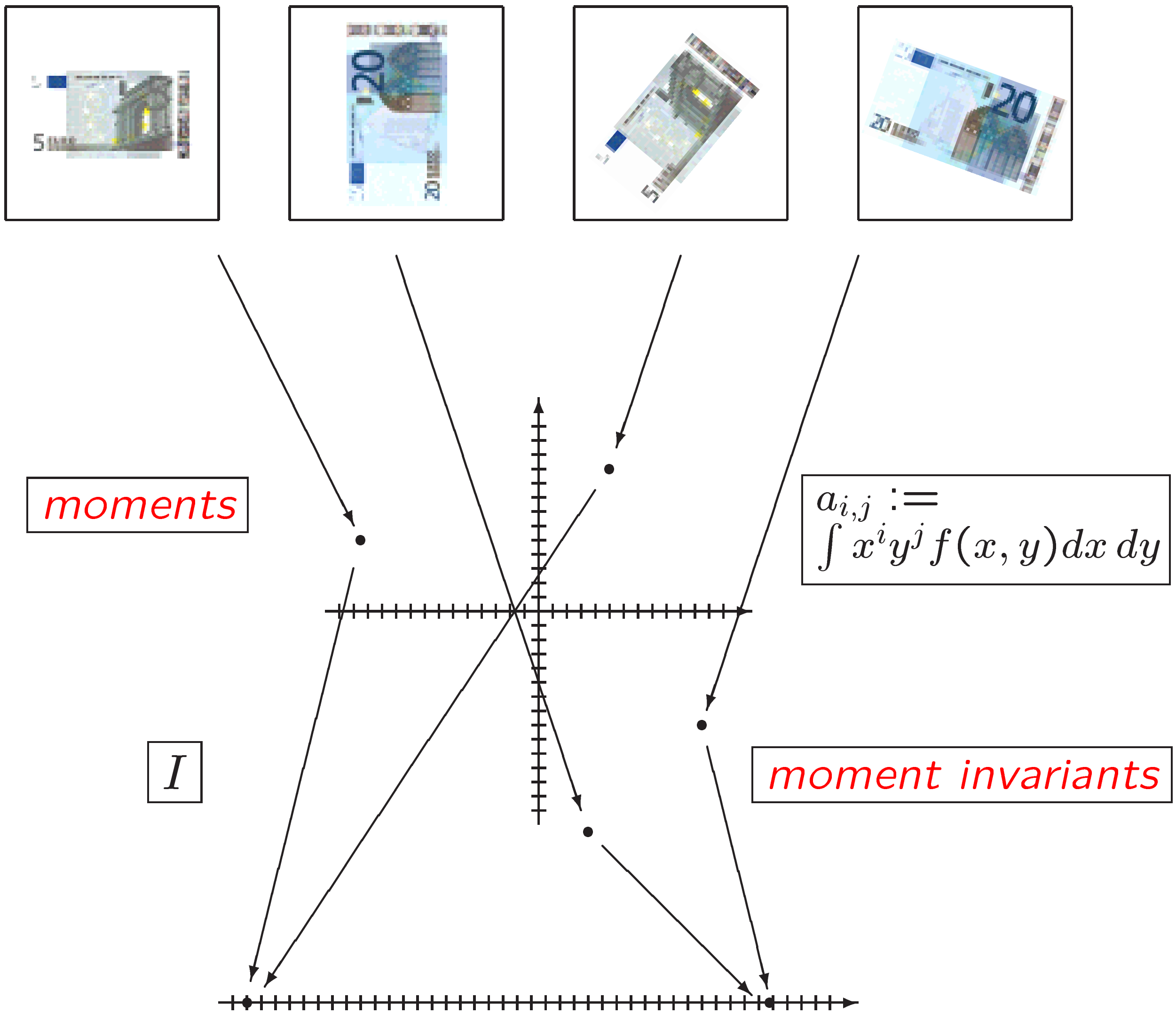
