trivial root of f

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

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

Equivalence?

$$(\mathbf{a}, \mathbf{b}) \text{ non trivial root of } g \overset{?}{\implies} \mathbf{a} \text{ non trivial root of } f$$

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

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

Equivalence?

$$(\mathbf{a}, \mathbf{b}) \text{ non trivial root of } g \overset{?}{\Longrightarrow} \mathbf{a} \text{ non trivial root of } f$$

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

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

Equivalence?

$$(\mathbf{a}, \mathbf{b}) \text{ non trivial root of } g \overset{?}{\Longrightarrow} \mathbf{a} \text{ non trivial root of } f$$

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

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

Equivalence?

$(\mathbf{a}, \mathbf{b})$ non trivial root of $g \overset{?}{\Longrightarrow}$ $\mathbf{a}$ non trivial root of f

$$\begin{pmatrix} \\ \\ \\ \epsilon_1 & & +\lambda B_1 \\ \epsilon_2 & -B_1 & +\lambda B_2 \\ \vdots & & \\ \epsilon_{s-n-2} & -B_{s-n-2} & +\lambda B_{s-n-1} \\ \epsilon_{s-n-1} & -B_{s-n-1} & \end{pmatrix}$$

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

Equivalence?

$$(\mathbf{a}, \mathbf{b}) \text{ non trivial root of } g \overset{?}{\Longrightarrow} \mathbf{a} \text{ non trivial root of } f$$

$$\begin{pmatrix}
 & & & & \\
 & & & & \\
 & & & & \\
\epsilon_1 & & & & +\lambda B_1 \\
\epsilon_2 & & & -B_1 & +\lambda B_2 \\
\vdots & & & & \\
\epsilon_{s-n-2} & -B_{s-n-2} & +\lambda B_{s-n-1} & & \\
\epsilon_{s-n-1} & -B_{s-n-1} & & &
\end{pmatrix}$$

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

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

Equivalence?

$$(\mathbf{a},\mathbf{b}) \text{ non trivial root of } g \overset{?}{\Longrightarrow} \mathbf{a} \text{ non trivial root of } f$$

$$\begin{pmatrix} & & \\ & & \\ & & \\ \epsilon_1 & & +\lambda B_1 \\ \epsilon_2 & -B_1 & +\lambda B_2 \\ \vdots & & \\ \epsilon_{s-n-2} & -B_{s-n-2} & +\lambda B_{s-n-1} \\ \epsilon_{s-n-1} & -B_{s-n-1} & \end{pmatrix}$$

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

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

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

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N;
  [Shoup'90]

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N; [Shoup'90]
- Let $\mathbb{L} = \mathbb{F}_p[\xi]/(P)$ and $\lambda = \xi \in \mathbb{L}$.

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N; [Shoup'90]
- Let $\mathbb{L} = \mathbb{F}_p[\xi]/(P)$ and $\lambda = \xi \in \mathbb{L}$.
- In the extension $\mathbb{L}$, $\det = 0 \iff \epsilon_i = 0$ for all i.

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N; [Shoup'90]
- Let $\mathbb{L} = \mathbb{F}_p[\xi]/(P)$ and $\lambda = \xi \in \mathbb{L}$.

- In the extension $\mathbb{L}$, $\det = 0 \iff \epsilon_i = 0$ for all i.
- For coefficients in $\mathbb{F}_p$ instead of $\mathbb{L}$: "put P inside the system"

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N; [Shoup'90]
- Let $\mathbb{L} = \mathbb{F}_p[\xi]/(P)$ and $\lambda = \xi \in \mathbb{L}$.

- In the extension $\mathbb{L}$, $\det = 0 \iff \epsilon_i = 0$ for all i.
- For coefficients in $\mathbb{F}_p$ instead of $\mathbb{L}$: "put P inside the system"

Theorem [G.-Koiran-Portier'10-13]

Let p be a prime number.

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N; [Shoup'90]
- Let $\mathbb{L} = \mathbb{F}_p[\xi]/(P)$ and $\lambda = \xi \in \mathbb{L}$.
- In the extension $\mathbb{L}$, $\det = 0 \iff \epsilon_i = 0$ for all i.
- For coefficients in $\mathbb{F}_p$ instead of $\mathbb{L}$: "put P inside the system"

Theorem [G.-Koiran-Portier'10-13]

Let p be a prime number.

- Resultant($\mathbb{F}_p$) is NP-hard for **linear-degree** polynomials.

Last step

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

- Compute an irreducible polynomial $P \in \mathbb{F}_p[\xi]$ of degree N; [Shoup'90]
- Let $\mathbb{L} = \mathbb{F}_p[\xi]/(P)$ and $\lambda = \xi \in \mathbb{L}$.

- In the extension $\mathbb{L}$, $\det = 0 \iff \epsilon_i = 0$ for all i.
- For coefficients in $\mathbb{F}_p$ instead of $\mathbb{L}$: "put P inside the system"

Theorem [G.-Koiran-Portier'10-13]

Let p be a prime number.

- RESULTANT($\mathbb{F}_p$) is NP-hard for **linear-degree** polynomials.
- RESULTANT($\mathbb{F}_q$) is NP-hard for **degree-2** polynomials for some $q = p^s$.

Conclusion

- Evaluation of the resultant:

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;
  - NP-**hard** in any characteristic;

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;
  - NP-**hard** in any characteristic;
  - No known difference between square and non-square systems.

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;
  - NP-**hard** in any characteristic;
  - No known difference between square and non-square systems.
- Some open problems:

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;
  - NP-**hard** in any characteristic;
  - No known difference between square and non-square systems.
- Some open problems:
  - NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;
  - NP-**hard** in any characteristic;
  - No known difference between square and non-square systems.
- Some open problems:
  - NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?
  - Improve the PSPACE upper bound in positive characteristics...

Conclusion

- Evaluation of the resultant:
  - Computable in **polynomial space**;
  - Evidences for PSPACE-hardness;
  - Similar results in Valiant's algebraic model.
- Checking the satisfiability of a polynomial system:
  - In characteristic 0, **in** AM ("almost NP");
  - In positive characteristic, **in** PSPACE;
  - NP-**hard** in any characteristic;
  - No known difference between square and non-square systems.
- Some open problems:
  - NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?
  - Improve the PSPACE upper bound in positive characteristics...
  - ... or the NP lower bound.