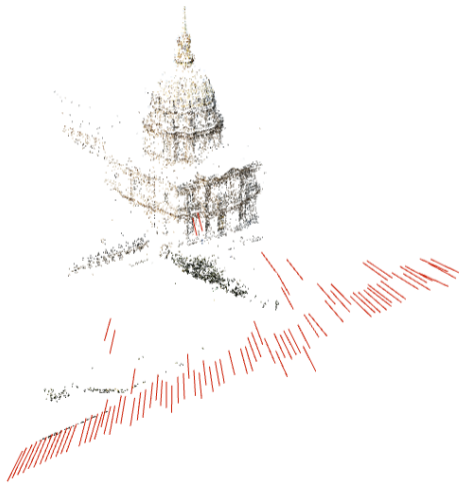


# *Numerically Computing Galois Groups of Minimal Problems*



Tim Duff

University of Missouri - Columbia

ISSAC 2025, July 28

CIMAT, Guanajuato Mexico

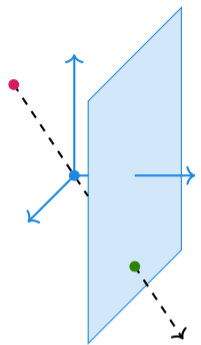
# Overview

The goal of this talk is to explain an unlikely intersection of three subjects:

1. *Computer vision* (mainly, minimal problems)
2. *Galois theory* for polynomial systems
3. *Numerical continuation methods* for solving these systems.

I'll also spend a large amount of time motivating the study of *minimal problems*.

For further reading and references: see the short article accompanying this tutorial (<https://arxiv.org/abs/2507.10407>, to appear in ISSAC 2025 Proceedings.)



Classical computer vision begins with the **pinhole camera** in standard coordinates, projecting a **3D point** onto the plane  $z = 1$ :

Not linear, but **projective linear**. Represented by a  $3 \times 4$  **camera matrix**

$$\begin{matrix} \begin{matrix} 0 & 1 \\ x=z \\ @y=zA \\ 1 \end{matrix} & \begin{matrix} 0 & 1 \\ x \\ @yA \\ z \end{matrix} & = & \begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix} & \begin{matrix} 0 & 1 \\ x \\ y \\ z \\ 1 \end{matrix} \end{matrix}$$

(Recall:  $n$ -dimensional projective space over the real numbers,

$$P^n = \mathbb{R}^{n+1} \setminus \{0\} / \sim = (\mathbf{x} \in \mathbb{R}^{n+1} \setminus \{0\}) / \sim$$

Points in  $\mathbb{R}^n$  have **homogeneous coordinates** in  $P^n$ .

If  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^{n+1}$  represent the same point in  $P^n$ ; we write  $\mathbf{x} \sim \mathbf{y}$ .)

$$\begin{matrix} \begin{matrix} 0 & 1 \\ x \\ @yA \\ z \end{matrix} \end{matrix} \begin{matrix} \mathbb{R}^3 \\ \mathbb{R}^2 \\ x=z \\ y=z \end{matrix}$$

## Anatomy of the pinhole camera

In general, we need coordinate systems for the camera ( $\mathbf{A} \in \mathbb{P} \text{Hom}(\mathbb{R}^4; \mathbb{R}^3) = \mathbb{P}^{11}$ ), the world points ( $\mathbf{q} \in \mathbb{P}^3$ ), and the image points ( $\mathbf{p} \in \mathbb{P}^2$ ).

A generic linear projection  $\mathbf{A} : \mathbb{P}^3 \rightarrow \mathbb{P}^2$  has 11 degrees of freedom.

Their physical meaning can be seen from RQ decomposition,

$$\mathbf{A} = \begin{pmatrix} 0 & s & x_0 \\ 0 & y & y_0 \\ 0 & 0 & 1 \end{pmatrix} \mathbf{R} | \mathbf{t} ;$$

where  $\mathbf{R} \in \text{SO}_3$  is a 3 × 3 rotation matrix,  $\mathbf{t}$  a translation vector.

The camera matrix  $\mathbf{R} | \mathbf{t}$  is said to be *calibrated*. It describes the position and orientation of the camera in space.

*Intrinsic parameters*  $x; s; x_0; y; y_0$  determine the camera's pixel width, image center, aspect ratio, skew, and focal length. They are often (not always!) known in practice.



## Perspective 3-Point Problem (aka P3P, Calibrated Resectioning, ...)

**Given:** 3D points  $\mathbf{q}_1; \mathbf{q}_2; \mathbf{q}_3 \in \mathbb{P}^3$  and matching 2D points  $\mathbf{p}_1; \mathbf{p}_2; \mathbf{p}_3 \in \mathbb{P}^2$

**Unknown:** calibrated camera  $(\mathbf{R} \ \mathbf{t})$  such that  $\mathbf{p}_i = (\mathbf{R} \ \mathbf{t})\mathbf{q}_i$  for  $i = 1; 2; 3$ :

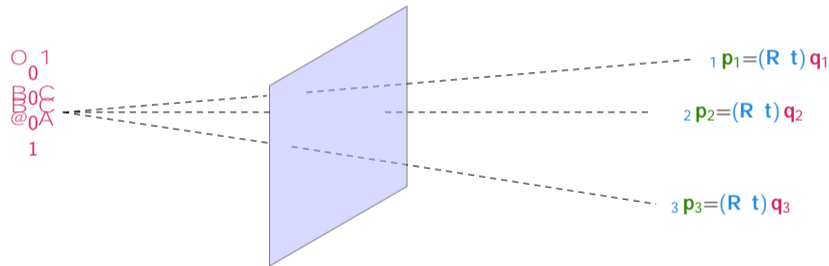
## Perspective 3-Point Problem (aka P3P, Calibrated Resectioning, ...)

