Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case

by Jérémy Berthomieu[abc], Jean-Charles Faugère[cab], Ludovic Perret[abc]

[a]. Sorbonne Universités, Univ Paris 06, Équipe PolSys, LIP6, Paris

[b]. CNRS, UMR 7606, LIP6, Paris

[c]. INRIA, Équipe PolSys, Centre Paris – Rocquencourt, Paris

JNCF 2014 – Luminy
Jeudi 6 Novembre 2014

IP1S: Isomorphism of Polynomials with One Secret [Patarin, 1996]

Input: $\boldsymbol{x} = (x_1, \ldots, x_n), (\boldsymbol{f} = (f_1, \ldots, f_m), \boldsymbol{g} = (g_1, \ldots, g_m)) \in \mathbb{K}[\boldsymbol{x}]^m \times \mathbb{K}[\boldsymbol{x}]^m$.

Output: Find – if any – $A \in \mathrm{GL}_n(\mathbb{L})$, $\mathbb{K} \subseteq \mathbb{L}$, s.t.

$$\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{f}(A \cdot \boldsymbol{x}).$$

Example.

$\boldsymbol{f} = (x^2 + y^2, x\,y, y^2)$, $\boldsymbol{g} = (4\,x^2 + 9\,y^2, 6\,x\,y, 4\,x^2)$

$\Rightarrow A = \pm\begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}$.

Cryptography application.

Authentification scheme based on the difficulty of solving IP1S.

Computer Algebra related problem: Functional Decomposition Problem.

Input: $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{g} = (g_1, \ldots, g_m) \in \mathbb{K}[\boldsymbol{x}]^m$ and $d \in \mathbb{N}, d \mid \deg \boldsymbol{g}$.

Output: Compute $\boldsymbol{h} \in \mathbb{K}[\boldsymbol{x}]^s$ and $\boldsymbol{f} \in \mathbb{K}[\boldsymbol{y}]^m$, $\boldsymbol{y} = (y_1, \ldots, y_s)$, s.t. $\boldsymbol{g} = \boldsymbol{f} \circ \boldsymbol{h}$.

Definition.

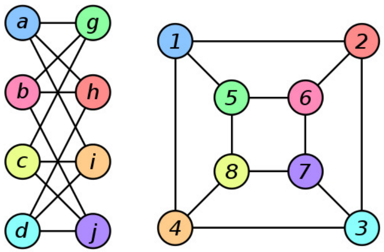
$G \simeq H \iff \exists \sigma\colon V(G) \to V(H)$, a permutation s.t.

$\forall u, v \in V(G), (u, v) \in E(G) \iff (\sigma(u), \sigma(v)) \in E(H)$.

Theorem. [Agrawal, Saxena, 2006]

Graph Isomorphism $\rightsquigarrow$ Equivalence of cubic polynomials by a linear map.

Example.



$\rightsquigarrow$ Polynomial-time algorithm for `IP1S` seems challenging.

Definition.

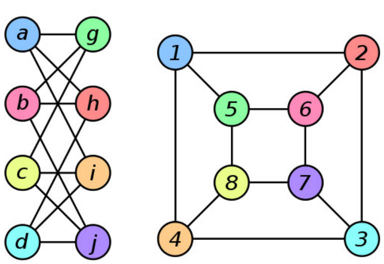
$G \simeq H \iff \exists \sigma\colon V(G) \to V(H)$, a permutation s.t.

$\forall u, v \in V(G), (u,v) \in E(G) \iff (\sigma(u), \sigma(v)) \in E(H)$.

Theorem. [Agrawal, Saxena, 2006]

Graph Isomorphism $\rightsquigarrow$ Equivalence of cubic polynomials by a linear map.

Example.



$$\boldsymbol{G}(\boldsymbol{x}) = \left(x_a x_g + x_a x_h + x_a x_i + x_b x_g + \cdots, \textstyle\sum_{\lambda=a}^{j} x_\lambda^3\right)$$
$$\boldsymbol{H}(\boldsymbol{x}) = \left(x_1 x_2 + x_1 x_4 + x_1 x_5 + x_2 x_3 + \cdots, \textstyle\sum_{\lambda=1}^{8} x_\lambda^3\right)$$

$\rightsquigarrow$ Polynomial-time algorithm for `IP1S` seems challenging.

Definition.

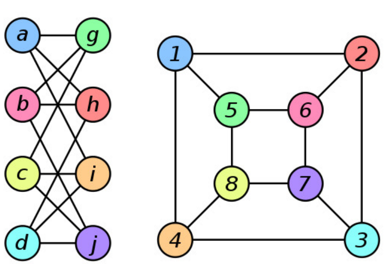
$G \simeq H \iff \exists \sigma\colon V(G) \to V(H)$, a permutation s.t.