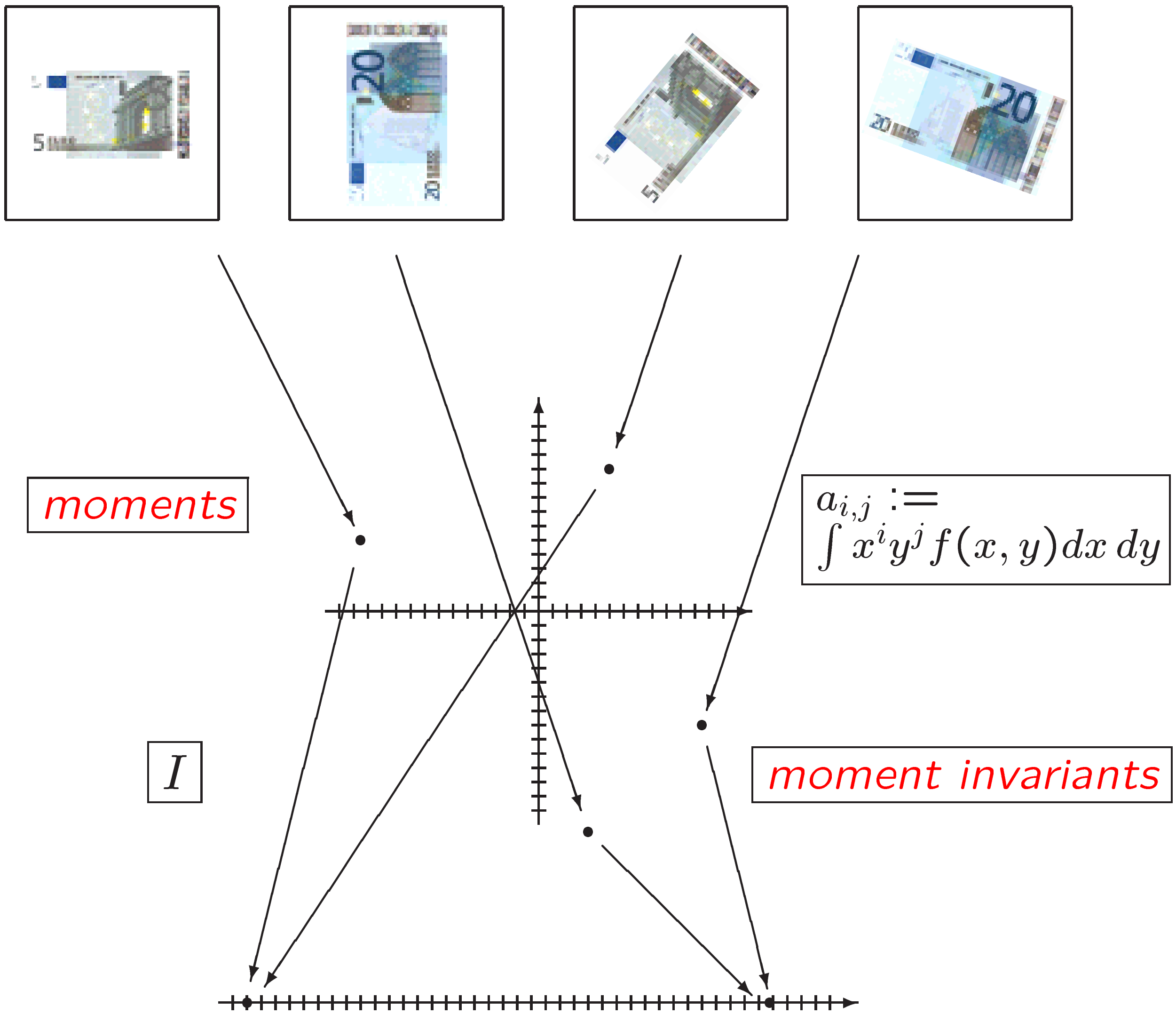
Moment invariants



