On the complexity of polynomial system solving

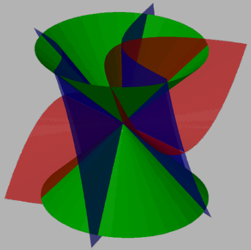
Bruno Grenet
LIX – École Polytechnique

partly based on a joint work with Pascal Koiran & Natacha Portier

XXV$^{\text{èmes}}$ rencontres arithmétiques de Caen

Île de Tatihou, June 30. – July 4., 2014

Is there a (nonzero) solution?

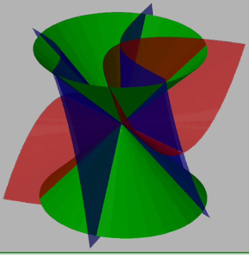


$$X^2 + Y^2 - Z^2 = 0$$

$$XZ + 3XY + YZ + Y^2 = 0$$

$$XZ - Y^2 = 0$$

Is there a (nonzero) solution?



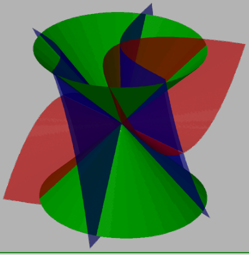
$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

PolSys$_{\mathbb{K}}$

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

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

Is there a (nonzero) solution?



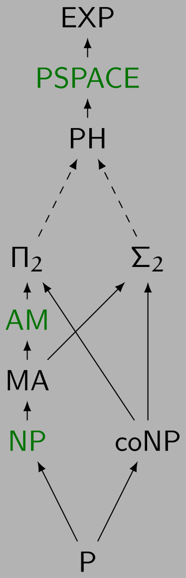
$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

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. $f(\mathbf{a}) = 0$?

- Lower and upper bounds in terms of complexity classes
- $\mathbb{K}$: Either $\mathbb{Z}$ or $\mathbb{F}_q$ for some $q = p^s$
- Variants: Homogeneity, number of polynomials



Definition

P	Deterministic polynomial time
NP, coNP	Non-deterministic polynomial time
MA, AM	Merlin-Arthur, Arthur-Merlin
Σ_2, Π_2 ,PH	Polynomial hierarchy
PSPACE	(Non-)deterministic polynomial space
EXP	Deterministic exponential time

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. $f(\mathbf{a}) = 0$?

$\textsc{HomPolSys}_{\mathbb{K}}$

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. $f(\mathbf{a}) = 0$?

Proposition

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_q$, $\textsc{PolSys}_{\mathbb{K}}$ and $\textsc{HomPolSys}_{\mathbb{K}}$ are polynomial-time equivalent.

$\text{HomPolSys}_{\mathbb{K}}$

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. $f(\mathbf{a}) = 0$?

Proposition

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_q$, $\text{PolSys}_{\mathbb{K}}$ and $\text{HomPolSys}_{\mathbb{K}}$ are polynomial-time equivalent.

Proof.

- $\text{PolSys}_{\mathbb{K}} \leqslant_m^P \text{HomPolSys}_{\mathbb{K}}$: Homogenization
- $\text{HomPolSys}_{\mathbb{K}} \leqslant_m^P \text{PolSys}_{\mathbb{K}}$: New polynomial $\sum_i X_i Y_i - 1$, where $Y_0, \ldots, Y_n$ are fresh variables

$$f_1, \dots, f_s \in \mathbb{K}[X_0, \dots, X_n], \qquad f_i = \sum_{|\alpha| = d_i} \gamma_{i,\alpha} \mathbf{X}^\alpha$$

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

$$f_1, \ldots, f_s \in \mathbb{K}[X_0, \ldots, X_n], \qquad f_i = \sum_{|\alpha| = d_i} \gamma_{i,\alpha} \mathbf{X}^\alpha$$

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

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

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

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

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

$$\mathrm{Res}(P,Q) = \det \begin{pmatrix} p_m & \ldots\ldots\ldots\ldots & p_0 & & \\ & \ddots & & \ddots & \\ & p_m & \ldots\ldots\ldots\ldots & & p_0 \\ q_n & \ldots\ldots\ldots & q_0 & & \\ & \ddots & & \ddots & \\ & q_n & \ldots\ldots\ldots & q_0 & \end{pmatrix}$$