$\forall u, v \in V(G), (u, v) \in E(G) \iff (\sigma(u), \sigma(v)) \in E(H)$.

Theorem. [Agrawal, Saxena, 2006]

Graph Isomorphism $\rightsquigarrow$ Equivalence of cubic polynomials by a linear map.

Example.



$$\boldsymbol{G}(\boldsymbol{x}) = \left(x_a\, x_g + x_a\, x_h + x_a\, x_i + x_b\, x_g + \cdots, \textstyle\sum_{\lambda=a}^{j} x_\lambda^3\right)$$
$$\boldsymbol{H}(\boldsymbol{x}) = \left(x_1\, x_2 + x_1\, x_4 + x_1\, x_5 + x_2\, x_3 + \cdots, \textstyle\sum_{\lambda=1}^{8} x_\lambda^3\right)$$
$$x_a\, x_g + x_a\, x_h + \cdots \sim x_1\, x_2 + x_1\, x_4 + \cdots$$

$\rightsquigarrow$ polynomials of the graph.

$\rightsquigarrow$ Polynomial-time algorithm for `IP1S` seems challenging.

Graph Isomorphism

Definition.

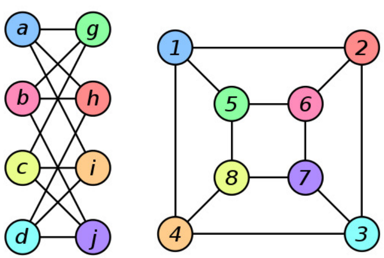
$G \simeq H \iff \exists \sigma : V(G) \to V(H)$, a permutation s.t.

$\forall u, v \in V(G), (u, v) \in E(G) \iff (\sigma(u), \sigma(v)) \in E(H)$.

Theorem. [Agrawal, Saxena, 2006]

Graph Isomorphism $\rightsquigarrow$ Equivalence of cubic polynomials by a linear map.

Example.



$$\boldsymbol{G}(\boldsymbol{x}) = \left(x_a x_g + x_a x_h + x_a x_i + x_b x_g + \cdots, \sum_{\lambda=a}^{j} x_\lambda^3\right)$$

$$\boldsymbol{H}(\boldsymbol{x}) = \left(x_1 x_2 + x_1 x_4 + x_1 x_5 + x_2 x_3 + \cdots, \sum_{\lambda=1}^{8} x_\lambda^3\right)$$

$$x_a x_g + x_a x_h + \cdots \sim x_1 x_2 + x_1 x_4 + \cdots$$

$\rightsquigarrow$ polynomials of the graph.

$\sum_{\lambda=a}^{j} x_\lambda^3 \sim \sum_{\lambda=1}^{8} x_\lambda^3 \rightsquigarrow \sigma$ permutation.

$\rightsquigarrow$ Polynomial-time algorithm for `IP1S` seems challenging.

Quadratic IP1S: State of the Art

- Gauss, $m = 1$, quadratic polynomials.
- Faugère, Perret, 2006:
  - Resolution with a Gröbner basis computation.
  - Good behaviour, unknown reason $\rightsquigarrow$ polynomial complexity?
- Bouillaget, Faugère, Fouque, Perret, 2011:
  - First complexity analysis.
- Macariot-Rat, Plût, Gilbert, 2013:
  - Polynomial-time algorithm for IP1S over $\mathbb{F}_q$ with homogeneous quadratic instances and $m = 2$.

Goal for the quadratic case.

$\rightsquigarrow$ Algorithm with proven polynomial complexity for any m.

Matrix representation.

Homogeneous polynomial f and $\operatorname{char}\mathbb{K}\neq 2$.

$\rightsquigarrow$ $f\simeq H$, Hessian matrix:

$$f=\alpha\,x_1^2+2\,\beta\,x_1\,x_2+\gamma\,x_2^2\ \simeq\ H=2\begin{pmatrix}\alpha & \beta\\ \beta & \gamma\end{pmatrix}.$$

Quadratic `IP1S` (Matrix case)

Input: $(\mathcal{H}=\{H_1,\ldots,H_m\},\mathcal{H}'=\{H_1',\ldots,H_m'\})\in(\mathbb{K}^{n\times n})^m\times(\mathbb{K}^{n\times n})^m$, symmetric.

Output: Find – if any – $A\in\mathrm{GL}_n(\mathbb{L})$, $\mathbb{K}\subseteq\mathbb{L}$, such that

$$\forall i, 1\leq i\leq m,\quad H_i'=A^{\mathrm{T}}\,H_i\,A.$$

Problem.

