Complexity of the resultant

Bruno Grenet

joint work with Pascal Koiran & Natacha Portier

LIX – École Polytechnique
Is there a (nonzero) solution?

\[ X^2 + Y^2 - Z^2 = 0 \]
\[ XZ + 3XY + YZ + Y^2 = 0 \]
\[ XZ - Y^2 = 0 \]
Is there a (nonzero) solution?

\[ X^2 + Y^2 - Z^2 = 0 \]
\[ XZ + 3XY + YZ + Y^2 = 0 \]
\[ XZ - Y^2 = 0 \]

**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. \( f(\mathbf{a}) = 0 \)?
Is there a (nonzero) solution?

\[ \begin{align*}
X^2 + Y^2 - Z^2 &= 0 \\
XZ + 3XY + YZ + Y^2 &= 0 \\
XZ - Y^2 &= 0
\end{align*} \]

**PolSys** \((\mathbb{K})\)

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

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

**HomPolSys** \((\mathbb{K})\)

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

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

\[ f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n], \quad f_i = \sum_{|\alpha|_1 \leq d_i} \gamma_{i,\alpha} X^\alpha \]

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

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

$$
\begin{align*}
R_1(\gamma) &= 0 \\
\vdots & \implies \exists \alpha, \\
R_h(\gamma) &= 0
\end{align*}
$$

$$
\begin{align*}
f_1(a) &= 0 \\
\vdots \\
f_s(a) &= 0
\end{align*}
$$
Two Univariate Polynomials

\[ P = \sum_{i=0}^{m} p_i X^i \quad , \quad Q = \sum_{j=0}^{n} q_j X^j \]
Two Univariate Polynomials

\[ P = \sum_{i=0}^{m} p_i X^i \quad , \quad Q = \sum_{j=0}^{n} q_j X^j \]

\[ R = \det \begin{pmatrix} p_m & \cdots & p_0 \\ \vdots & \ddots & \vdots \\ q_n & \cdots & q_0 \end{pmatrix} \Rightarrow \text{Sylvester Matrix} \]

Non-trivial root?
Two Univariate Polynomials

\[ P = \sum_{i=0}^{m} p_i X^i \quad \text{and} \quad Q = \sum_{j=0}^{n} q_j X^j \]

\[
\begin{pmatrix}
p_m & \cdots & p_0 \\
\vdots & \ddots & \vdots \\
p_m & \cdots & p_0 \\
q_n & \cdots & q_0 \\
\vdots & \ddots & \vdots \\
q_n & \cdots & q_0
\end{pmatrix}
\]

\[ R = \det \text{Sylvester Matrix} \]

\[ \Rightarrow \text{Sylvester Matrix} \]
Two Bivariate Polynomials

\[ P = \sum_{i=0}^{m} p_i X^i Y^{m-i}, \quad Q = \sum_{j=0}^{n} q_j X^j Y^{n-j} : \]

\[ R = \text{det} \begin{pmatrix} p_m & \cdots & p_0 \\ \vdots & \ddots & \vdots \\ q_n & \cdots & q_0 \end{pmatrix} \]

\[ \implies \text{Sylvester Matrix} \]

\[ \blacktriangleright \text{Non trivial root?} \]
More generally

- Wlog, homogeneous polynomials, non trivial roots
More generally

▶ Wlog, homogeneous polynomials, non trivial roots

▶ $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n] \leadsto$ a unique resultant polynomial
More generally

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

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

- Wlog, homogeneous polynomials, non trivial roots
  - $f_1, \ldots, f_{n+1} \in K[X_0, \ldots, X_n] \mapsto$ a unique resultant polynomial

- Sylvester Matrix $\mapsto$ Macaulay Matrix (exponential size)
  - $s$ polynomials $\neq n + 1$ variables $\mapsto$ several polynomials needed

**Resultant**($K$)

| Input: $f_1, \ldots, f_{n+1} \in K[X_0, \ldots, X_n]$, homogeneous |
|Question: Is there a nonzero $a \in \overline{K}^{n+1}$ s.t. $f(a) = 0$? |
Macaulay matrices

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

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

**Definition**

The first Macaulay matrix is defined as follows:

- Its rows and columns are indexed by \( \mathcal{M}_D^n \);
- The row indexed by \( X^\alpha \) represents
  \[
  \frac{X^\alpha}{X_i^{d_i}} f_i, \text{ where } i = \min\{j : d_j \leq \alpha_j\}.
  \]

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

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.
Theorem [Canny’87]

The resultant is computable in polynomial space.