Sylvester Matrix

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

$$\mathrm{Res}(P,Q) = \det \begin{pmatrix} p_m & \cdots\cdots\cdots & p_0 & & \\ & \ddots & & \ddots & \\ & & p_m & \cdots\cdots\cdots & p_0 \\ q_n & \cdots\cdots & q_0 & & \\ & \ddots & & \ddots & \\ & & q_n & \cdots\cdots & q_0 \end{pmatrix}$$

Sylvester Matrix

More generally

- $f_1, \dots, f_{n+1} \in \mathbb{K}[X_0, \dots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial
  - Sylvester matrix $\rightsquigarrow$ Macaulay matrices (exponential size)

More generally

- $f_1, \dots, f_{n+1} \in \mathbb{K}[X_0, \dots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial
  - Sylvester matrix $\rightsquigarrow$ Macaulay matrices (exponential size)
- s polynomials $> n+1$ variables $\rightsquigarrow$ several polynomials needed

More generally

- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$ $\rightsquigarrow$ a unique resultant polynomial
  - Sylvester matrix $\rightsquigarrow$ Macaulay matrices (exponential size)
- s polynomials $> n + 1$ variables $\rightsquigarrow$ several polynomials needed
- s polynomials $< n + 1$ variables $\rightsquigarrow$ trivial

- $f_1, \dots, f_{n+1} \in \mathbb{K}[X_0, \dots, X_n]$ ⇝ a unique resultant polynomial
  - Sylvester matrix ⇝ Macaulay matrices (exponential size)
- s polynomials $>$ $n + 1$ variables ⇝ several polynomials needed
- s polynomials $<$ $n + 1$ variables ⇝ trivial

RESULTANT$_{\mathbb{K}}$

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

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

Upper bounds

Theorem

Let $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n]$. Then

$$\forall \mathbf{a} \in \overline{\mathbb{K}}, f(\mathbf{a}) \neq 0 \iff \exists q_1, \ldots, q_s \in \mathbb{K}[\mathbf{X}], 1 = q_1 f_1 + \cdots + q_s f_s.$$

Theorem

Let $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n]$. Then

$$\forall a \in \overline{\mathbb{K}}, f(a) \neq 0 \iff \exists q_1, \ldots, q_s \in \mathbb{K}[\mathbf{X}], 1 = q_1 f_1 + \cdots + q_s f_s.$$

Sketch of an algorithm.

- Write $q_i = \sum_{|\alpha| \leqslant D} q_{i,\alpha} \mathbf{X}^\alpha$ where the $q_{i,\alpha}$'s are indeterminates.
- $\sum_i q_i f_i = 1$ is a **linear system** of D^n equations on sD^n variables.
- Linear systems can be solved in logarithmic space.
- Do not store the linear system, but compute entries on demand.

$\implies$ $\textsc{PolSys}_{\mathbb{K}}$ can be solved in space $\operatorname{poly}(n \log D, \log s)$.

$$\forall a \in \overline{\mathbb{K}},\ f(a) \neq 0 \iff \exists\ q_1, \ldots, q_s \text{ s.t. } 1 = q_1 f_1 + \cdots + q_s f_s.$$

Theorem [Kollár'88, Fitchas-Galligo'90]

The q_i's can be chosen such that $\deg(q_i) \leqslant \max(3, d)^n$.

$$\forall a \in \overline{\mathbb{K}},\ f(a) \neq 0 \iff \exists\ q_1, \ldots, q_s \text{ s.t. } 1 = q_1 f_1 + \cdots + q_s f_s.$$

Theorem [Kollár'88, Fitchas-Galligo'90]

The q_i's can be chosen such that $\deg(q_i) \leqslant \max(3, d)^n$.