**Given:** 3D points  $\mathbf{q}_1; \mathbf{q}_2; \mathbf{q}_3 \in \mathbb{P}^3$  and matching 2D points  $\mathbf{p}_1; \mathbf{p}_2; \mathbf{p}_3 \in \mathbb{P}^2$

**Unknown:** calibrated camera  $(\mathbf{R} \ \mathbf{t})$  such that  $\mathbf{p}_i = (\mathbf{R} \ \mathbf{t})\mathbf{q}_i$  for  $i = 1; 2; 3$ :

Choose projective representatives such that  $\mathbf{q}_i = [q_{i1} \ q_{i2} \ q_{i3} \ 1]^T$ ; and  $\mathbf{p}_i^T \mathbf{p}_i = 1$ :

Define (unknown) scalar *depths*  $z_1; z_2; z_3$  such that  $z_i \mathbf{p}_i = (\mathbf{R} \ \mathbf{t})\mathbf{q}_i$ :



Grunert (1847) derived 3 polynomial equations in 3 unknowns: for  $1 \leq i < j \leq 3$ :

$$z_i^2 + z_j^2 - 2 z_i z_j \mathbf{p}_i^T \mathbf{p}_j - (\mathbf{q}_i - \mathbf{q}_j)^T (\mathbf{q}_i - \mathbf{q}_j) = 0$$

For generic data  $(\mathbf{q}_1; \mathbf{q}_2; \mathbf{q}_3; \mathbf{p}_1; \mathbf{p}_2; \mathbf{p}_3)$ , this system has 8 (complex-valued) solutions.

**Universal problem of algebraic vision:** Let  $\gamma : X \rightarrow \mathbb{R}^m$  be a map of algebraic varieties, where  $X$  is a space of unknown states and  $\gamma(X) \subset \mathbb{R}^m$  is a space of idealized data. Given a measurement  $y$  of "true" data  $y = \gamma(x)$ , recover  $x \in X$  with  $\hat{x} \in X$ .

**Universal problem of algebraic vision:** Let  $\pi : X \rightarrow \mathbb{R}^m$  be a map of algebraic varieties, where  $X$  is a space of unknown states and  $\mathbb{R}^m$  is a space of idealized data. Given a measurement  $y$  of "true" data  $y = \pi(x)$ , recover  $x \in X$  with  $x \approx x$ .

**Example 1:** Perspective  $n$ -point (PnP / calibrated resectioning)

$$\text{PnP} : \text{SE}_3 \rightarrow \mathbb{R}^{2n}$$

$$(\mathbf{R} \mid \mathbf{t}) \mapsto (\Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_1); \dots; \Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_n))$$

where  $\Pi(x; y; z) = (x=z; y=z)$ :

**Universal problem of algebraic vision:** Let  $\pi : X \rightarrow \mathbb{R}^m$  be a map of algebraic varieties, where  $X$  is a space of unknown states and  $\mathbb{R}^m$  is a space of idealized data. Given a measurement  $y$  of "true" data  $y = \pi(x)$ , recover  $x \in X$  with  $x \approx x$ .

**Example 1:** Perspective  $n$ -point (PnP / calibrated resectioning)

$$\text{PnP} : \text{SE}_3 \rightarrow \mathbb{R}^{2n}$$

$$(\mathbf{R} \mid \mathbf{t}) \mapsto (\Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_1); \dots; \Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_n))$$

where  $\Pi(x; y; z) = (x=z; y=z)$ :

Three regimes:

**Universal problem of algebraic vision:** Let  $\pi : X \rightarrow \mathbb{R}^m$  be a map of algebraic varieties, where  $X$  is a space of unknown states and  $\mathbb{R}^m$  is a space of idealized data. Given a measurement  $y$  of "true" data  $y = \pi(x)$ , recover  $x \in X$  with  $x = x$ .

**Example 1:** Perspective  $n$ -point (PnP / calibrated resectioning)

$$\begin{aligned} \text{PnP} : \text{SE}_3 \times \mathbb{R}^{2n} \\ (\mathbf{R} \mid \mathbf{t}) \not\equiv (\Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_1); \dots; \Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_n)) \\ \text{where } \Pi(x; y; z) = (x=z; y=z): \end{aligned}$$

Three regimes:

- | **Underconstrained**,  $\dim(X) > \dim(\mathbb{R}^m) = m$ : eg. P1P / P2P

**Universal problem of algebraic vision:** Let  $\pi : X \rightarrow \mathbb{R}^m$  be a map of algebraic varieties, where  $X$  is a space of unknown states and  $\mathbb{R}^m$  is a space of idealized data. Given a measurement  $y$  of "true" data  $y = \pi(x)$ , recover  $x \in X$  with  $x = x$ .

**Example 1:** Perspective  $n$ -point (PnP / calibrated resectioning)

$$\text{PnP} : \text{SE}_3 \rightarrow \mathbb{R}^{2n}$$

$$(\mathbf{R} \mid \mathbf{t}) \mapsto (\Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_1); \dots; \Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_n))$$

where  $\Pi(x; y; z) = (x=z; y=z)$ :

Three regimes:

- | **Underconstrained**,  $\dim(X) > \dim(\mathbb{R}^m) = m$ : eg. P1P / P2P
- | **Overconstrained**,  $\dim(\mathbb{R}^m) < m$ : eg. P4P, P5P, ...

**Universal problem of algebraic vision:** Let  $\pi : X \rightarrow \mathbb{R}^m$  be a map of algebraic varieties, where  $X$  is a space of unknown states and  $\pi(X) \subset \mathbb{R}^m$  is a space of idealized data. Given a measurement  $y$  of "true" data  $y = \pi(x)$ , recover  $x \in X$  with  $x \approx x$ .