Proof idea.

- The resultant can be expressed as \( \text{det}(M) / \text{det}(N) \), 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.
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).
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 $G_x^M$ its graph of configurations:
  - initial configuration $c_i$,
  - accepting configuration $c_a$;
- $G_x^M$ can be represented by a boolean circuit;
- There exists a path $c_i \leadsto c_a$ in $G_x^M$ iff $x \in \mathcal{L}(\mathcal{M})$;
- Let $A \simeq$ adjacency matrix of $G_x^M$:
  $$\det(A) \neq 0 \iff \exists c_i \leadsto c_a.$$
The resultant in Valiant’s model of computation

**Theorem**

In Valiant’s algebraic model of computation:

- The resultant belongs to VPSPACE, \[\text{[Koiran-Perifel’07]}\]
- Determinants of *succinctly represented* matrices is VPSPACE-complete. \[\text{[Malod’11]}\]
Upper bounds for polynomial systems

PSPACE

Upper bounds

- \( \text{PolSys}(\mathbb{F}_p) \in \text{PSPACE} \)
Upper bounds for polynomial systems

**Upper bounds**

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

\[ \implies \text{HomPolSys}(\mathbb{F}_p), \text{Resultant}(\mathbb{F}_p) \in \text{PSPACE} \]

**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.
Upper bounds for polynomial systems

Upper bounds

- \( \text{PolSys}(\mathbb{F}_p) \in \text{PSPACE} \)
  \[ \implies \text{HomPolSys}(\mathbb{F}_p), \text{Resultant}(\mathbb{F}_p) \in \text{PSPACE} \]
- Under GRH, \( \text{PolSys}(\mathbb{Z}) \in \text{AM} \) [Koiran'96]
Upper bounds for polynomial systems

- \( \text{PolSys}(\mathbb{F}_p) \in \text{PSPACE} \)
  \( \implies \) \( \text{HomPolSys}(\mathbb{F}_p), \text{Resultant}(\mathbb{F}_p) \in \text{PSPACE} \)

- Under GRH, \( \text{PolSys}(\mathbb{Z}) \in \text{AM} \)  \[ \text{[Koiran'96]} \]
  \( \implies \) \( \text{HomPolSys}(\mathbb{Z}), \text{Resultant}(\mathbb{Z}) \in \text{AM} \)
Proof sketch of Koiran’s result

- Let $f = (f_1, \ldots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$;
- Let $P(x)$ be the set of prime numbers $\leq x$;
- Let $P_f(x)$ be the set of prime numbers $\leq x$, s.t. $f$ has a root mod $p$. 
Proof sketch of Koiran’s result

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

**Theorem**

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

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

[Koiran’96]
Proof sketch of Koiran’s result

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

**Theorem**

There exist polynomial-time computable $\Lambda$ and $x_0$ s.t.

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

**Algorithm.**

1. Compute $\Lambda$, $x_0$;
2. Take a random hash function $h : \mathcal{P}(x_0) \to \{0, 1\}^{2 + \lceil \log \Lambda \rceil}$;
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 $f = (f_1, \ldots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$;
- Let $\mathcal{P}(x)$ be the set of prime numbers $\leq x$;
- Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leq x$, 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 $\#\mathcal{P}_f(x_0) \leq A$;
- If $f$ has a root in $\mathbb{C}$, then $\#\mathcal{P}_f(x_0) \geq 8A(\log A + 3)$.

Algorithm.

1. Compute $A$, $x_0$;
2. Take a random hash function $h : \mathcal{P}(x_0) \rightarrow \{0, 1\}^{2+\lceil\log A\rceil}$;
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 $f = (f_1, \ldots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$;

Let $\mathcal{P}(x)$ be the set of prime numbers $\leq x$;

Let $\mathcal{P}_f(x)$ be the set of prime numbers $\leq x$, s.t. $f$ has a root mod $p$.