How to solve `IP1S` for quadratic polynomials with $m\geq 2$?

Linearization.

$A^{\mathrm{T}} H_i A = H_i'$, for all $i \geq 1$. If H_1 is invertible, then

$$A^{\mathrm{T}} H_1 A = H_1', \; A^{-1} H_1^{-1} H_i A = H_1'^{-1} H_i', \; \forall\, i > 1.$$

Otherwise, we combine the matrices to have an invertible matrix.

$\rightsquigarrow$ Instance of the Edmonds's problem.

Reasonable hypothesis.

- Carlitz, 1954: $\mathbb{P}(H_1 \in \mathrm{GL}_n(\mathbb{F}_q)) = \prod_{i=1}^{\lceil n/2 \rceil} \left(1 - \frac{1}{q^{2i-1}}\right) = 1 - \frac{1}{q} + O\left(\frac{1}{q^3}\right)$.
- Can be tested in randomized polynomial time.

Regular case.

$\exists \lambda_1, \ldots, \lambda_n \in \mathbb{K}$, $\sum_{i=1}^{m} \lambda_i H_i \in \mathrm{GL}_n(\mathbb{K})$.

Irregular case encodes difficult problems.

Theorem (First step): Randomized polynomial-time Algorithm

Input: $\mathcal{H} = \{H_1, \ldots, H_m\}, \mathcal{H}' = \{H_1', \ldots, H_m'\} \subseteq (\mathbb{K}^{n\times n})^m$, symmetric.

Output:

- $\textsc{Not Regular}$;
- $D = \mathrm{Diag}(d_1, \ldots, d_n), \tilde{\mathcal{H}} = \{D, \tilde{H}_2, \ldots, \tilde{H}_m\}, \tilde{\mathcal{H}}' = \{D, \tilde{H}_2', \ldots, \tilde{H}_m'\} \subseteq \mathrm{GL}_n(\mathbb{K})^m$, s.t. $A^{\mathrm{T}} H_i A = H_i'$, for some $A \in \mathrm{GL}_n(\mathbb{K}) \iff \tilde{A}^{\mathrm{T}} \tilde{H}_i \tilde{A} = \tilde{H}_i'$, with $\tilde{A}^{\mathrm{T}} D \tilde{A} = D$.

In this talk.

From now on, $D = \mathrm{Id}$, $A^{\mathrm{T}} A = \mathrm{Id} \iff A \in \mathcal{O}_n(\mathbb{K})$.

Linearization.

$$\text{If } A \in \mathcal{O}_n(\mathbb{K}), \quad A^{\mathrm{T}} H_i A = H_i' \iff A^{-1} H_i A = H_i' \iff H_i A = A H_i'.$$

Conjugacy problem by an orthogonal matrix.

$H_i\,A = A\,H_i'$, $\forall i, 1 \leq i \leq m$ with $A \in \mathcal{O}_n(\mathbb{K})$?

$\rightsquigarrow$ Problem almost linear, non-linear part: $A \in \mathcal{O}_n(\mathbb{K})$.

Theorem [Chistov, Ivanyos, Karpinski, 1997].

For $\bar{\mathbb{K}}$ algebraically closed,

$$\begin{gathered}\exists A \in \mathcal{O}_n(\bar{\mathbb{K}}),\quad H_i\,A = A\,H_i',\quad \forall i \\ \Big\Updownarrow \\ \exists Y \in \mathrm{GL}_n(\bar{\mathbb{K}}),\quad H_i\,Y = Y\,H_i',\quad \forall i.\end{gathered}$$

- Particular case of Edmonds's problem.
- Potential extension field!
- Polynomial bound on the degree?
- How to compute $A \in \mathcal{O}_n(\bar{\mathbb{K}})$?

- Linear equations: $H_i\,Y = Y\,H_i'$.
- Polynomial inequation: $\det Y \neq 0$.

Theorem [Chistov, Ivanyos, Karpinski, 1997] (Matrix case)

Let $\mathcal{H} = \{H_1, \ldots, H_m\}, \mathcal{H}' = \{H_1', \ldots, H_m'\} \subseteq \mathbb{K}^{n\times n}$ with $\mathbb{K} = \mathbb{F}_q$ or $\mathbb{K} = \mathbb{Q}(\alpha)$.
We can decide in deterministic polynomial time whether $\exists Y \in \mathrm{GL}_n(\mathbb{K})$ s.t.

$$H_i\,Y = Y\,H_i', \quad \forall i, 1 \leq i \leq m,$$

and exhibit such an element if one exists.