Corollary

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_q$, $\textsc{PolSys}_{\mathbb{K}}$ belongs to PSPACE.

$$\forall a \in \overline{\mathbb{K}},\ f(a) \neq 0 \iff \exists\ q_1, \ldots, q_s \text{ s.t. } 1 = q_1 f_1 + \cdots + q_s f_s.$$

Theorem [Kollár'88, Fitchas-Galligo'90]

The q_i's can be chosen such that $\deg(q_i) \leqslant \max(3, d)^n$.

Corollary

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_q$, $\textsc{PolSys}_{\mathbb{K}}$ belongs to PSPACE.

More specifically, $\textsc{PolSys}_{\mathbb{K}} \in \mathsf{DSPACE}((n \log d \log s)^{\mathcal{O}(1)})$.

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 a gcd of n determinants of Macaulay matrices.
- Macaulay matrices can be represented by polynomial-size boolean circuits.
- The determinant can be computed in logarithmic space.

Theorem [Canny'87]

The resultant is computable in polynomial space.

Proof idea.

- The resultant can be expressed as a gcd of n determinants of Macaulay matrices.
- Macaulay matrices can be represented by polynomial-size boolean circuits.
- The determinant can be computed in logarithmic space.

Theorem [Koiran-Perifel'07]

The same holds true in Valiant's algebraic model of computation.

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

- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$, 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.

- $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_0, \ldots, X_n]$, 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 $\mathbf{X}^{\alpha}$ represents

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

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

- Resultant : GCD of the determinants of n Macaulay matrices

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

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]

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 and $\mathcal{G}_{\mathcal{M}}^{x}$ its *graph of configurations*, with initial configuration c_i and 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 $\mathcal{M}$ accepts x;
- Let $A \simeq$ adjacency matrix of $\mathcal{G}_{\mathcal{M}}^{x}$: $\det(A) \neq 0 \iff \exists c_i \rightsquigarrow c_a$.

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

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 and $\mathcal{G}_{\mathcal{M}}^{x}$ its *graph of configurations*, with initial configuration c_i and 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 $\mathcal{M}$ accepts x;
- Let $A \simeq$ adjacency matrix of $\mathcal{G}_{\mathcal{M}}^{x}$: $\det(A) \neq 0 \iff \exists c_i \rightsquigarrow c_a$.

Theorem [Malod'11]

The same holds true in Valiant's algebraic model of computation.

Theorem [Koiran'96]

Under the Extended Riemann Hypothesis, $\text{PolSys}_{\mathbb{Z}}$ is in AM.

Theorem [Koiran'96]

Under the Extended Riemann Hypothesis, $\textsc{PolSys}_{\mathbb{Z}}$ is in AM.

- $L \in NP$ iff there exists $V \in P$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, (x, y) \in V.$$

Theorem [Koiran'96]

Under the Extended Riemann Hypothesis, $\textsc{PolSys}_{\mathbb{Z}}$ is in AM.

- $L \in \mathrm{NP}$ iff there exists $V \in \mathrm{P}$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, (x, y) \in V.$$

- $L \in \mathrm{MA}$ iff there exists $V \in \mathrm{P}$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, \mathrm{Pr}_{r \in \Sigma^{p(|x|)}}((x, y, r) \in V) \geqslant 2/3.$$

Theorem [Koiran'96]

Under the Extended Riemann Hypothesis, $\textsc{PolSys}_{\mathbb{Z}}$ is in AM.

- $L \in NP$ iff there exists $V \in P$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, (x, y) \in V.$$

- $L \in MA$ iff there exists $V \in P$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, \Pr_{r \in \Sigma^{p(|x|)}}((x, y, r) \in V) \geqslant 2/3.$$

- $L \in AM$ iff there exists $V \in P$ and a polynomial p s.t. for all x,

$$x \in L \iff \Pr_{r \in \Sigma^{p(|x|)}}(\exists y \in \Sigma^{p(|x|)} (x, r, y) \in V) \geqslant 2/3.$$

Theorem [Koiran'96]

Under the Extended Riemann Hypothesis, $\textsc{PolSys}_{\mathbb{Z}}$ is in AM.