**Theorem**

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

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

**Algorithm.**

1. Compute $A$, $x_0$;
2. Take a random hash function $h : \mathcal{P}(x_0) \rightarrow \{0, 1\}^{2 + \lceil \log A \rceil}$;
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. $\leq 1/4$ if $f$ has no root in $\mathbb{C}$. 
Lower bounds for non-square systems

Notation: \( F_0 = \mathbb{Q} \)
Lower bounds for non-square systems

Notation: \( \mathbb{F}_0 = \mathbb{Q} \)

**Proposition** [Folklore]

For \( p = 0 \) or prime, \( \text{PolSys}(\mathbb{F}_p) \) & \( \text{HomPolSys}(\mathbb{F}_p) \) are \( \text{NP-hard} \).
Lower bounds for non-square systems

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

**Proposition** [Folklore]

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

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

\[\text{Boolean variables } u_1, \ldots, u_n \quad \text{Equations} \quad \begin{align*}
  u_i = \text{True} \\
  u_i = \neg u_j \\
  u_i = u_j \lor u_k \\
\end{align*} \]

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

\[\begin{align*}
  X_0 \cdot (X_i + X_0) \\
  X_0 \cdot (X_i + X_j) \\
  (X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)
\end{align*} \]
Lower bounds for non-square systems

Notation: \( F_0 = \mathbb{Q} \)

**Proposition** [Folklore]

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

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

**Boolsys**

- **Boolean variables**
  \( u_1, \ldots, u_n \)

- **Equations**
  - \( u_i = \text{True} \)
  - \( u_i = \neg u_j \)
  - \( u_i = u_j \lor u_k \)
Lower bounds for non-square systems

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

**Proposition** [Folklore]

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

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

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

**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, \( \text{PolSys}(\mathbb{F}_p) \) & \( \text{HomPolSys}(\mathbb{F}_p) \) are \textbf{NP-hard}.

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

**\text{BoolSys}**

- Boolean variables \( u_1, \ldots, u_n \)
- Equations
  - \( u_i = \text{True} \)
  - \( u_i = \neg u_j \)
  - \( u_i = u_j \lor u_k \)

**\text{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
  - \( X_0 \cdot (X_i + X_0) \)
Lower bounds for non-square systems

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

**Proposition** [Folklore]

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

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

<table>
<thead>
<tr>
<th><strong>Boolsys</strong></th>
<th><strong>HomPolSys</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Boolsys Diagram" /></td>
<td><img src="image" alt="HomPolSys Diagram" /></td>
</tr>
<tr>
<td><img src="image" alt="Boolsys Table" /></td>
<td><img src="image" alt="HomPolSys Table" /></td>
</tr>
</tbody>
</table>
Lower bounds for non-square systems

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

Proposition [Folklore]

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

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

<table>
<thead>
<tr>
<th><strong>Boolsys</strong></th>
<th><strong>HomPolSys</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Boolean variables $u_1, \ldots, u_n$</td>
<td>▶ Variables (over $\mathbb{F}_p$) $X_0$ and $X_1, \ldots, X_n$</td>
</tr>
<tr>
<td>▶ Equations</td>
<td>▶ Polynomials $X_0^2 - X_i^2$ for every $i &gt; 0$ and</td>
</tr>
<tr>
<td>• $u_i = \text{True}$</td>
<td>• $X_0 \cdot (X_i + X_0)$</td>
</tr>
<tr>
<td>• $u_i = \neg u_j$</td>
<td>• $X_0 \cdot (X_i + X_j)$</td>
</tr>
<tr>
<td>• $u_i = u_j \lor u_k$</td>
<td>• $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$</td>
</tr>
</tbody>
</table>
**Proposition**  

\[ \text{RESULTANT}(\mathbb{Z}) \text{ is NP-hard.} \]

---

[Heintz-Morgenstern’93]
Proposition [Heintz-Morgenstern’93]

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

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

[Heintz-Morgenstern’93]

\[
\text{RESULTANT}(\mathbb{Z}) \text{ is NP-hard.}
\]

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

\[
\begin{align*}
X_1^2 - X_0^2 &= 0 \\
&\vdots \\
X_n^2 - X_0^2 &= 0 \\
\sum_{i=1}^n u_i x_i &= 0
\end{align*}
\]

\[\square\]
Proposition [Heintz-Morgenstern'93]