$\rightsquigarrow$ Easy randomized polynomial-time algorithm [Schwartz-Zippel].

- Solve the linear system.
- Pick up at random a solution.

What about $A^{\mathrm{T}}\,A = \mathrm{Id}$?

From Y, how to compute A s.t. $A^{\mathrm{T}}\,A = \mathrm{Id}$ and $H_i\,A = A\,H_i'$?

Proposition.

From $Y \in \mathrm{GL}_n(\mathbb{K})$ solution of $H_i\, Y = Y\, H_i'$,

$\rightsquigarrow$ $A = Y\, \sqrt{Y^{\mathrm{T}}\, Y}^{-1}$ solution of $H_i\, A = A\, H_i'$ and $A \in \mathcal{O}_n(\bar{\mathbb{K}})$.

Numerical computation $\rightsquigarrow$ Polynomial-time algorithm (Gantmacher, 1959).

Problem.

$A \in \mathcal{O}_n(\mathbb{K}) \quad \Longleftrightarrow \quad \sqrt{Y^{\mathrm{T}}\, Y} \in \mathrm{GL}_n(\mathbb{K})$.

$\rightsquigarrow$ Direct computation of $\sqrt{Y^{\mathrm{T}}\, Y}$ may yield an exponential degree extension!

Square root of a Jordan Normal Form.

Jordan block $J_{\lambda,d}=\begin{pmatrix}\lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda\end{pmatrix}\Rightarrow\sqrt{J_{\lambda,d}}=\begin{pmatrix}\sqrt{\lambda} & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & \sqrt{\lambda}\end{pmatrix}\in\mathbb{K}(\sqrt{\lambda})[J_{\lambda,d}]$.

$$Y^{\mathrm{T}}Y=P\,\mathrm{Diag}(J_{\lambda_1,d_1},\ldots,J_{\lambda_r,d_r})\,P^{-1}\Rightarrow\sqrt{Y^{\mathrm{T}}Y}=P\,\mathrm{Diag}\left(\sqrt{J_{\lambda_1,d_1}},\ldots,\sqrt{J_{\lambda_r,d_r}}\right)P^{-1}.$$

- $\sqrt{Y^{\mathrm{T}}Y}$ may be in an extension of degree $2\,n!$.
- Alternative method for finite fields:

Generalized Jordan Normal Form.

If $\lambda_1,\ldots,\lambda_s$ are conjugate with minimal polynomial $\mathcal{P}$ of companion matrix $C(\mathcal{P})$, then

$$\mathrm{Diag}(J_{\lambda_1,d},\ldots,J_{\lambda_s,d})\sim J_{\mathcal{P},d}=\begin{pmatrix}C(\mathcal{P}) & U & & \\ & \ddots & \ddots & \\ & & \ddots & U \\ & & & C(\mathcal{P})\end{pmatrix}\in\mathbb{K}^{ds\times ds},U=\begin{pmatrix}0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ 1 & 0 & \cdots & 0\end{pmatrix}\in\mathbb{K}^{d\times d}.$$

$$\Rightarrow\sqrt{J_{\mathcal{P},d}}=\begin{pmatrix}C(\mathcal{Q}) & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & C(\mathcal{Q})\end{pmatrix},\ \mathcal{Q}(x)\,\mathcal{Q}(-x)=\mathcal{P}(x^2).$$

If $\mathbb{K}=\mathbb{F}_q$, $\sqrt{J_{\mathcal{P},d}}$ is defined over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$.

Proposition.

We can compute in polynomial time $S, T \in \mathbb{L}^{n\times n}$, $\mathbb{K} \subseteq \mathbb{L}$, s.t.

$$S\,T^{-1} = A \in \mathcal{O}_n(\mathbb{L}), \quad A^{\mathrm{T}}\,H_i\,A = H_i',\ \forall i, 1 \leq i \leq m.$$

We can compute and test in polynomial time $S^{\mathrm{T}}\,H_i\,S = T^{\mathrm{T}}\,H_i'\,T$.

However, product $S\,T^{-1}$ may not be computed in polynomial time over $\mathbb{K}$.