Moment invariants

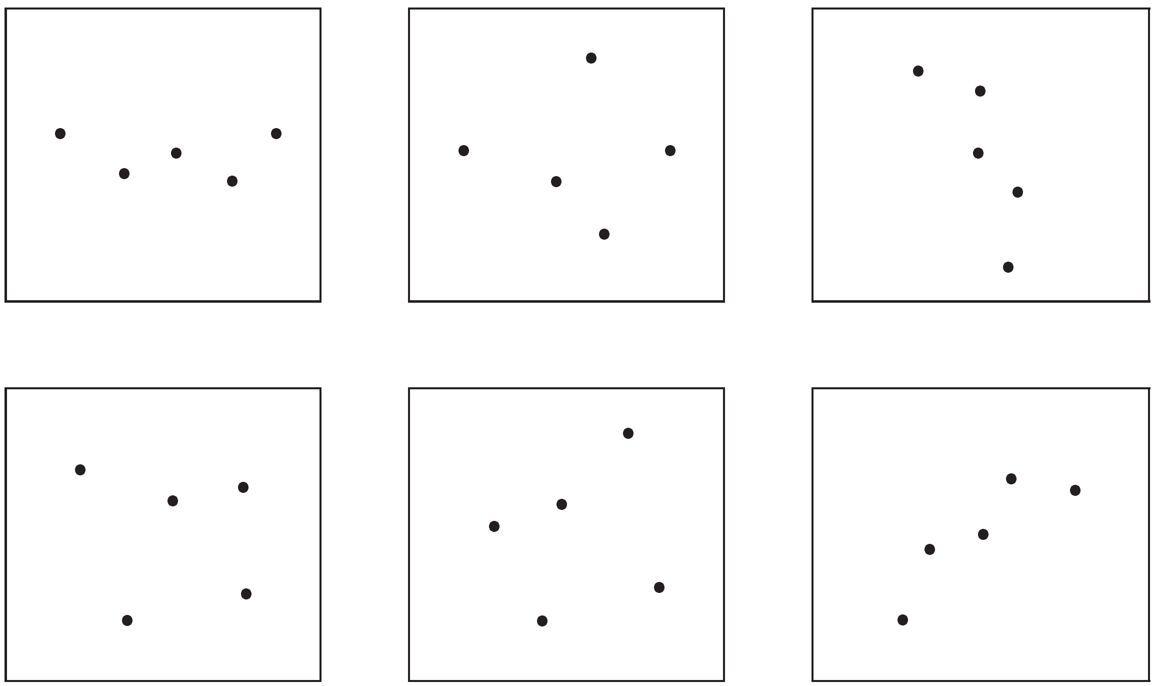


$$
\begin{aligned}
I_1 &= a_{00}(a_{20} + a_{02}) - a_{10}^2 - a_{01}^2, \\
I_2 &= a_{0,0}\left(a_{2,0}a_{0,2} - a_{1,1}^2\right) + 2a_{1,1}a_{1,0}a_{0,1} \\
&\quad - a_{1,0}^2 a_{0,2} - a_{0,1}^2 a_{2,0}
\end{aligned}
$$

are invariant under the Euclidean group AO_2.

Point configurations

Which objects are the "same"?



Strategy: Use $(S_5 \times \mathrm{AO}_2)$-invariants, i.e., functions $f\colon (\mathbb{R}^2)^5 \to \mathbb{R}$ with

$$f(P_1, \ldots, P_5) = f\left(\varphi(P_{\pi(1)}), \ldots, \varphi(P_{\pi(5)})\right)$$

for all $\varphi \in \mathrm{AO}_2$, $\pi \in S_5$.

Setting

G: linear algebraic group over $K = \bar{K}$.

X: affine G-variety.

$K[X]$: ring of regular functions.

$K[X]^G = \{f \in K[X] \mid f(g(x)) = f(x)$
$\forall x \in X, \ g \in G\}$: *invariant ring*.

Problems:

- Is $K[X]^G$ finitely generated? (Hilbert's 14th Problem)
- Find generators.

Setting

G: linear algebraic group over $K = \bar{K}$.

X: affine G-variety.

$K[X]$: ring of regular functions.

$K[X]^G = \{f \in K[X] \mid f(g(x)) = f(x) \; \forall x \in X, \; g \in G\}$: *invariant ring*.