**Example 1:** Perspective  $n$ -point (PnP / calibrated resectioning)

$$\text{PnP} : \text{SE}_3 \rightarrow \mathbb{R}^{2n}$$

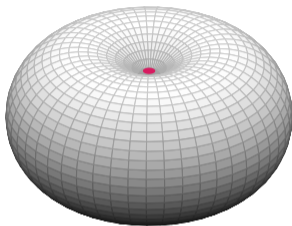
$$(\mathbf{R} \mid \mathbf{t}) \mapsto (\Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_1); \dots; \Pi((\mathbf{R} \mid \mathbf{t})\mathbf{q}_n))$$

where  $\Pi(x; y; z) = (x/z; y/z)$ :

Three regimes:

- | **Underconstrained**,  $\dim(X) > \dim(\pi(X)) = m$ : eg. P1P / P2P
- | **Overconstrained**,  $\dim(\pi(X)) < m$ : eg. P4P, P5P, ...
- | **Minimal / well-constrained**,  $\dim(X) = \dim(\pi(X)) = m$ : eg. P3P

**Underconstrained regime:** infinitely-many (complex) solutions, so exact recovery of  $(\mathbf{R}/\mathbf{t})$  is hopeless. Still, there may be *some* constraints worth studying.

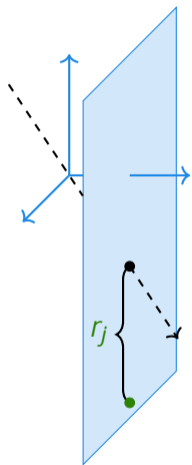


**Exercise:** For two generic 3D-2D point matches,  $(\mathbf{q}_1; \mathbf{p}_1); (\mathbf{q}_2; \mathbf{p}_2)$ , viewed by some calibrated camera  $\mathbf{A} = (\mathbf{R}/\mathbf{t})$ , show that the *camera center*  $[\ker \mathbf{A}] \supseteq \mathbb{P}^3$ , where

$$\ker \mathbf{A} = \text{span} \begin{matrix} \mathbf{R}^T \mathbf{t} \\ 1 \end{matrix}$$

must lie on a quartic surface with two singular points at the  $\mathbf{q}_i$ , and the equation of this surface is *independent* of the camera orientation  $\mathbf{R}$ .

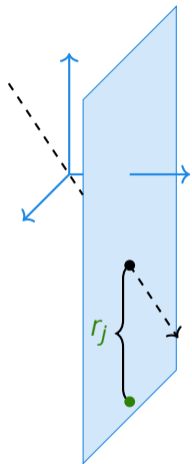
**Overconstrained regime:** again, exact recovery is hopeless. One must choose some objective to minimize, eg. the *reprojection error*,



$$\min_{\mathbf{A}} \sum_{j=1}^n \left( \frac{\mathbf{p}_{ij}[1]}{\mathbf{p}_{ij}[3]} \frac{\mathbf{A}[1:] \mathbf{q}_j}{\mathbf{A}[3:] \mathbf{q}_j} \right)^2 + \frac{\mathbf{p}_{ij}[2]}{\mathbf{p}_{ij}[3]} \frac{\mathbf{A}[2:] \mathbf{q}_j}{\mathbf{A}[3:] \mathbf{q}_j} \right) \quad (1)$$

*Local optimization* requires an initial guess. Minimal solvers help here!

**Overconstrained regime:** again, exact recovery is hopeless. One must choose some objective to minimize, eg. the *reprojection error*,



$$\min_{\mathbf{A}} \sum_{j=1}^n \left( \frac{\mathbf{p}_{ij}[1]}{\mathbf{p}_{ij}[3]} \frac{\mathbf{A}[1::] \mathbf{q}_j}{\mathbf{A}[3::] \mathbf{q}_j} \right)^2 + \frac{\mathbf{p}_{ij}[2]}{\mathbf{p}_{ij}[3]} \frac{\mathbf{A}[2::] \mathbf{q}_j}{\mathbf{A}[3::] \mathbf{q}_j} \quad (1)$$

*Local optimization* requires an initial guess. Minimal solvers help here!

*Global optimization* is oftentimes impractical...

**Conjecture (Connelly-D- Loucks-Tavitas, Math. Comp. '24)**

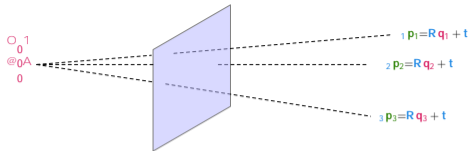
*For uncalibrated cameras with  $n = 6$  measurements, the number of complex-valued regular critical points of (1) equals*

$$(80=3)n^3 - 368n^2 + (5068=3)n - 2580:$$

**(Open)** How many critical points if  $\mathbf{A}$  is constrained to be calibrated?

## Minimal regime (P3P cont.)

Given a solution  $(\mathbf{p}_1; \mathbf{p}_2; \mathbf{p}_3)$   
to Grunert's equations,



$$\|\mathbf{p}_i\|^2 + \|\mathbf{p}_j\|^2 - 2\mathbf{p}_i^T \mathbf{p}_j = \|\mathbf{q}_i - \mathbf{q}_j\|^2 = (\mathbf{q}_i - \mathbf{q}_j)^T (\mathbf{q}_i - \mathbf{q}_j); \quad 1 \leq i < j \leq 3; \quad \mathbf{q}_i \in \mathbb{R}^3;$$

