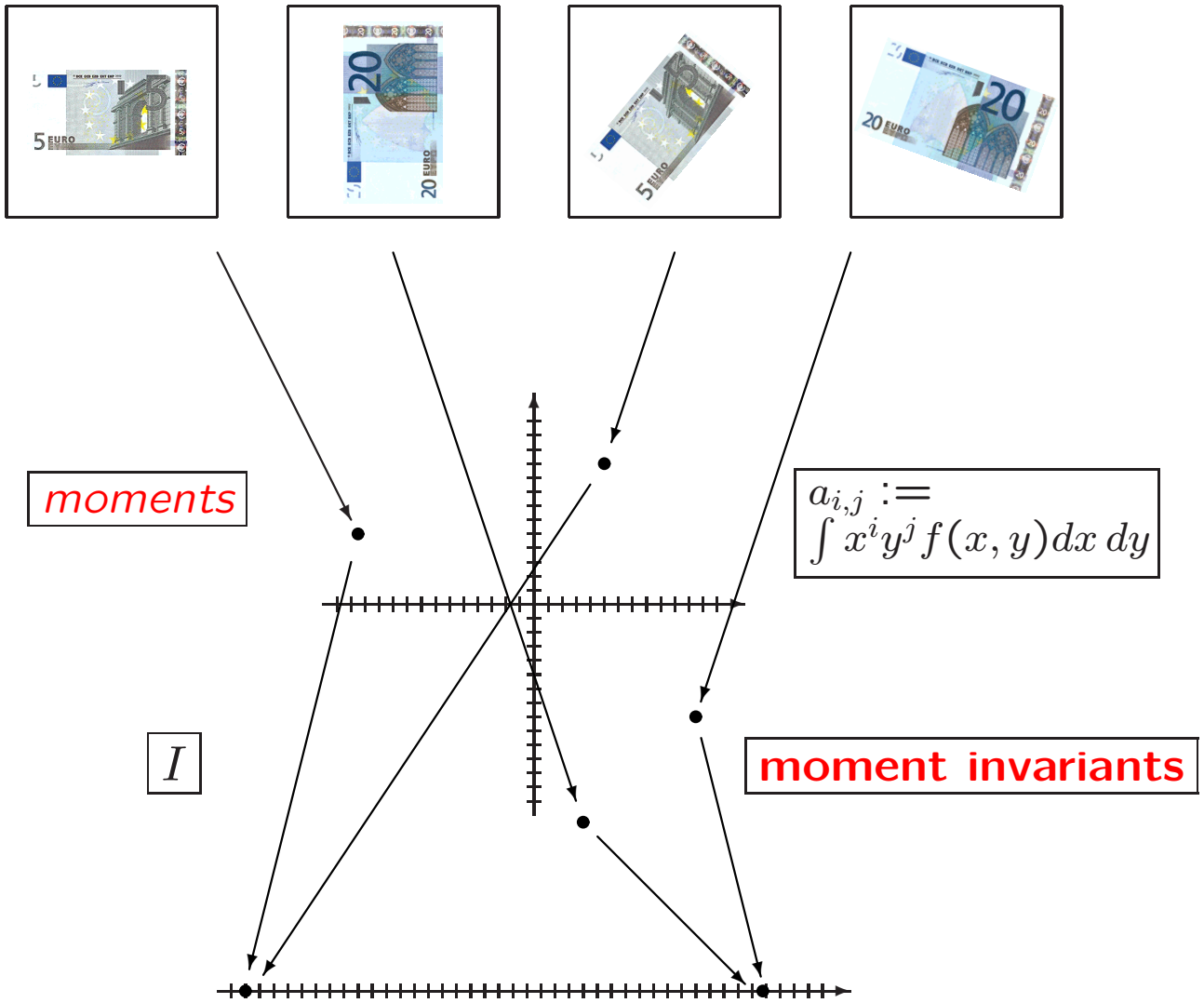
Computational Invariant Theory

Gregor Kemper
Technische Universität München

Tutorial at ISSAC,
München, July 25, 2010



$$
\begin{aligned}
I_1 &= a_{00}(a_{20}+a_{02}) - a_{10}^2 - a_{01}^2, \\
I_2 &= a_{00}\left(a_{20}a_{02} - a_{11}^2\right) + 2a_{11}a_{10}a_{01} - a_{10}^2 a_{02} - a_{01}^2 a_{20}
\end{aligned}
$$

are invariant under AO_2.