Problems:

- Is $K[X]^G$ finitely generated? (Hilbert's 14th Problem)
- Find generators.
- Separating properties of invariants?

Proposition. Assume G reductive. Then $x, y \in X$ can be separated by invariants iff

$$\overline{G.x} \cap \overline{G.y} = \emptyset.$$

$|G| < \infty \Rightarrow$ all orbits can be separated.

Graph invariants

$X = V = \{K$-weighted graphs with n nodes$\}$,

$$V \cong K^{\binom{n}{2}}.$$

The symmetric group $G = S_n$ acts on V by permuting the nodes.
Suppose $K[V]^G = K[f_1, \dots, f_r]$. Then

$$g, g' \in V \text{ isomorphic} \quad \Leftrightarrow \quad f_i(g) = f_i(g')\ \forall i.$$

Embeddable into V:

- unweighted graphs;
- oriented graphs (with modified S_n-action);
- discretely weighted graphs;
- graph of distances between n points.

Graph invariants

$X = V = \{K$-weighted graphs with n nodes$\}$,

$$V \cong K^{\binom{n}{2}}.$$

The symmetric group $G = S_n$ acts on V by permuting the nodes.
Suppose $K[V]^G = K[f_1, \ldots, f_r]$. Then

$g, g' \in V$ isomorphic $\quad \Leftrightarrow \quad f_i(g) = f_i(g') \; \forall i.$

Embeddable into V:

- unweighted graphs;
- oriented graphs (with modified S_n-action);
- discretely weighted graphs;
- graph of distances between n points.

PROBLEM: Calculation only feasible for $n \leq 5$.

Distribution of distances

Idea: Use the *distribution* of distances.
Precisely: For $P_1, \ldots, P_n \in \mathbb{R}^m$ set $d_{i,j} := ||P_i - P_j||^2$ and form

$$F_{P_1,\ldots,P_n}(X) := \prod_{1 \leq i < j \leq n} \left(X - d_{i,j} \right).$$

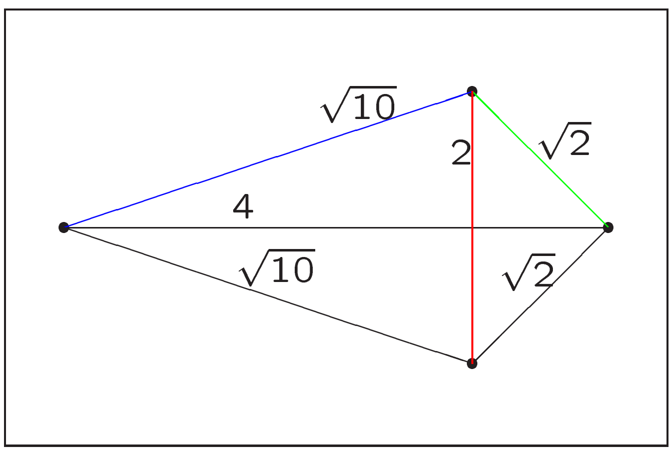
The coefficients of $F_{P_1,\ldots,P_n}(X)$ are invariant under $G := S_n \times \mathrm{AO}_m$. Do they separate G-orbits?

Distribution of distances

Idea: Use the *distribution* of distances. Precisely: For $P_1, \ldots, P_n \in \mathbb{R}^m$ set $d_{i,j} := ||P_i - P_j||^2$ and form

$$F_{P_1,\ldots,P_n}(X) := \prod_{1 \le i < j \le n} \left(X - d_{i,j} \right).$$

The coefficients of $F_{P_1,\ldots,P_n}(X)$ are invariant under $G := S_n \times \mathrm{AO}_m$. Do they separate G-orbits?