we can recover the calibrated camera  $(\mathbf{R} / \mathbf{t}) \in \text{SE}_3$  as follows:

$$\mathbf{R} = \mathbf{P}\mathbf{Q}^{-1}; \quad \text{where}$$

$$\mathbf{P} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \mathbf{p}_3 \\ \mathbf{p}_1 & \mathbf{p}_2 & \mathbf{p}_3 \end{pmatrix} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 \\ \mathbf{p}_1 & \mathbf{p}_3 \end{pmatrix} \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_3 \end{pmatrix}^{-1}$$

$$\mathbf{Q} = \begin{pmatrix} \mathbf{q}_1 & \mathbf{q}_2 & \mathbf{q}_3 \\ \mathbf{q}_1 & \mathbf{q}_2 & \mathbf{q}_3 \end{pmatrix} = \begin{pmatrix} \mathbf{q}_1 & \mathbf{q}_2 \\ \mathbf{q}_1 & \mathbf{q}_3 \end{pmatrix} \begin{pmatrix} \mathbf{q}_1 & \mathbf{q}_3 \end{pmatrix}^{-1}; \quad \text{and}$$

$$\mathbf{t} = \mathbf{p}_i - \mathbf{R}\mathbf{q}_i \quad (\text{any } i.)$$

*Minimal solvers* (eg. Ding et al., CVPR '23) can run in less than a microsecond!

Why does anybody care?

PnP assumes 3D-2D matches.  
Is that reasonable?

retrieved image (known 3D) vs query image (only 2D)

## Why does anybody care?

PnP assumes 3D-2D matches.  
Is that reasonable?

**Random Sampling and Consensus**, aka **RANSAC**, is used in computer vision for **outlier-robust** model-fitting.

## Why does anybody care?

PnP assumes 3D-2D matches.  
Is that reasonable?

**Random Sampling and Consensus**, aka **RANSAC**, is used in computer vision for **outlier-robust** model-fitting.

Over  $N$  trials:

## Why does anybody care?

PnP assumes 3D-2D matches.  
Is that reasonable?

Random Sampling and  
Consensus, aka RANSAC, is used  
in computer vision for  
**outlier-robust** model-fitting.

Over  $N$  trials:

1. Sample  $k$  out of  $n$  3D-2D  
matches, uniformly at random

## Why does anybody care?

PnP assumes 3D-2D matches.  
Is that reasonable?

Random Sampling and Consensus, aka RANSAC, is used in computer vision for **outlier-robust** model-fitting.

Over  $N$  trials:

1. Sample  $k$  out of  $n$  3D-2D matches, uniformly at random
2. (Somehow) solve PnP

retrieved image (known 3D) vs query image (only 2D)

## Why does anybody care?

PnP assumes 3D-2D matches.  
Is that reasonable?

Random Sampling and Consensus, aka RANSAC, is used in computer vision for **outlier-robust** model-fitting.

Over  $N$  trials:

1. Sample  $k$  out of  $n$  3D-2D matches, uniformly at random
2. (Somehow) solve PnP
3. Measure consensus of solutions on remaining samples, and keep the maximum-consensus solution

retrieved image (known 3D) vs query image (only 2D)

# RanSaC, analyzed

Assume we have the following:

## RanSaC, analyzed

Assume we have the following:

1.  $N$ , the number of trials,

## RanSaC, analyzed

Assume we have the following:

1.  $N$ , the number of trials,
2. a PkP solver,

## RanSaC, analyzed

Assume we have the following:

1.  $N$ , the number of trials,
2. a PkP solver,
3. a consensus criterion (depends on some threshold),

## RanSaC, analyzed

Assume we have the following:

1.  $N$ , the number of trials,
2. a PkP solver,
3. a consensus criterion (depends on some threshold),
4. a confidence  $\alpha \in (0; 1)$ ; the desired probability of obtaining an outlier-free sample of  $k$  matches after  $N$  trials.

## RanSaC, analyzed

Assume we have the following:

1.  $N$ , the number of trials,
2. a PkP solver,
3. a consensus criterion (depends on some threshold),
4. a confidence  $\delta \in (0; 1)$ ; the desired probability of obtaining an outlier-free sample of  $k$  matches after  $N$  trials.

Let  $p \in (0; 1)$  denote the fraction of erroneous matches, so that the probability of drawing an all-inlier sample in one trial is

$$P = \frac{\binom{pn}{k}}{\binom{n}{k}} \quad (2)$$

From our specification above, we should have

$$(1 - P)^N \leq \delta \implies N \geq \frac{\log(1 - \delta)}{\log(1 - P)} \quad (3)$$

# Minimal Solvers Maximize Sample Efficiency!

**Figure:** RanSaC trials needed to find an outlier-free subsample of size  $k$  with confidence  $s = :95$  from  $n \in [10; 100]$  total matches, and with  $p = :5$  outlier probability.

## Back to the P3P

$$\begin{aligned}x_1^2 + x_2^2 - 2 \mathbf{p}_1^T \mathbf{p}_2 - x_1 x_2 &= (\mathbf{q}_1 \quad \mathbf{q}_2)^T (\mathbf{q}_1 \quad \mathbf{q}_2); \\x_1^2 + x_3^2 - 2 \mathbf{p}_1^T \mathbf{p}_3 - x_1 x_3 &= (\mathbf{q}_1 \quad \mathbf{q}_3)^T (\mathbf{q}_1 \quad \mathbf{q}_3); \\x_2^2 + x_3^2 - 2 \mathbf{p}_2^T \mathbf{p}_3 - x_2 x_3 &= (\mathbf{q}_2 \quad \mathbf{q}_3)^T (\mathbf{q}_2 \quad \mathbf{q}_3): \end{aligned} \quad (4)$$

Three quadrics in three unknowns generally have  $2^3=8$  solutions.