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

**Proof.** Partition: \(S = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}, \exists S' \subseteq S, \sum_{i \in S'} u_i = \sum_{j \not\in S'} u_j\)

\[
\begin{align*}
X_1^2 - X_0^2 &= 0 \\
\vdots \\
X_n^2 - X_0^2 &= 0 \\
u_1 X_1 + \cdots + u_n X_n &= 0
\end{align*}
\]

\[\blacksquare\]

<table>
<thead>
<tr>
<th></th>
<th><strong>PolSys</strong></th>
<th><strong>HomPolSys</strong></th>
<th><strong>RESULTANT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(\mathbb{Z})</td>
<td>NP-hard</td>
<td>NP-hard</td>
<td>NP-hard</td>
</tr>
<tr>
<td>(\mathbb{F}_p)</td>
<td>NP-hard</td>
<td>NP-hard</td>
<td><strong>Open</strong></td>
</tr>
</tbody>
</table>
Hardness in positive characteristics

- HomPolSys($\mathbb{F}_p$) is NP-hard:
  \[ \# \text{homogeneous polynomials} \geq \# \text{variables} \]

**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

- $\text{HomPolSys}(\mathbb{F}_p)$ is NP-hard:
  - $\#$ homogeneous polynomials $\geq \#$ 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

- $\text{HomPolSys}(\mathbb{F}_p)$ is NP-hard: \[
\# \text{homogeneous polynomials} \geq \# \text{variables}
\]

- 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
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$
Idea of the reduction

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

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

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

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

for $\alpha_{ij}$ algebraically independent

Replace algebraic independence by random choice.
Idea of the reduction

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

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

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

if $\alpha_{ij}$ algebraically independent
Idea of the reduction

- For $f_1, \ldots, f_s$ homogeneous of degree 2,
  \[
  g_i := \sum_{j=1}^{s} \alpha_{ij} f_j, 0 \leq i \leq n.
  \]

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

  - if $\alpha_{ij}$ algebraically independent

- Replace algebraic independence by random choice
Two useful results

**Effective Bertini Theorem**

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

$$F(\alpha) \neq 0 \implies \forall a \left( \forall i, f_i(a) = 0 \iff \forall j, g_j(a) = 0 \right).$$
**Effective Bertini Theorem**

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

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

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

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

$$\mathbb{P}[F(A_0, \ldots, A_n) = 0] \leq \frac{d}{q}$$
The randomized reduction

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

$\text{[Shoup'90]}$

$\Rightarrow$
The randomized reduction

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

$\implies f_j(a) = 0 \implies g_i(a) = 0$.

If the $f_j$ have no common root, $P[\text{the } g_i \text{ have a common root}] = P[F(\alpha) = 0] \leq 3$.

Theorem [G.-Koiran-Portier’10-13]
Let $p$ be a prime number.
$\mathbb{R/e.sc/s.sc/u.sc/l.sc/t.sc}(\mathbb{F}_q)$ is $\text{NP}$-hard for degree-2 polynomials for some $q = p^s$, under randomized reductions.
The randomized reduction

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

\[\text{If the } f_j \text{ have no common root,} \]
\[\mathbb{P}[\text{the } g_i \text{ have a common root}] = \mathbb{P}[\mathbb{F}(\alpha) = 0] \leq 3 \]

\[\text{Theorem [G.-Koiran-Portier'10-13]}\]
\[\text{Let } p \text{ be a prime number.} \]
\[\mathbb{R/e.sc/s.sc/u.sc/l.sc/t.sc} (\mathbb{F}_{q^s}) \text{ is } \text{NP } \text{hard for degree-} 2 \text{ polynomials for some } q = p^s, \text{ under randomized reductions.} \]
The randomized reduction

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

$\Rightarrow f_j(a) = 0 \implies g_i(a) = 0$

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

Let $p$ be a prime number. $\text{R/e.sc/s.sc/u.sc/l.sc/t.sc/a.sc/n.sc/t.sc}$

$(\mathbb{F}_q^p)$ is $\text{NP}$-hard for degree-2 polynomials for some $q = p^s$, under randomized reductions.
The randomized reduction