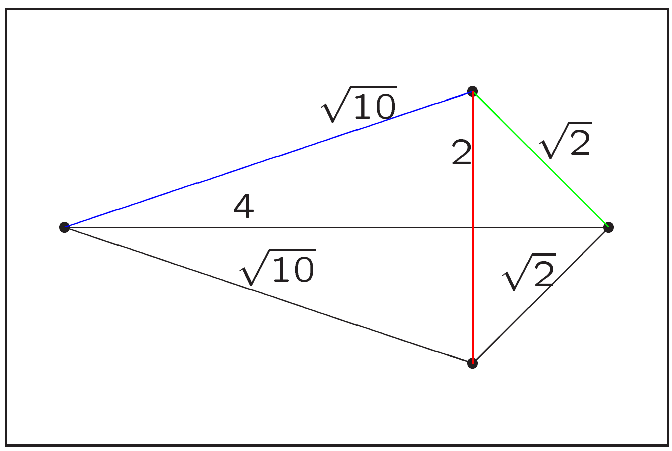


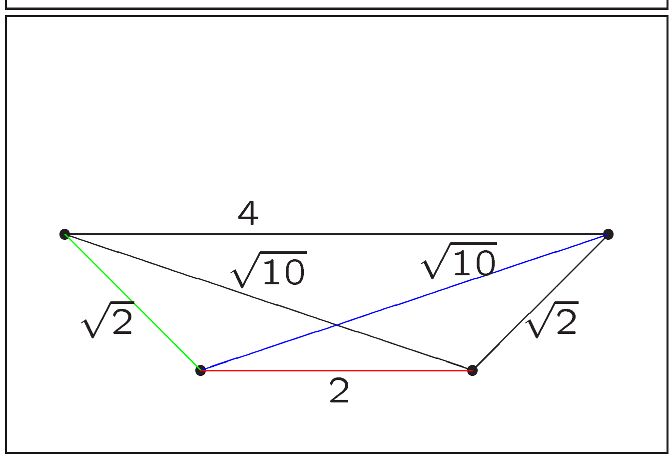
Distribution of distances

Idea: Use the *distribution* of distances. Precisely: For $P_1, \dots, P_n \in \mathbb{R}^m$ set $d_{i,j} := ||P_i - P_j||^2$ and form

$$F_{P_1,\dots,P_n}(X) := \prod_{1 \le i < j \le n} \left(X - d_{i,j}\right).$$

The coefficients of $F_{P_1,\dots,P_n}(X)$ are invariant under $G := S_n \times \mathrm{AO}_m$. Do they separate G-orbits?





Reconstructible n-point configurations

Definition. We call an n-point configuration $(P_1, \ldots, P_n) \in (\mathbb{R}^m)^n$ *reconstructible* if for all $(Q_1, \ldots, Q_n) \in (\mathbb{R}^m)^n$ with

$$F_{P_1,\ldots,P_n}(X) = F_{Q_1,\ldots,Q_n}(X)$$

there exist $g \in \mathrm{AO}_m(\mathbb{R})$ and $\pi \in S_n$ s.t.

$$Q_i = g(P_{\pi(i)}) \quad \text{for} \quad i = 1, \ldots, n.$$

Theorem (??, M. Boutin, Ke)**:** There exists a Zariski-open, dense subset $S \subseteq (\mathbb{R}^m)^n$ such that all n-point configurations from S are reconstructible.

Reconstructible n-point configurations

Definition. We call an n-point configuration $(P_1, \ldots, P_n) \in (\mathbb{R}^m)^n$ *reconstructible* if for all $(Q_1, \ldots, Q_n) \in (\mathbb{R}^m)^n$ with

$$F_{P_1,\ldots,P_n}(X) = F_{Q_1,\ldots,Q_n}(X)$$

there exist $g \in \mathrm{AO}_m(\mathbb{R})$ and $\pi \in S_n$ s.t.

$$Q_i = g(P_{\pi(i)}) \quad \text{for} \quad i = 1, \ldots, n.$$

Theorem (??, M. Boutin, Ke)**:** There exists a Zariski-open, dense subset $S \subseteq (\mathbb{R}^m)^n$ such that all n-point configurations from S are reconstructible.

Reconstruction from areas: The distribution of areas $a_{i,j,k}$ of triangles spanned by P_i, P_j, P_k $(1 \leq i < j < k \leq n)$ is $\left(S_n \times \mathrm{SL}_m^{\pm}\right)$-invariant, and again it separates a dense open subset of all orbits.