- $L \in \mathsf{NP}$ iff there exists $V \in \mathsf{P}$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, (x, y) \in V.$$

- $L \in \mathsf{MA}$ iff there exists $V \in \mathsf{P}$ and a polynomial p s.t. for all x,

$$x \in L \iff \exists y \in \Sigma^{p(|x|)}, \Pr_{r \in \Sigma^{p(|x|)}}((x, y, r) \in V) \geqslant 2/3.$$

- $L \in \mathsf{AM}$ iff there exists $V \in \mathsf{P}$ and a polynomial p s.t. for all x,

$$x \in L \iff \Pr_{r \in \Sigma^{p(|x|)}}(\exists y \in \Sigma^{p(|x|)} (x, r, y) \in V) \geqslant 2/3.$$

$$\mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{AM}$$

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

- Let $f = (f_1, \ldots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$;
- Let $\pi_f(x)$ 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 $|\pi_f(x_0)| \leqslant A$;
- If f has a root in $\mathbb{C}$, then $|\pi_f(x_0)| \geqslant 8A(\log A + 3)$.

- Let $f = (f_1, \ldots, f_s)$, with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$;
- Let $\pi_f(x)$ 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 $|\pi_f(x_0)| \leqslant A$;
- If f has a root in $\mathbb{C}$, then $|\pi_f(x_0)| \geqslant 8A(\log A + 3)$.

Proof idea.

- Using Hilbert's Nullstellensatz, there exists $b \in \mathbb{Z}$ and $q_i \in \mathbb{Z}[\mathbf{X}]$ such that $q_1 f_1 + \cdots + q_s f_s = b$, with $\log b = \exp(s, d)$.
- Using effective quantifier elimination, consider a root α of f such that $\mathbb{Q}(\alpha) = \mathbb{Q}/\langle R \rangle$ where R is "small". Roots of R in $\mathbb{F}_p$ yield roots of f in $\mathbb{F}_p$. Use an Effective Chebotarev Density Theorem (ERH) to prove that R has "many" roots.

Theorem

Let U be a universe and $\{S_x \subseteq U : x \in \Sigma^\star\}$ a collection of sets s.t. for all x, either $|S_x| \leqslant \alpha|U|$ or $|S_x| \geqslant 4\alpha|U|$, and $S_x \in \mathrm{NP}$.
Then the following problem is in AM: Given x, does $|S_x| \geqslant 4\alpha|U|$?

Theorem

Let U be a universe and $\{S_x \subseteq U : x \in \Sigma^\star\}$ a collection of sets s.t. for all x, either $|S_x| \leqslant \alpha|U|$ or $|S_x| \geqslant 4\alpha|U|$, and $S_x \in \mathrm{NP}$. Then the following problem is in AM: Given x, does $|S_x| \geqslant 4\alpha|U|$?

Proof idea.

- $4\alpha \simeq 1$: Arthur chooses $y \in U$ at random, and asks Merlin a certificate that $y \in S_x$. If $|S_x| \simeq |U|$, $\Pr(y \in S_x) \simeq 1$.
- $\alpha \ll 1$: Consider a set T of size $4\alpha|U|$ and a family of universal hash functions $h : U \to T$.
  1. Arthur chooses h and $t \in T$ at random.
  2. Merlin must return $y \in S_x$ s.t. $h(y) = t$, with a certificate

Theorem

Let U be a universe and $\{S_x \subseteq U : x \in \Sigma^\star\}$ a collection of sets s.t. for all x, either $|S_x| \leqslant \alpha|U|$ or $|S_x| \geqslant 4\alpha|U|$, and $S_x \in \mathrm{NP}$. Then the following problem is in AM: Given x, does $|S_x| \geqslant 4\alpha|U|$?

Proof idea.