Invariant theory: philosophy

"Invariants describe the intrinsic properties of objects."

Given an equivalence relation, *invariants* are functions which are constant on all equivalence classes.

Try to find invariants that separate as many classes as possible.

Applications in geometry, linear algebra, computer vision, graph theory, coding theory, Galois theory, equivariant dynamical systems, quantum computing . . .

Invariant theory: setup

K: algebraically closed field.

G: linear algebraic group over K.

X: *G-variety*, i.e., affine variety over K with action given by a morphism $G \times X \to X$.

Special case: $X = K^n =: V$. Then V is called a *G-module*.

$K[X]$: ring of regular functions;
for $X = V$: $K[V] = K[x_1, \ldots, x_n]$ polynomial ring.

$K[X]^G$: *invariant ring*. $K[X]^G$ is a subalgebra of $K[X]$.

Special case: $K[V]^G$ is a graded algebra.

Example: Symmetric group

The symmetric group S_n acts on $V = K^n$ by permuting coordinates.

Theorem: $K[V] = K[s_1, \ldots, s_n]$ is generated by the *elementary symmetric polynomials*, given by

$$\prod_{i=1}^{n} (X + x_i) = X^n + s_1 X^{n-1} + \cdots + s_{n-1} X + s_n.$$

The s_i are algebraically independent.

Example: Orthogonal group

$G = \mathrm{O}_2(\mathbb{C})$ orthogonal group, $V = (\mathbb{C}^2)^3$ with diagonal action. Define $f_{i,j} \in \mathbb{C}[V]^G$ by

$$f_{i,j}(v_1, v_2, v_3) := \langle v_i, v_j \rangle \quad (1 \leq i \leq j \leq 3).$$

Theorem:

$$\mathbb{C}[V]^G = \mathbb{C}[f_{1,1}, f_{1,2}, f_{1,3}, f_{2,2}, f_{2,3}, f_{3,3}].$$

"Everything that's interesting in the Euclidean geometry of three vectors can be expressed in terms of the scalar products" —

really???

Problems

- Is $K[X]^G$ finitely generated (as K-algebra) (Hilbert's 14th problem)?
- If so, find generators!
- Compute the invariant field $K(X)^G$ (if X is irreducible).
- What sort of an algebra is $K[X]^G$?
- Orbit separation: $x, y \in X$ with

$$G(x) \neq G(y).$$

Does there exist $f \in K[X]^G$ with

$$f(x) \neq f(y)?$$

Example: Orthogonal group

$G = \mathrm{O}_2(\mathbb{C})$, $V = (\mathbb{C}^2)^3$, $f_{i,j}(v_1, v_2, v_3) := \langle v_i, v_j \rangle$ $(1 \leq i \leq j \leq 3)$.

$$\mathbb{C}[V]^G = \mathbb{C}[f_{1,1}, f_{1,2}, f_{1,3}, f_{2,2}, f_{2,3}, f_{3,3}],$$

subject to the relation

$$\det \begin{pmatrix} f_{1,1} & f_{1,2} & f_{1,3} \\ f_{1,2} & f_{2,2} & f_{2,3} \\ f_{1,3} & f_{2,3} & f_{3,3} \end{pmatrix} = 0.$$

$K[V]^G$ is a hypersurface.

Invariant field: $\mathbb{C}(X)^G$ is isomorphic to a rational function field.

Orbit separation: If $f_{i,j}(v) = f_{i,j}(w)$ for all i, j, and rank $\left(f_{i,j}(v)\right)_{i,j} = 2$, then $G(v) = G(w)$. But: Invariants can't separate isotropic vectors from the zero vector!

Types of groups

G **linear algebraic group:** G is given by polynomial equations.

G **reductive:** G linear algebraic, and has trivial unipotent radical. Examples: the classical groups (GL_n, SL_n, O_n, Sp_{2n}), all finite groups.

G **linearly reductive:** Every G-module is completely reducible.

G **finite.**

Connections:

$$\left.\begin{array}{l}\text{linearly reductive}\\ \\ \text{finite}\end{array}\right\} \Rightarrow \text{reductive} \Rightarrow \text{linear algebraic}$$

If $\mathrm{char}(K) = 0$: reductive $\Longleftrightarrow$ linearly reductive.