Derksen's algorithm (1999)

G: linearly reductive group, given as $G = \mathcal{V}(I_G)$, $I_G \subseteq K[t_1, \ldots, t_m]$.

$X = V$: linear representation, given by $A = (a_{i,j})$, $a_{i,j} \in K[t_1, \ldots, t_m]$.

1. Form the ideal

$$I_0 := \left(I_G\right) + \left(y_i - \sum_{j=1}^{n} a_{i,j} x_j \,\middle|\, i = 1, \ldots, n\right) \subseteq K[\underline{x}, \underline{y}, \underline{t}].$$

2. Compute generators $f_1, \ldots, f_r$ of

$$I := I_0 \cap K[\underline{x}, \underline{y}]$$

("*Derksen ideal*").

3. The $\mathcal{R}(f_i(\underline{x}, 0))$ generate $K[V]^G$.
(
$\mathcal{R}$: $K[V] \to K[V]^G$ is the *Reynolds operator*.)

Separating invariants

Definition. A subset $S \subseteq K[X]^G$ is called *separating* if for $x, y \in X$ we have

$$\exists\ f \in K[X]^G:\ f(x) \neq f(y) \quad \Rightarrow \quad \exists\ f \in S:\ f(x) \neq f(y).$$

Separating invariants

Definition. A subset $S \subseteq K[X]^G$ is called *separating* if for $x, y \in X$ we have

$$\exists\ f \in K[X]^G:\ f(x) \neq f(y) \quad \Rightarrow \quad \exists\ f \in S:\ f(x) \neq f(y).$$

Problem: Find separating invariants.
Find description of

$$\mathcal{D} := \{(x,y) \in X \times X \mid f(x) = f(y)\ \forall f \in K[X]^G\}.$$

Assume G reductive, $X = V$ linear representation.

Compute $I :=$ Derksen ideal. Form

$$J_0 := \left(h(\underline{x},\underline{z}), h(\underline{y},\underline{z}) \middle| h \in I\right) \subseteq K[\underline{x},\underline{y},\underline{z}]$$

and

$$J := J_0 \cap K[\underline{x},\underline{y}].$$

Then

$$\mathcal{D} = \mathcal{V}(J).$$

Algorithm:

1. Compute the Derksen ideal $I \subseteq K[\underline{x}, \underline{y}]$.
2. Form $J_0 := \left(h(\underline{x}, \underline{z}), h(\underline{y}, \underline{z}) \middle| h \in I \right) \subseteq K[\underline{x}, \underline{y}, \underline{z}]$.
3. Compute $J := J_0 \cap K[\underline{x}, \underline{y}]$.
4. Produce homogeneous invariants $f_1, \ldots, f_s$ until

$$J \subseteq \sqrt{\left(f_1(\underline{x}) - f_1(\underline{y}), \ldots, f_s(\underline{x}) - f_s(\underline{y}) \right)}.$$

Algorithm:

1. Compute the Derksen ideal $I \subseteq K[\underline{x}, \underline{y}]$.

2. Form $J_0 := \left(h(\underline{x}, \underline{z}), h(\underline{y}, \underline{z}) \middle| h \in I\right) \subseteq K[\underline{x}, \underline{y}, \underline{z}]$.

3. Compute $J := J_0 \cap K[\underline{x}, \underline{y}]$.

4. Produce homogeneous invariants $f_1, \ldots, f_s$ until

   $$J \subseteq \sqrt{\left(f_1(\underline{x}) - f_1(\underline{y}), \ldots, f_s(\underline{x}) - f_s(\underline{y})\right)}.$$