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

$$\begin{align*}
\blacktriangleright \quad & f_j(a) = 0 \implies g_i(a) = 0 \\
\blacktriangleright \quad & \text{If the } f_j \text{ have no common root,}
\end{align*}$$

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

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

$\rightarrow f_j(\alpha) = 0 \implies g_i(\alpha) = 0$

$\rightarrow$ If the $f_j$ have no common root,

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

**Theorem** [G.-Koiran-Portier’10-13]

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

- $\text{HomPolSys}(\mathbb{F}_p)$ is NP-hard:
  \[ \# \text{homogeneous polynomials} \geq \# \text{variables} \]

- 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

- $\text{HomPolSys}(\mathbb{F}_p)$ is NP-hard:
  - $\#$ homogeneous polynomials $\geq \#$ variables

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

### $\text{HomPolSys}$

- 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 $f_1, \ldots, f_n$
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

- $f_{n+1}, \ldots, f_s$
Reduction

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

New system

$g(X, Y) =$

\[
\begin{pmatrix}
\end{pmatrix}
\]
Reduction

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

New system

$$g(X, Y) = \begin{pmatrix}
f_1(X) \\
\vdots \\
f_n(X) \\
\end{pmatrix} + \lambda Y_2^1 f_1^2(X) - Y_2^1 + \lambda Y_2^{s-n-2} f_{s-n-1}(X) - Y_2^{s-n-1}$$
Reduction

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

**New system**

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

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

**New system**

\[
g(X, Y) = \begin{pmatrix}
f_1(X) \\ \\
\vdots \\ \\
f_n(X) \\ \\
f_{n+1}(X) \\ \\
f_{n+2}(X)
\end{pmatrix}
\]

(unchanged)

\[
+ \lambda Y_1^2 - Y_1^2 + \lambda Y_2^2
\]

\[
= \Rightarrow \left( a, 0 \right)
\]
Reduction

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

New system

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

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

New system

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

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

New system

$$
g(X, Y) = \begin{pmatrix} f_1(X) \\ \vdots \\ f_n(X) \\ f_{n+1}(X) \\ f_{n+2}(X) \\ \vdots \\ f_{s-1}(X) \\ f_s(X) \\ \end{pmatrix}$$

\[ + \lambda Y_1^2 + \lambda Y_2^2 - Y_1^2 + \lambda Y_2^2 + \lambda Y_3^2 + \lambda Y_{s-n-2}^2 + \lambda Y_{s-n-1}^2 - Y_1^2 + \lambda Y_2^2 + \lambda Y_{s-n-1}^2 - Y_1^2 + \lambda Y_2^2 \]

\[ \vdots \]

$$
a \text{ root of } f \implies (a, 0) \text{ root of } g$$
Equivalence?

\[(a, b) \text{ non trivial root of } g \iff a \text{ non trivial root of } f\]

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

\(? = \iff \forall i, \epsilon_i = 0 = \iff f_1(a) = \cdots = f_s(a) = 0\)
Equivalence?

\((a, b)\) non trivial root of \(g \implies a\) non trivial root of \(f\)

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

\(\implies a = 0 \implies b = 0\)
Equivalence?

\((a, b)\) non trivial root of \(g\) \(\iff\) \(a\) non trivial root of \(f\)

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

- \(a = 0 \iff b = 0\)
- \(a_0 = 1\) and \(a_i = \pm 1\)
Equivalence?

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

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

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

\((a, b)\) non trivial root of \(g \implies a\) non trivial root of \(f\)

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

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

\[(a, b) \text{ non trivial root of } g \iff a \text{ non trivial root of } f\]

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

\[\begin{align*}
\epsilon_i &= f_{n+i}(a) \\
B_i &= b_i^2
\end{align*}\]

\[\Box\quad \begin{cases}
\quad a = 0 \implies b = 0 \\
\quad a_0 = 1 \text{ and } a_i = \pm 1 \\
\quad \epsilon_i = f_{n+i}(a) \\
\quad B_i = b_i^2
\end{cases}\]
Equivalence?