Hilbert's 14th problem:

Theorem (Hilbert, Nagata, Haboush, Popov): $K[X]$ is finitely generated for all G-modules $X \iff G$ reductive.

If G is linearly reductive, have a *Reynolds operator*

$$\mathcal{R}\colon K[X] \twoheadrightarrow K[X]^G$$

(a G-equivariant projection of $K[X]^G$-modules).

Open question: For which groups G is it true that $K[V]^G$ is finitely generated for all G-modules V?

Algorithms: the state of the art

	facts	$K[V]^G$	$K[X]^G$	$K(X)^G$	separating
G algebraic	$K[V]^G$ normal	?	?	Müller-Quade/ Beth/Ke (1999/2007)	?
G reductive	$K[X]^G$ finitely generated	Ke (2003)	Derksen/Ke (2008)	see above	Ke (2003)
G linearly reductive	$\mathcal{R}$: $K[X] \twoheadrightarrow K[X]^G$	Derksen (1999)	Derksen (1999)	see above	see above
G finite	$K[X]$ integral over $K[X]^G$	Sturmfels/Ke (1993/1999)	see above	Fleischmann/ Ke/Woodcock (2007)	Derksen/Ke (2002)

Finite groups: algorithms

Let G be finite with linear action on V, $n = \dim(V)$.

Primary invariants: There exist homogeneous invariants $f_1, \ldots, f_n$ such that $K[V]^G$ is integral over $K[f_1, \ldots, f_n]$ (Noether normalization).
Criterion: the variety given by $f_1, \ldots, f_n$ is $\{0\}$.

Secondary invariants: homogeneous generators of $K[V]^G$ as a module over $K[f_1, \ldots, f_n]$ are called secondary invariants.

Together, primary and secondary invariants generate $K[V]^G$.

Finite groups: the nonmodular case

Assume that $|G|$ is *not* a multiple of $\mathrm{char}(K)$ (e.g., $\mathrm{char}(K) = 0$).

Cohen-Macaulay property: $K[V]^G$ is free as a $K[f_1, \ldots, f_n]$-module.

Molien's formula: The *Hilbert series* is

$$H\left(K[V]^G, t\right) := \sum_{d=0}^{\infty} \dim\left(K[V]_d^G\right) t^d = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det\left(1 - t\sigma\right)}.$$

Let $f_1, \ldots, f_n \in K[V]^G$ be primary invariants. Then

$$H\left(K[V]^G, t\right) = \frac{t^{d_1} + \cdots + t^{d_m}}{\left(1 - t^{\deg(f_1)}\right) \cdots \left(1 - t^{\deg(f_n)}\right)}$$

with $d_1, \ldots, d_m$ the degrees of secondary invariants.

Application: coding theory

Let $C \subseteq \mathbb{F}_3^n$ be a self-dual linear code, assume $\mathbf{1} = (1, \ldots, 1) \in C$.
Complete weight enumerator:

$$f(x, y, z) := \sum_{\mathbf{c} \in C} x^{n_0(\mathbf{c})} y^{n_1(\mathbf{c})} z^{n_2(\mathbf{c})} \in \mathbb{C}[x, y, z],$$

with $n_0(\mathbf{c}) =$ number of 0's in $\mathbf{c}$ etc.

For $\mathbf{c} \in C$:

$$\left.\begin{array}{ll} \langle \mathbf{c}, \mathbf{1} \rangle = 0 & \Rightarrow 3 \mid (n_1(\mathbf{c}) - n_2(\mathbf{c})) \\ \langle \mathbf{c}, \mathbf{c} \rangle = 0 & \Rightarrow 3 \mid (n_1(\mathbf{c}) + n_2(\mathbf{c})) \end{array}\right\} \Rightarrow 3 \mid n_1(\mathbf{c}).$$

So f(x,y,z) is invariant under $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}$ with $\omega := e^{2\pi i/3}$.

Application: coding theory

Two bijections of C: $\mathbf{c} \mapsto -\mathbf{c}$ and $\mathbf{c} \mapsto \mathbf{1} + \mathbf{c}$. So $f(x, y, z)$ is invariant under $y \leftrightarrow z$ and $x \mapsto y \mapsto z \mapsto x$.