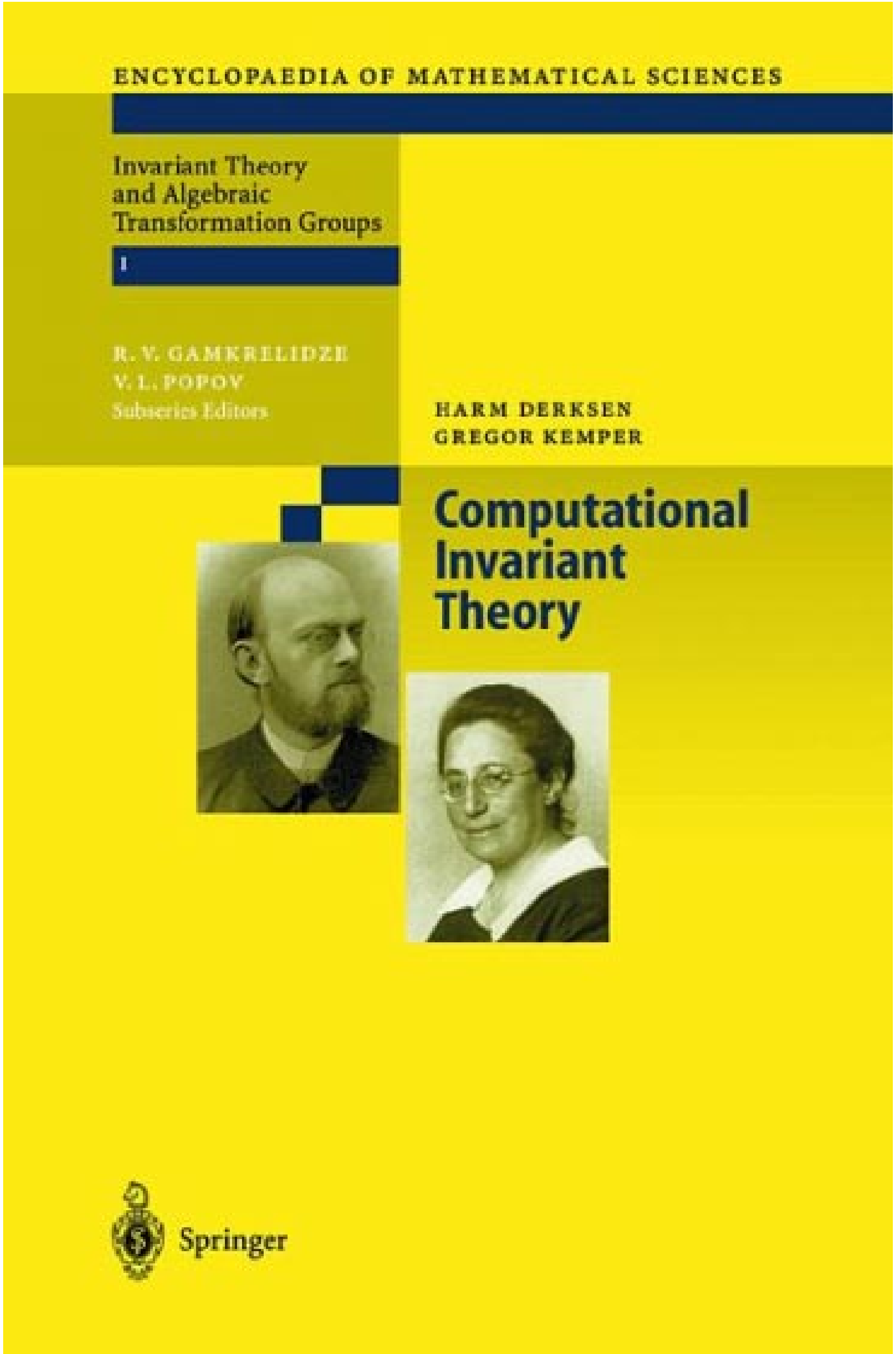
5. Set $A := K[f_1, \ldots, f_s]$ and compute the normalization

   $$B := \widetilde{A}$$

   (de Jong's algorithm).

6. Compute the *inseparable closure* of B:

   $K[V]^G = \{f \in K[\underline{x}] \mid f^q \in B,\ q$ a p-power$\}$.


ENCYCLOPAEDIA OF MATHEMATICAL SCIENCES
Invariant Theory and Algebraic Transformation Groups
I
R. V. GAMKRELIDZE
V. L. POPOV
Subseries Editors
HARM DERKSEN
GREGOR KEMPER
Computational Invariant Theory
Springer