This is indeed the case for the system above.

P3P is a non-minimal problem|in fact, it is even easier than solving 3 quadrics in 3 unknowns, because of  $\mathbf{A}=\mathbf{A}^T$ -symmetry

## Back to the P3P

$$\begin{aligned}x_1^2 + x_2^2 - 2 \mathbf{p}_1^T \mathbf{p}_2 - x_1 x_2 &= (\mathbf{q}_1 \quad \mathbf{q}_2)^T (\mathbf{q}_1 \quad \mathbf{q}_2); \\x_1^2 + x_3^2 - 2 \mathbf{p}_1^T \mathbf{p}_3 - x_1 x_3 &= (\mathbf{q}_1 \quad \mathbf{q}_3)^T (\mathbf{q}_1 \quad \mathbf{q}_3); \\x_2^2 + x_3^2 - 2 \mathbf{p}_2^T \mathbf{p}_3 - x_2 x_3 &= (\mathbf{q}_2 \quad \mathbf{q}_3)^T (\mathbf{q}_2 \quad \mathbf{q}_3): \end{aligned} \quad (4)$$

Three quadrics in three unknowns generally have  $3^3=27$  solutions.

This is indeed the case for the system above.

P3P is an easy minimal problem|in fact, it is even easier than solving 3 quadrics in 3 unknowns, because of  $\mathbf{z}=\mathbf{z}$ -symmetry

$$(\ x_1; \ x_2; \ x_3) \text{ solves (4)} \quad , \quad (\ x_1; \ x_2; \ x_3) \text{ solves (4)}$$

# Decomposing P3P

Consider the rational  $\mathbb{Z} = 2\mathbb{Z}$ -invariants

$$(1; 2; 3) = (1=3; 2=3; 3^2);$$

and set, for  $1 \leq i < j \leq 3$ ;

$$c_{ij} = 2p_i^T p_j; \quad d_{ij} = (q_i \quad q_j)^T (q_i \quad q_j):$$

Our system:

$$1^2 + 2^2 - 2 p_1^T p_2 = (q_1 \quad q_2)^T (q_1 \quad q_2);$$

$$1^2 + 3^2 - 2 p_1^T p_3 = (q_1 \quad q_3)^T (q_1 \quad q_3);$$

$$2^2 + 3^2 - 2 p_2^T p_3 = (q_2 \quad q_3)^T (q_2 \quad q_3):$$

# Decomposing P3P

Consider the rational  $\mathbb{Z} = 2\mathbb{Z}$ -invariants

$$(x_1; x_2; x_3) = (x_1 = x_3; x_2 = x_3; x_3^2);$$

and set for  $1 \leq i < j \leq 3$ ;

$$c_{ij} = 2p_i^T p_j; \quad d_{ij} = (q_i \quad q_j)^T (q_i \quad q_j):$$

Our system:

$$x_1^2 + x_2^2 + c_{12} x_1 x_2 = d_{12};$$

$$x_1^2 + x_3^2 + c_{13} x_1 x_3 = d_{13};$$

$$x_2^2 + x_3^2 + c_{23} x_2 x_3 = d_{23};$$

# Decomposing P3P

Consider the rational  $\mathbb{Z} = 2\mathbb{Z}$ -invariants

$$(x_1; x_2; x_3) = (x_1 = x_3; x_2 = x_3; x_3^2);$$

and set for  $1 \leq i < j \leq 3$ :

$$c_{ij} = 2p_i^T p_j; \quad d_{ij} = (q_i \quad q_j)^T (q_i \quad q_j):$$

Our system:

$$x_1^2 + x_2^2 + c_{12} x_1 x_2 = d_{12} x_3;$$

$$1 + x_1^2 + c_{13} x_1 = d_{13} x_3;$$

$$1 + x_2^2 + c_{23} x_2 = d_{23} x_3;$$

# Decomposing P3P

Consider the rational  $\mathbb{Z}=2\mathbb{Z}$ -invariants

$$(1; 2; 3) = (1=3; 2=3; 3^2);$$

and set for  $1 \leq i < j \leq 3$ ;

$$c_{ij} = 2p_i^T p_j; \quad d_{ij} = (q_i \quad q_j)^T (q_i \quad q_j):$$

Our system:

$$\begin{aligned} & 1^2 + 2^2 + c_{12} 1 2 = d_{12} 3; \\ d_{13} 1^2 + 2^2 + c_{12} 1 2 &= d_{12} 1 + 1^2 + c_{13} 1; \\ d_{23} 1^2 + 2^2 + c_{12} 1 2 &= d_{12} 1 + 2^2 + c_{23} 2; \end{aligned}$$

# Decomposing P3P

Consider the rational  $\mathbb{Z} = 2\mathbb{Z}$ -invariants

$$(1; 2; 3) = (1=3; 2=3; 3^2);$$

and set for  $1 \leq i < j \leq 3$ :

$$c_{ij} = 2p_i^T p_j; \quad d_{ij} = (q_i \quad q_j)^T (q_i \quad q_j):$$

Our system:

$$n \quad 1^2 + 2^2 - 2c_{12} 1 2 = d_{12} 3;$$

! linear in 3

$$\begin{cases} d_{13} 1^2 + 2^2 + c_{12} 1 2 = d_{12} 1 + 1^2 + c_{13} 1 ; \\ d_{23} 1^2 + 2^2 + c_{12} 1 2 = d_{12} 1 + 2^2 + c_{23} 2 \end{cases}$$

! intersection of two plane conics!