- $4\alpha \simeq 1$: Arthur chooses $y \in U$ at random, and asks Merlin a certificate that $y \in S_x$. If $|S_x| \simeq |U|$, $\Pr(y \in S_x) \simeq 1$.
- $\alpha \ll 1$: Consider a set T of size $4\alpha|U|$ and a family of universal hash functions $h : U \to T$.
  1. Arthur chooses h and $t \in T$ at random.
  2. Merlin must return $y \in S_x$ s.t. $h(y) = t$, with a certificate

Proof ($\textsc{PolSys}_{\mathbb{Z}} \in \mathrm{AM}$). $U = \{p \leqslant x_0 : p \text{ is prime}\}$, $S_f = \pi_f(x_0)$.

Lower bounds

Proposition **[Folklore]**

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_p$, $\textsc{PolSys}_{\mathbb{K}}$ & $\textsc{HomPolSys}_{\mathbb{K}}$ are **NP-hard**.

Proposition **[Folklore]**

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_p$, $\textsc{PolSys}_{\mathbb{K}}$ & $\textsc{HomPolSys}_{\mathbb{K}}$ are NP-hard.

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

BoolSys

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

Proposition **[Folklore]**

For $\mathbb{K} = \mathbb{Z}$ or $\mathbb{F}_p$, $\textsc{PolSys}_{\mathbb{K}}$ & $\textsc{HomPolSys}_{\mathbb{K}}$ are NP-hard.

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

BoolSys

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

$\textsc{HomPolSys}_{\mathbb{K}}$

- 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
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

Proposition [Heintz-Morgenstern'93]

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

Proposition **[Heintz-Morgenstern'93]**

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

Proof. $\textsc{Partition}_{\mathbb{Z}}$:

Input: $S = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}$

Question: Does there exist $S' \subseteq S$, $\sum_{i \in S'} u_i = \sum_{j \notin S'} u_j$?

Proposition [Heintz-Morgenstern'93]

RESULTANT$_{\mathbb{Z}}$ is **NP-hard**.

Proof. PARTITION$_{\mathbb{Z}}$:

Input: $S = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}$

Question: Does there exist $S' \subseteq S$, $\sum_{i \in S'} u_i = \sum_{j \notin S'} u_j$?

$$\rightsquigarrow \left\{ \begin{array}{rcl} X_1^2 - X_0^2 & = & 0 \\ & \vdots & \\ X_n^2 - X_0^2 & = & 0 \\ u_1 X_1 + \cdots + u_n X_n & = & 0 \end{array} \right.$$

□

Proposition [Heintz-Morgenstern'93]

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

Proof. $\textsc{Partition}_{\mathbb{Z}}$:

Input: $S = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}$

Question: Does there exist $S' \subseteq S$, $\displaystyle\sum_{i \in S'} u_i = \sum_{j \notin S'} u_j$?

$$\rightsquigarrow \left\{ \begin{array}{rcl} X_1^2 - X_0^2 & = & 0 \\ & \vdots & \\ X_n^2 - X_0^2 & = & 0 \\ u_1 X_1 + \cdots + u_n X_n & = & 0 \end{array} \right.$$

□

Note. $\textsc{Partition}_{\mathbb{F}_p} \in \mathsf{P}$

- $\textsc{HomPolSys}_{\mathbb{F}_p}$ is NP-hard:

  \# homogeneous polynomials $\geqslant$ # variables

$\textsc{HomPolSys}_{\mathbb{K}}$

- 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
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

- $\text{HomPolSys}_{\mathbb{F}_p}$ is NP-hard:

  \# homogeneous polynomials $\geqslant$ # variables

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

$\text{HomPolSys}_{\mathbb{K}}$

- 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
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

- $\textsc{HomPolSys}_{\mathbb{F}_p}$ is NP-hard:

  \# homogeneous polynomials $\geqslant$ \# variables

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

$\textsc{HomPolSys}_{\mathbb{K}}$

- 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
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

- Define $g_i = \sum_{j=1}^{s} \alpha_{ij} f_j$, $0 \leqslant i \leqslant n$: $f(\mathbf{a}) = \mathbf{0} \implies g(\mathbf{a}) = \mathbf{0}$.

