Computing isomorphisms of projective varieties using Lie algebras

Mickaël Montessinos[1]

joint work with Wouter Castryck[2] Mingjie Chen[2] Péter Kutas[1,3] Jun Bo Lau[2] Alexander Lemmens[2]

[1]Eötvös Loránd University, Hungary

[2]KU Leuven, Belgium

[3]University of Birmingham, United Kingdom

Wednesday 12th August, 2026

AM-PQC 2026

Hips don't Lie

Fix a projective variety $X_0 \subset \mathbb{P}^N_{\mathbb{F}_q}$. X is *projectively equivalent* to X_0, denoted by $X \sim X_0$, if there exists $T \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that $TX = X_0$.

The projective equivalence problem

Given $X \sim X_0$, compute some T such that $TX = X_0$.

Example

The curve $C \subset \mathbb{P}^2_{\mathbb{F}_5}$ with equation $xz = y^2 + yz + z^2$ is projectivally equivalent to the conic $C_0 : y^2 = xz$ via

$$T = \begin{pmatrix} 1 & -3 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Indeed, setting $x = u - 3v$, $y = v - w$ and $z = w$, we get:

$$y^2 = xz \iff uw = v^2 + vw + w^2.$$

True Lies

- `Vero2`: A post-quantum protocol from the intersection of conics (Alzati, Di Tullio, Gyawali and Tortora, 2025). X_0 is a Veronese surface.
- `Vero3`: A key exchange protocol from the intersection of quadric surfaces (Di Tullio, Gyawali, 2023). X_0 is a Veronese threefold.
- `Grass`: A post-quantum signature scheme from the secant variety of the Grassmanian (Di Tullio, Gyawali, 2023). X_0 is a secant Grassmanian.

Theorem (Castryck, Chen, Kutas, Lau, Lemmens, M.)

- The security of the above protocols reduces heuristically to a projective equivalence problem with respect to the variety X_0.
- The projective equivalence problem to a Veronese variety over a finite field may be solved in polynomial time in the degree and size of the base field. (Known over $\mathbb{Q}$ from de Graaf, Harrison, Pílníková, Schicho (2006))

Little Lies

Other hard problem may be rephrased as a similar equivalence problem:

- The code equivalence problem.
- The Alternating Trilinear Form Equivalence Problem.

However, the attack does not apply vertbatim if the underlying Lie algebras involved are trivial.

Lies my teacher told me

Definition

A *Lie algebra* over a field k is a vector space L with a bilinear product $[\cdot,\cdot]\colon L^2 \to L$ satisfying the *Jacobi* condition

$$[a,[b,c]] + [c,[b,a]] + [b,[c,a]] = 0$$

Example

$\mathfrak{gl}_n(k)$ is the algebra of square matrices of degree n over k, with the Lie bracket product:

$$[A,B] = AB - BA$$

Definition

If L is a Lie algebra over k, a *representation* of L is a homomorphism $\rho\colon L \to \mathfrak{gl}_n(k)$.

A beautiful Lie

Let $X \subset \mathbb{P}_k^N$ be a projective variety.

Definition (optimised for succinctness)

The Lie algebra $L(X, k)$ is the set of matrices $M \in \mathrm{GL}_{N+1}(k)$ such that $M.x$ is tangent to the affine cone of X for all $x \in X$.

Intuitions

- If $TX_0 = X$, then $TL(X_0, \mathbb{F}_q)T^{-1} = L(X, \mathbb{F}_q)$.
- $L(X, k)$ comes with a representation $L(X, k) \to \mathfrak{gl}_{N+1}(k)$.
- $L(X, k)$ is defined by linear equations.
- $L(X, k)$ is the Lie algebra of the algebraic group

$$\{T \in \mathrm{GL}_{N+1}(k) \mid TX = X\}.$$

Love the way you Lie

Set $n, d \in \mathbb{N}$ and $N = \binom{n+d}{n} - 1$. Let (e_{ij}) be the canonical basis of $\mathfrak{gl}_{n+1}(\mathbb{F}_q)$.