# Decomposing P3P | Summary

## Decomposing P3P | Summary

Instead of solving a degree-8 problem, we can:

1. First, solve a degree-4 problem,

$$\begin{aligned} & x_1^2 + x_2^2 - 2c_{12} x_1 x_2 = d_{12}^2; \\ d_{13} \quad & x_1^2 + x_2^2 + c_{12} x_1 x_2 = d_{12}^2 x_1 + x_1^2 + c_{13} x_1; \\ d_{23} \quad & x_1^2 + x_2^2 + c_{12} x_1 x_2 = d_{12}^2 x_1 + x_2^2 + c_{23} x_2; \end{aligned}$$

# Decomposing P3P | Summary

Instead of solving a degree-8 problem, we can:

1. First, solve a degree-4 problem,

$$\begin{aligned} & x_1^2 + x_2^2 - 2c_{12} x_1 x_2 = d_{12} x_3; \\ d_{13} x_1^2 + x_2^2 + c_{12} x_1 x_2 &= d_{12} x_1 + x_1^2 + c_{13} x_1; \\ d_{23} x_1^2 + x_2^2 + c_{12} x_1 x_2 &= d_{12} x_1 + x_2^2 + c_{23} x_2; \end{aligned}$$

2. Then, recover depths by solving a degree-2 problem,

$$\begin{aligned} x_1 &= d_{13} x_3; \\ x_2 &= d_{23} x_3; \\ x_3^2 &= d_{12} x_3; \end{aligned}$$

## Decomposing P3P | Summary

Instead of solving a degree-8 problem, we can:

1. First, solve a degree-4 problem,

$$\begin{aligned} & 1^2 + 2^2 - 2c_{12} \cdot 1 \cdot 2 = d_{12} \cdot 3; \\ d_{13} \cdot 1^2 + 2^2 + c_{12} \cdot 1 \cdot 2 &= d_{12} \cdot 1 + 1^2 + c_{13} \cdot 1; \\ d_{23} \cdot 1^2 + 2^2 + c_{12} \cdot 1 \cdot 2 &= d_{12} \cdot 1 + 2^2 + c_{23} \cdot 2; \end{aligned}$$

2. Then, recover depths by solving a degree-2 problem,

$$\begin{aligned} 1 &= 1 \cdot 3; \\ 2 &= 2 \cdot 3; \\ 3^2 &= 3; \end{aligned}$$

3. Finally, recover  $(R, j, t)$  from depths by solving a degree-1 problem.

Some natural next questions:

- | Do other minimal problems have such decompositions?
- | If yes, how to find / analyze them?
- | Do problems have optimal decompositions?

All of these questions can be addressed by computing the problem's Galois group

# Galois Groups

Let  $\pi : X \rightarrow Z$  be a minimal problem. By this, I mean a rational, dominant map between irreducible complex algebraic varieties of the same dimension.

Let  $\mathbb{C}(X)$  and  $\mathbb{C}(Z)$  denote the fields of rational functions on  $X$  and  $Z$ ; respectively.

The algebraic extension  $\mathbb{C}(X) = \mathbb{C}(Z)$  is finite of degree  $d > 0$ ; which equals the generic fiber size or degree of  $\pi$  (ie.  $\deg(\pi) = d$ ).

Let  $\overline{\mathbb{C}(X)}$  denote a normal closure of the extension  $\mathbb{C}(X) = \mathbb{C}(Z)$ .

**Definition:**  $\text{Gal}(\overline{\mathbb{C}(X)} = \mathbb{C}(Z))$  is the Galois group of:

# Galois Groups

Let  $f: X \rightarrow Z$  be a minimal problem. By this, I mean a rational, dominant map between irreducible complex algebraic varieties of the same dimension.

Let  $\mathbb{C}(X)$  and  $\mathbb{C}(Z)$  denote the fields of rational functions on  $X$  and  $Z$ ; respectively.

The algebraic extension  $\mathbb{C}(X)/\mathbb{C}(Z)$  is finite of degree  $d > 0$ ; which equals the generic fiber size or degree of  $f$  (ie.  $\deg(f) = d$ ).

Let  $\overline{\mathbb{C}(X)}$  denote a normal closure of the extension  $\mathbb{C}(X)/\mathbb{C}(Z)$ .

**Definition:**  $\text{Gal}(\overline{\mathbb{C}(X)}/\mathbb{C}(Z))$  is the Galois group of:

If you don't like this definition, you can instead think about monodromy.

# Monodromy Groups

Let  $f : X \rightarrow Z$  be a minimal problem of degree  $d$ :

There exists a dense, Zariski open  $U \subset Z$  over which the restricted map

$$f|_U : f^{-1}(U) \rightarrow U$$

is a  $d$ -sheeted covering of complex manifolds.

For any  $p \in U$ ; the monodromy group  $\text{Mon}(f|_U; p)$  acts on the fiber  $f^{-1}(p)$ .

# Monodromy Groups

Let  $\pi : X \rightarrow Z$  be a minimal problem of degree  $d$ :

There exists a dense, Zariski open  $U \subset Z$  over which the restricted map

$$\pi|_U : \pi^{-1}(U) \rightarrow U$$

is a  $d$ -sheeted covering of complex manifolds.

For any  $p \in U$ ; the monodromy group  $\text{Mon}(\pi|_U; p)$  acts on the fiber  $\pi^{-1}(p)$ .

**Example:** Recall that P3P is a minimal problem of degree 8

Let us describe the monodromy action...