- Define $g_i = \sum_{j=1}^{s} \alpha_{ij} f_j$, $0 \leqslant i \leqslant n$: $f(\alpha) = 0 \implies g(\alpha) = 0$.
- **Effective Bertini Theorem:** There exists F of degree 3^{n+1} s.t. the reciprocal holds as soon as $F(\alpha) \neq 0$. [Krick-Pardo-Sombra'01]

- Define $g_i = \sum_{j=1}^{s} \alpha_{ij} f_j$, $0 \leqslant i \leqslant n$: $f(\mathbf{a}) = 0 \implies g(\mathbf{a}) = 0$.
- **Effective Bertini Theorem:** There exists F of degree 3^{n+1} s.t. the reciprocal holds as soon as $F(\boldsymbol{\alpha}) \neq 0$. [Krick-Pardo-Sombra'01]
- **Schwartz-Zippel Lemma:** [DeMillo-Lipton, Zippel, Schwartz, '78-'80]

$$\Pr_{\alpha \in \mathbb{F}_q^{s(n+1)}}(F(\boldsymbol{\alpha}) = 0) \leqslant \frac{\deg(F)}{|\mathbb{F}_q|}$$

- Define $g_i = \sum_{j=1}^{s} \alpha_{ij} f_j$, $0 \leqslant i \leqslant n$: $f(\mathbf{a}) = 0 \implies g(\mathbf{a}) = 0$.
- **Effective Bertini Theorem:** There exists F of degree 3^{n+1} s.t. the reciprocal holds as soon as $F(\boldsymbol{\alpha}) \neq 0$. **[Krick-Pardo-Sombra'01]**
- **Schwartz-Zippel Lemma:** **[DeMillo-Lipton, Zippel, Schwartz, '78-'80]**

$$\Pr_{\alpha \in \mathbb{F}_q^{s(n+1)}}(F(\boldsymbol{\alpha}) = 0) \leqslant \frac{\deg(F)}{|\mathbb{F}_q|}$$

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

- Define $g_i = \sum_{j=1}^{s} \alpha_{ij} f_j$, $0 \leqslant i \leqslant n$: $f(\alpha) = 0 \implies g(\alpha) = 0$.
- **Effective Bertini Theorem:** There exists F of degree 3^{n+1} s.t. the reciprocal holds as soon as $F(\boldsymbol{\alpha}) \neq 0$. [Krick-Pardo-Sombra'01]
- **Schwartz-Zippel Lemma:** [DeMillo-Lipton, Zippel, Schwartz, '78-'80]

$$\Pr_{\alpha \in \mathbb{F}_q^{s(n+1)}}(F(\boldsymbol{\alpha}) = 0) \leqslant \frac{\deg(F)}{|\mathbb{F}_q|}$$

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

- Define $g_i = \sum_{j=1}^{s} \alpha_{ij} f_j$, $0 \leqslant i \leqslant n$: $f(\mathbf{a}) = 0 \implies g(\mathbf{a}) = 0$.
- **Effective Bertini Theorem:** There exists F of degree 3^{n+1} s.t. the reciprocal holds as soon as $F(\boldsymbol{\alpha}) \neq 0$. [Krick-Pardo-Sombra'01]
- **Schwartz-Zippel Lemma:** [DeMillo-Lipton, Zippel, Schwartz, '78-'80]

$$\Pr_{\alpha \in \mathbb{F}_q^{s(n+1)}}(F(\boldsymbol{\alpha}) = 0) \leqslant \frac{\deg(F)}{|\mathbb{F}_q|}$$

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

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

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

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

$\textsc{HomPolSys}_{\mathbb{K}}$

- 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
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

- $\textsc{HomPolSys}_{\mathbb{F}_p}$ is NP-hard:

  \# homogeneous polynomials $\geqslant$ # variables

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

$\textsc{HomPolSys}_{\mathbb{K}}$

- 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 $f_1, \ldots, f_n$
  - $X_0 \cdot (X_i + X_0)$
  - $X_0 \cdot (X_i + X_j)$ $f_{n+1}, \ldots, f_s$
  - $(X_i + X_0)^2 - (X_j + X_0) \cdot (X_k + X_0)$

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

New system

$$g(\mathbf{X}, \mathbf{Y}) = \left(\vphantom{\begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix}} \right.$$

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

New system

$$g(\mathbf{X}, \mathbf{Y}) = \left(\begin{array}{l} f_1(\mathbf{X}) \\ \quad \vdots \\ f_n(\mathbf{X}) \\ \\ \\ \\ \\ \end{array} \right. \qquad \text{(untouched)}$$

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

New system

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

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

New system

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

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

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

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

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

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

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

$(\mathbf{a}, \mathbf{b})$ 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 $a_i = \pm 1$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 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"

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

- 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.