\((a, b)\) non trivial root of \(g \iff a\) non trivial root of \(f\)

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

\[\Rightarrow a = 0 \iff b = 0\]

\[\Rightarrow a_0 = 1 \text{ and } a_i = \pm 1\]

\[\Rightarrow \epsilon_i = f_{n+i}(a)\]

\[\Rightarrow B_i = b_i^2\]
Equivalence?

\[(a, b) \text{ non trivial root of } g \quad \Rightarrow \quad a \text{ non trivial root of } f\]

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

\[\det = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_{s-n} \lambda^{s-n-1})\]

\[\Rightarrow a = 0 \quad \Rightarrow \quad b = 0\]

\[\Rightarrow a_0 = 1 \quad \text{and} \quad a_i = \pm 1\]

\[\Rightarrow \epsilon_i = f_{n+i}(a)\]

\[\Rightarrow B_i = b_i^2\]
Equivalence?

\[(a, b) \text{ non trivial root of } g \quad \Rightarrow \quad a \text{ non trivial root of } f\]

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

\[\det = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_{s-n} \lambda^{s-n-1})\]

\[\det = 0 \quad \Rightarrow \quad \forall i, \epsilon_i = 0 \quad \Rightarrow \quad f_1(a) = \cdots = f_s(a) = 0\]

\[\triangleright a = 0 \quad \Rightarrow \quad b = 0\]

\[\triangleright a_0 = 1 \text{ and } a_i = \pm 1\]

\[\triangleright \epsilon_i = f_{n+i}(a)\]

\[\triangleright B_i = b_i^2\]
Last step

\[ \text{det} = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_N \lambda^{N-1}) \]

- Compute an irreducible polynomial \( P \in \mathbb{F}_p[\xi] \) of degree \( N \);
  
  \[ \text{[Shoup'90]} \]
Last step

\[ \det = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_N \lambda^{N-1}) \]

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

\[ \text{det} = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_N \lambda^{N-1}) \]

- 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 \( \mathbb{L} \), \( \text{det} = 0 \iff \epsilon_i = 0 \) for all \( i \).
Last step

\[
\det = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_N \lambda^{N-1})
\]

- 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

\[
\det = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_N \lambda^{N-1})
\]

- 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**

Let \( p \) be a prime number.

[G.-Koiran-Portier’10-13]
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 \( N \);
  \[ \text{[Shoup'90]} \]
- Let \( L = \mathbb{F}_p[\xi]/(P) \) and \( \lambda = \xi \in L \).

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

**Theorem** \[ \text{[G.-Koiran-Portier'10-13]} \]

Let \( p \) be a prime number.

- \( \text{RESULTANT}(\mathbb{F}_p) \) is NP-hard for \textbf{linear-degree} polynomials.
Last step

\[
det = \pm (\epsilon_1 + \epsilon_2 \lambda + \cdots + \epsilon_N \lambda^{N-1})
\]

- 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.

- \( \text{Resultant}(\mathbb{F}_p) \) is NP-hard for **linear-degree** polynomials.
- \( \text{Resultant}(\mathbb{F}_q) \) is NP-hard for **degree-2** polynomials for some \( q = p^s \).
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 $F_p$?
- Improve the PSPACE upper bound in positive characteristics. . .
- . . . or the NP lower bound.
Conclusion

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

- 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 \( F_p \)?
  - Improve the PSPACE upper bound in positive characteristics...
    - ... or the NP lower bound.
Conclusion

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

▶ 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.
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 \textit{polynomial space};
  • Evidences for \textsc{PSPACE}-hardness;
  • Similar results in Valiant’s algebraic model.

▶ Checking the satisfiability of a polynomial system:
  • In characteristic 0, \textit{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 \textit{polynomial space};
  • Evidences for PSPACE-hardness;
  • Similar results in Valiant’s algebraic model.

▶ Checking the satisfiability of a polynomial system:
  • In characteristic 0, \textit{in AM} (“almost NP”);
  • In positive characteristic, \textit{in PSPACE};
  • \textit{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 \textit{polynomial space};
  • Evidences for PSPACE-hardness;
  • Similar results in Valiant’s algebraic model.

► Checking the satisfiability of a polynomial system:
  • In characteristic 0, \textbf{in AM} (“almost NP”);
  • In positive characteristic, \textbf{in PSPACE};
  • \textbf{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.