Consider a 1-parameter family of systems

$$H(\mathbf{x}; t) = \begin{pmatrix} \dot{x}_1^2 + c_{12}(t)x_2 + d_{12}(t) \\ \dot{x}_2^2 + c_{13}(t)x_3 + d_{13}(t) \\ \dot{x}_3^2 + c_{23}(t)x_3 + d_{23}(t) \end{pmatrix} = \mathbf{0}$$

where  $\mathbf{p} = (c_{12}(0); \dots; d_{23}(0)) = (c_{12}(1); \dots; d_{23}(1)) \in \mathbb{U} \times \mathbb{C}^3 \times \mathbb{C}^3$ :

Suppose we have a solution  $\mathbf{x} \in \mathbb{C}^3$  at  $t = 0$ , ie.  $H(\mathbf{x}_0; 0) = \mathbf{0}$ :

The implicit function theorem constructs a local solution function

$$\mathbf{x}(t) = \mathbf{x}_0 + \int_0^t \frac{\partial H}{\partial \mathbf{x}}(\mathbf{x}(s); s) \mathbf{x}'(s) ds$$

In general,  $\mathbf{x}(0) \neq \mathbf{x}(1)$  because more than one solution exists!

The monodromy group  $\text{Mon}(\mathbb{U}; \mathbf{p})$  consists of all permutations on the solution set  $\mathcal{S}(\mathbf{p})$  that send  $\mathbf{x}(0)$  to  $\mathbf{x}(1)$  for each local solution function:

## P3P monodromy

If  $(t)$  is a local solution function, so is  $^0(t) = (t)$ . Since

$$(t) = {}^0(t) \quad 8t^2 \in [0; 1];$$

the monodromy group is not the full-symmetric group  $S_8$ . Any monodromy permutation must preserve a nontrivial partition of the solution set

$${}^1(p) = f_1; \quad 1g \text{ t f } 2; \quad 2g \text{ t f } 3; \quad 3g \text{ t f } 4; \quad 4g:$$

The group of all such permutations is the wreath product  $S_2 \circ S_4$ . Thus,

$$\text{Mon}( ; U; p) = S_2 \circ S_4$$

Surprisingly, this containment is strict!

# Calibrated Resectioning with Points and Lines

$$p;l : \mathbb{P}^3 \times \mathbb{P}^l \text{Gr}(\mathbb{P}^1; \mathbb{P}^3) \xrightarrow{SE_3} \mathbb{P}^3 \times \mathbb{P}^2 \times \mathbb{P}^l \text{Gr}(\mathbb{P}^1; \mathbb{P}^3) \times \text{Gr}(\mathbb{P}^1; \mathbb{P}^2) \xrightarrow{SE_3} \mathbb{P}^3 \times \mathbb{P}^2 \times \mathbb{P}^l \text{Gr}(\mathbb{P}^1; \mathbb{P}^3) \times \text{Gr}(\mathbb{P}^1; \mathbb{P}^2)$$

$$(q_1; \dots; q_i; \ell_1; \dots; \ell_l; (R, t)) \xrightarrow{SE_3} (q_i; (R, t)q_i; 1 \dots i; 3; \ell_j; \wedge^2(R, t)\ell_j; 1 \dots j) \xrightarrow{SE_3}$$

We get a branched cover when  $p+l = 3$ :

Previously (D., Korotynskiy, Pajdla, Regan, SIAM J. Appl. Alg. Geom., 2023), we numerically computed the following table of Galois/monodromy groups:

Problem	$p$	$l$	$\deg(p;l)$	$\text{Gal}(p;l)$	$\text{Deck}(p;l)$
P3P	3	0	8	$S_2 \circ S_4 \setminus A_8$	$S_2$
P2P1L	2	1	4	$S_2 \circ S_2$	$S_2$
P1P2L	1	2	8	$S_2 \circ S_4 \setminus A_8$	$S_2$
P3L	0	3	8	$S_8$	trivial

## Resectioning with Points and Lines (cont.)

Prior work (Kukelova et al., CVPR '16), (Ramalingam et al., ICRA '11) proposed degree-4 / degree-8 solvers for P2P1L / P1P2L. Although we do not theoretically prove that our solutions are of the lowest possible degrees, we believe...

Can the theoretical improvements suggested by Galois groups also be made practical? Yes|(D. Hraby, Pollefeys, CVPR 2024, arXiv 2404.16552).

Method	Avg.	Min	Max
P2P1L Ours	314	231	3061
P2P1L Kuk.	1861	1439	10102
P2P1L Ram.	8898	5805	49984
P1P2L Ours	504	364	4554
P1P2L Kuk.	1967	1484	12931

Table: Solver timings in nanoseconds

Method	Avg. $R_{\text{err}}$	Avg. $t_{\text{rel}}$
P2P1L Ours	5.3e-12	3.7e-10
P2P1L Kuk.	2.8e-05	2.0e-05
P2P1L Ram.	4.7e-07	2.3e-05
PP1P2L Ours	1.2e-07	2.0e-06
P1P2L Kuk.	3.3e-05	3.4e-05

Table: Average solver errors ( $R_{\text{err}}$  in radians.)

## A non-toy problem

A radial camera is a surjective projective linear map  $\mathbb{P}^3 \rightarrow \mathbb{P}^2$ :

Intuition: The usual pinhole camera  $\mathbb{P}^3 \rightarrow \mathbb{P}^2$  does not account for lens distortions. Usually, the distortion is radially-symmetric.

However, the space of **radial lines** through the image center forms a  $\mathbb{P}^1$ , and each radial line is invariant under distortion.