$H_i\,Y = Y\,H_i'$, $\forall i$. If $Y^{\mathrm{T}}\,Y = P\begin{pmatrix}\sqrt{2} & 0 & 0\\ 0 & -\sqrt{2} & 0\\ 0 & 0 & 3\end{pmatrix}P^{-1}$, then

$$\begin{aligned}
S, T &= \begin{pmatrix}\mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\sqrt{3})\\ \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\sqrt{3})\\ \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\sqrt{3})\end{pmatrix},\\
S^{\mathrm{T}}, T^{\mathrm{T}}, T^{-1} &= \begin{pmatrix}\mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2})\\ \mathbb{K}(\mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2})\\ \mathbb{K}(\sqrt{3}) & \mathbb{K}(\sqrt{3}) & \mathbb{K}(\sqrt{3})\end{pmatrix},\\
S^{\mathrm{T}}\,H_i\,S, T^{\mathrm{T}}\,H_i'\,T &= \begin{pmatrix}\mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}, \mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}, \sqrt{3})\\ \mathbb{K}(\sqrt[4]{2}, \mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}, \sqrt{3})\\ \mathbb{K}(\sqrt[4]{2}, \sqrt{3}) & \mathbb{K}(\mathrm{i}\sqrt[4]{2}, \sqrt{3}) & \mathbb{K}(\sqrt{3})\end{pmatrix}
\end{aligned}$$

Result.

$\rightsquigarrow$ Each column of S and T (row of T^{-1}) is defined over an extension of $\mathbb{K}$ of degree at most $2\,n$, [Cai, 1994].

$\rightsquigarrow$ We can compute and check that $\mathcal{H}$ and $\mathcal{H}'$ are conjugate by an orthogonal matrix over $\mathbb{L}$ in polynomial time.

$H_i\,Y = Y\,H_i'$, $\forall i$. If $Y^{\mathrm{T}}\,Y = P \begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & -\sqrt{2} & 0 \\ 0 & 0 & 3 \end{pmatrix} P^{-1}$, then

$$
\begin{aligned}
S\,,T \;&=\; \begin{pmatrix} \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\sqrt{3}) \\ \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\sqrt{3}) \\ \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\sqrt{3}) \end{pmatrix}, \\
S^{\mathrm{T}}, T^{\mathrm{T}}, T^{-1} \;&=\; \begin{pmatrix} \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}) \\ \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) \\ \mathbb{K}(\sqrt{3}) & \mathbb{K}(\sqrt{3}) & \mathbb{K}(\sqrt{3}) \end{pmatrix}, \\
S^{\mathrm{T}}\,H_i\,S\,,T^{\mathrm{T}}\,H_i'\,T \;&=\; \begin{pmatrix} \mathbb{K}(\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}, \mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\sqrt[4]{2}, \sqrt{3}) \\ \mathbb{K}(\sqrt[4]{2}, \mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}, \sqrt{3}) \\ \mathbb{K}(\sqrt[4]{2}, \sqrt{3}) & \mathbb{K}(\mathrm{i}\,\sqrt[4]{2}, \sqrt{3}) & \mathbb{K}(\sqrt{3}) \end{pmatrix}
\end{aligned}
$$

$n = m$	20	30	40	50	60	70	80	90	100
Timings (Magma 2.19)	0.040	0.20	0.84	2.7	7.5	17	40	79	130

Table 1. Timings for solving IP1S over $\mathbb{F}_{65521}$ in s.

$n = m$	20	30	40	50	60	70	80	90	100
Timings (Magma 2.19)	0.010	0.030	0.080	0.25	0.68	1.4	3.2	6.25	16
Timings (M4RI)			0.010	0.030	0.06	0.14	0.27	0.51	0.91

Table 2. Timings for solving IP1S over $\mathbb{F}_2$ in s.

Application to cryptography.

- Complexity in $O(n^{2\omega})$ because of the linear system.
- If $m \geq 3$, for generic instances, linear system $H_i\, Y = Y\, H_i'$ yields Y with one free parameter (Schur's Lemma).
  - Find A by solving $Y^{\mathrm{T}}\, Y = \mathrm{Id}$.
- If $\mathbb{K} = \mathbb{F}_q$, in the worst case, $\sqrt{Y^{\mathrm{T}}\, Y} \in \mathrm{GL}_n(\mathbb{F}_{q^2})$.
  - Solves IP1S over $\mathbb{F}_{q^2}$.

Conclusion and Perspectives

- Polynomial-time algorithm for regular quadratic instances:
  - over $\mathbb{F}_q$ for odd q;
  - over any field of characteristic 0;
  - over $\mathbb{F}_q$ for even q in even dimension, under some conditions;
  - careful analysis of the degree of the extension.

- Irregular case to deal with: no invertible Hessian matrix,
  - work in progress ;
  - characteristic 2 in every dimension.
- Cubic and higher degree instances.
- What about `IP2S`: with $\boldsymbol{g}(\boldsymbol{x}) = B \cdot \boldsymbol{f}(A \cdot \boldsymbol{x})$, $B \in \mathrm{GL}_m(\mathbb{K})$?

Thank you for your attention!