Definition (Veronese variety)

The *Veronese embedding of dimension n and degree d* is the map

$$\nu_d^{(n)}: \begin{array}{ccc} \mathbb{P}^n & \longrightarrow & \mathbb{P}^N \\ (x_0 : x_1 : \cdots : x_n) & \longmapsto & (x_0^d : x_0^{d-1}x_1 : \ \ldots : x_n^d). \end{array}$$

The *Veronese variety* of dimension n and degree d is $\nu_d^{(n)}(\mathbb{P}^n_{\mathbb{F}_q})$.

The Lie algebra of the Veronese variety

Let $X = \nu_d^{(n)}$. Assuming $p \nmid d$, we have an isomorphism

$$\rho_d: \begin{array}{ccc} \mathfrak{gl}_{n+1}(\mathbb{F}_q) & \to & L(X, \mathbb{F}_q) \\ e_{ij} & \mapsto & \left(P \mapsto x_i \frac{\partial P}{\partial x_j}\right). \end{array}$$

Required property

If $TL(X,k)T^{-1} = L(X_0,k)$, then $TX = X_0$.

Algorithm

Input: Equations for X.

Output: $T \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that $TX_0 = X$.

1. Compute $L(X, \mathbb{F}_q)$.
2. Compute an isomorphism $\varphi \colon L(X, \mathbb{F}_q) \to L(X_0, \mathbb{F}_q)$.
3. Post-compose φ with some automorphism of $L(X_0, \mathbb{F}_q)$.
4. Find $T \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that conjugation by T induces the map φ.

House of Lies

Let $X = \nu_d^{(n)}(\mathbb{P}^{n+1}_{\mathbb{F}_q})$, with d coprime to q, and q odd or $n > 1$.

$\mathrm{Aut}(\mathfrak{gl}_{n+1}(\mathbb{F}_q))$

The automorphism group of $\mathfrak{gl}_{n+1}(\mathbb{F}_q)$ is generated by the following elements:

1. $c_U : x \mapsto UxU{-}1$, where $U \in \mathrm{GL}_{n+1}(\mathbb{F}_q)$.
2. $\tau : x \mapsto -x^t$.
3. $h_\lambda : x \mapsto x + \lambda \mathrm{Tr}(\mathrm{M}) I_{n+1}$, with $\lambda \in \mathbb{F}_q \setminus \{-1\}$.

Getting the right automorphism

1. For $U \in \mathrm{GL}_{n+1}(\mathbb{F}_q)$, there exists $V \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that $\rho_d(c_U(x)) = V\rho_d(x)V^{-1}$.
2. For $\lambda \in \mathbb{F}_q \setminus \{-1\}$ and $\varepsilon \in \{0, 1\}$, there is an isomorphism

$$\begin{array}{ccc} \mathrm{Sp}(\rho_d(e_{1,1})) & \to & \mathrm{Sp}(\rho_d \circ h_\lambda \circ \tau^\varepsilon(e_{1,1})) \\ t & \mapsto & (-1)^\varepsilon t + \lambda d \end{array}$$

Algorithm

Input: An isomorphism $\varphi\colon L(X, \mathbb{F}_q) \to L(X_0, \mathbb{F}_q)$.

Output: An automorphism ψ of $L(X_0, \mathbb{F}_q)$ such that $\varphi \circ \psi$ is induced by an inner automorphism of $\mathfrak{gl}_{N+1}(\mathbb{F}_q)$.

1. Compute $\mathrm{Sp}(\rho_d(e_{1,1}))$ and $\mathrm{Sp}(\varphi^{-1}(\rho_d(e_{1,1})))$.
2. Interpolate ε and λ such that $x \mapsto (-1)^{\varepsilon} x + \lambda d$ is a mulciplicity-preserving bijection between the two sets.
3. Output $\rho_d \circ h_\lambda \circ \tau^{\varepsilon} \circ \rho_d^{-1}$.

No Lie

More details in the eprint:

https://ia.cr/2026/351

Implementation in Magma:

https://gitlab.com/Mickanos/equivalence-to-veronese-varieties