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

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

- 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.

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

Main results

	Lower bound	Upper bound
$\mathbb{Z}$	NP-hard	AM
$\mathbb{F}_p$	NP-hard	PSPACE

	Lower bound	Upper bound
$\mathbb{Z}$	NP-hard	AM
$\mathbb{F}_p$	NP-hard	PSPACE

- Evaluation of the resultant in PSPACE

	Lower bound	Upper bound
$\mathbb{Z}$	NP-hard	AM
$\mathbb{F}_p$	NP-hard	PSPACE

- Evaluation of the resultant in PSPACE
- Ideal membership problem is EXPSPACE-complete [Mayr-Meyer'82]

  Input: $g, f_1, \ldots, f_s \in \mathbb{K}[\mathbf{X}]$

  Question: Does g belong to $\langle f_1, \ldots, f_s \rangle$?

	Lower bound	Upper bound
$\mathbb{Z}$	NP-hard	AM
$\mathbb{F}_p$	NP-hard	PSPACE

- Evaluation of the resultant in PSPACE
- Ideal membership problem is EXPSPACE-complete [Mayr-Meyer'82]

  Input: $g, f_1, \ldots, f_s \in \mathbb{K}[\mathbf{X}]$
  Question: Does g belong to $\langle f_1, \ldots, f_s \rangle$?

- PolSys$_{\mathbb{K}}$ is NP$_{\mathbb{K}}$ complete (BSS model)

Some open questions

- Reduce the gap between NP and PSPACE in positive characteristics

- Reduce the gap between NP and PSPACE in positive characteristics
- Derandomize Koiran's theorem: $\textsc{PolSys}_{\mathbb{Z}} \in \mathsf{NP}$?

Some open questions

- Reduce the gap between NP and PSPACE in positive characteristics
- Derandomize Koiran's theorem: $\textsc{PolSys}_{\mathbb{Z}} \in \mathrm{NP}$?
- NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?

Some open questions

- Reduce the gap between NP and PSPACE in positive characteristics
- Derandomize Koiran's theorem: $\textsc{PolSys}_{\mathbb{Z}} \in \mathsf{NP}$?
- NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?
- Complexity of solving sparse or lacunary polynomial systems?

Some open questions

- Reduce the gap between NP and PSPACE in positive characteristics
- Derandomize Koiran's theorem: $\textsc{PolSys}_{\mathbb{Z}} \in \mathsf{NP}$?
- NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?
- Complexity of solving sparse or lacunary polynomial systems?
- Complexity of root finding, especially:

  Input: $f_1, \dots, f_n \in \mathbb{K}[X_0, \dots, X_n]$, homogeneous
  Output: A root $\alpha \in \overline{\mathbb{K}}$ of f

  $\rightsquigarrow$ always a solution: PPAD, TFNP, …?

- Reduce the gap between NP and PSPACE in positive characteristics
- Derandomize Koiran's theorem: $\textsc{PolSys}_{\mathbb{Z}} \in \mathrm{NP}$?
- NP-hardness for degree-2 polynomial systems in $\mathbb{F}_p$?
- Complexity of solving sparse or lacunary polynomial systems?
- Complexity of root finding, especially:

  Input: $f_1, \dots, f_n \in \mathbb{K}[X_0, \dots, X_n]$, homogeneous
  Output: A root $\alpha \in \overline{\mathbb{K}}$ of f

  $\rightsquigarrow$ always a solution: PPAD, TFNP, …?

Thank you!