**Goal:** recover unknown 3D scene and cameras from matched 1D projections.

To obtain a metrically accurate reconstruction, we need 4 radial cameras  $A_1; \dots; A_4 \in \mathbb{P}(\mathbb{R}^2 \times \mathbb{R}^4)$ ; and to assume they are **re-calibrated** which means

$$A_i = \begin{bmatrix} r_{i1}^T & t_{i;1} \\ r_{i2}^T & t_{i;2} \end{bmatrix} \quad \text{where} \quad \|r_{i1}\| = \|r_{i2}\| = 1; \quad r_{i1}^T r_{i2} = 0:$$

Up to similarity transformation in  $\mathbb{R}^3$ ; we may assume

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}; \quad A_2 = \begin{bmatrix} r_{21}^T & 0 \\ r_{22}^T & 1 \end{bmatrix} :$$

This leaves  $0 + 3 + 5 + 5 = 13$  unknowns, and a **minimal problem**: given matches  $p_{i1}; p_{i2}; p_{i3}; p_{i4} \in \mathbb{P}^1$ ; and  $q_1; \dots; q_{13} \in \mathbb{P}^3$  and  $A_i$  as above such that

$$A_i q_j = p_{ij} \quad 8 \leq i \leq 4; \quad 1 \leq j \leq 13:$$

The number of complex solutions is **3584**

Can we do better?

## We can do better!

(Hruby, Korotynskiy, D., et. al, CVPR '23) reconstructs radial cameras by decomposing into subproblems of degree at most 28

The number 28 is the Galois width of a finite group / branched cover naturally associated to this reconstruction problem.

I will explain what this means.

# Galois width

Here is a simple model for an exact, algebraic algorithm:

1. Initialize  $F_0 = \mathbb{Q}$

# Galois width

Here is a simple model for an exact, algebraic algorithm:

1. Initialize  $F_0 = \mathbb{Q}$
2. For  $i = 1; \dots; m$ ; either
  - (i) do arithmetic in  $F_i = F_{i-1}$ ; OR

# Galois width

Here is a simple model for an exact, algebraic algorithm:

1. Initialize  $F_0 = \mathbb{Q}$
2. For  $i = 1; \dots; m$ ; either
  - (i) do arithmetic in  $F_i = F_{i-1}$ ; OR
  - (ii) compute a root of a polynomial: formally, extend the working field  $F_i = F_{i-1}(\alpha)$

# Galois width

Here is a simple model for an exact, algebraic algorithm:

1. Initialize  $F_0 = \mathbb{Q}$
2. For  $i = 1; \dots; m$ ; either
  - (i) do arithmetic in  $F_i = F_{i-1}$ ; OR
  - (ii) compute a root of a polynomial: formally, extend the working field  $F_i = F_{i-1}(\alpha)$
3. Output:  $\mathbb{Q} \subseteq F_m$

# Galois width

Here is a simple model for an exact, algebraic algorithm:

1. Initialize  $F_0 = \mathbb{Q}$
2. For  $i = 1; \dots; m$ ; either
  - (i) do arithmetic in  $F_i = F_{i-1}$ ; OR
  - (ii) compute a root of a polynomial: formally, extend the working field  $F_i = F_{i-1}(\alpha)$
3. Output:  $\mathbb{Q} \subseteq F_m$

## Definition

An *algorithm* computing an algebraic number  $\alpha \in \overline{\mathbb{Q}}$  is a finite tower of fields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_m \subseteq \overline{\mathbb{Q}} :$$

## Definition

The *Galois width* of an algebraic number  $\alpha \in \overline{\mathbb{Q}}$  is the quantity

$$\text{gw}(\alpha) = \min_{\substack{\text{algorithms} \\ \mathbb{Q} = F_0 \subseteq \dots \subseteq F_m \subseteq \overline{\mathbb{Q}}}} \max_{0 \leq i < m} [F_{i+1} : F_i] :$$

## Definition

The *Galois width* of an algebraic number  $\alpha \in \overline{\mathbb{Q}}$  is the quantity

$$\text{gw}(\alpha) = \min_{\substack{\text{algorithms} \\ \mathbb{Q} = F_0 \subset \dots \subset F_m \subset \overline{\mathbb{Q}}} } \max_{0 \leq i < m} [F_{i+1} : F_i] :$$

There is a parallel notion in the world of finite groups.

## Definition

The *Galois width* of a finite group  $G$  is the quantity

$$\text{gw}(G) = \min_{\substack{\text{subgroup chains} \\ \text{id} = H_m \subset \dots \subset H_0 = G}} \max_{0 \leq i < m} [H_i : H_{i+1}] :$$

## Theorem (D 25)

For any algebraic number  $\alpha \in \overline{\mathbb{Q}}$  with minimal polynomial  $p(x) \in \mathbb{Q}[x]$  and Galois group  $G = \text{Gal}(p(x))$ ; we have  $\text{gw}(\alpha) = \text{gw}(G)$ :

## Theorem (Properties of the Galois width (D '25))

Let  $G$  be any finite group.

- $\text{gw}(H) \leq \text{gw}(G)$  for any subgroup  $H \leq G$ :
- $\text{gw}(G) = \max(\text{gw}(N); \text{gw}(G/N))$  for any normal subgroup  $N \trianglelefteq G$ :
- For any composition series  $id = N_m \trianglelefteq N_{m-1} \trianglelefteq \dots \trianglelefteq N_0 = G$ ; we have

$$\text{gw}(G) = \max_{0 \leq i < m} \text{gw}(N_i/N_{i+1}):$$

- If  $G$  is simple, then

$$\text{gw}(G) = \min_{H < G} [G : H]:$$

- For any prime  $p$ ; we have  $\text{gw}(Z/pZ) = p$ :
- For any  $n \geq 1$ ; we have  $\text{gw}(S_n) = \text{gw}(A_n) = \begin{cases} 3 & \text{if } n = 4; \\ n & \text{else.} \end{cases}$