The MacWilliams identity shows that $f(x, y, z)$ is invariant under $\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$.

So $f(x, y, z) \in \mathbb{C}[x, y, z]^G$ with

$$G = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \right\rangle.$$

$|G| = 2592$.

Application: coding theory

Molien's formula yields

$$H\left(\mathbb{C}[x,y,z]^G,t\right)=\frac{1+t^{24}}{\left(1-t^{12}\right)^2\left(1-t^{36}\right)}.$$

In general, have

$$H\left(K[V]^G,t\right)=\frac{t^{\deg(g_1)}+\ldots+t^{\deg(g_m)}}{\left(1-t^{\deg(f_1)}\right)\ldots\left(1-t^{\deg(f_n)}\right)}.$$

Guess: There are primary invariants of degrees 12, 12, 36 and secondary invariants of degrees 0 and 24.

MAGMA finds such invariants in less than 15 seconds.

MAGMA code

```
> K<z>:=CyclotomicField(12);
> w:=z^4;
> s3:=(z^5+z^7);
> G:=MatrixGroup<3,K | DiagonalMatrix([1,w,1]),
>   PermutationMatrix(K,[1,3,2]),PermutationMatrix(K,[2,3,1]),
>   [1/s3,1/s3,1/s3, 1/s3,w/s3,w^2/s3, 1/s3,w^2/s3,w/s3]>;
> #G;
2592
> R:=InvariantRing(G);
> // This only sets up the data structure
> SetVerbose("Invariants",1);
```

MAGMA code

```
> time prim:=PrimaryInvariants(R);
PRIMARY INVARIANTS
Compute Molien series
Molien time: 0.530
Try degree vector [ 12, 12, 36 ] (time: 0.540)
Primaries of degrees [ 12, 12, 36 ] found!
Time: 2.340
> time sec:=SecondaryInvariants(R);
Number of secondary invariants: 2
Hilbert series numerator: t^24 + 1
Time: 10.530
```

Finite groups: the modular case

Assume that $|G|$ is a multiple of $\mathrm{char}(K)$. This case is much harder, in theory as well as in practice!

Fist step: Compute primary invariants $f_1, \ldots, f_n$, set $A := K[f_1, \ldots, f_n]$.

The group generators $\sigma_1, \ldots, \sigma_l$ define A-linear maps

$$K[V] \to K[V], \quad f \mapsto \sigma_i(f) - f.$$

$K[V]^G$ is the kernel of the combined map $K[V] \to K[V]^l$.

$K[V]$ is a free A-module: $K[V] \cong A^r$.

Obtain $K[V]^G$ by computing the kernel of the map

$$A^r \to A^{lr}.$$

This is the computation of a syzygy module.

Invariants of finite groups in MAGMA

In the nonmodular and modular case, have commands

`PrimaryInvariants`

`SecondaryInvariants`

`FundamentalInvariants`

`InvariantsOfDegree`

`Relations`

`HilbertSeries`

`IsCohenMacaulay`

`Depth`

Finite groups: Noether's degree bound

Let G ba finite, V a G-module. Write

$$\beta\left(K[V]^G\right) := \min\left\{k \mid K[V]^G \text{ can be generated in degree } \leq k\right\}.$$

Theorem (Noether's degree bound): If $|G|$ is not a multiple of $\mathrm{char}(K)$, then

$$\beta\left(K[V]^G\right) \leq |G|.$$

In the case $\mathrm{char}(K) < |G|$, it took until 2000 until Fleischmann and Fogarty proved this!

If $|G|$ is a multiple of $\mathrm{char}(K)$ (the modular case), Noether's degree bound fails catastrophically!

Finite reflection groups

Suppose $|G| < \infty$, $\mathrm{char}(K) \nmid |G|$. Then

$K[V]^G \cong$ polynomial ring $\iff$ G is generated by reflections.

Serre (19??): In the modular case, the implication "$\Rightarrow$" still holds.

There are many counterexamples to "$\Leftarrow$".

Ke, Malle (1997): Classification of finite irreducible groups with $K[V]^G$ polynomial.

Algorithms: the state of the art

	facts	$K[V]^G$	$K[X]^G$	$K(X)^G$	separating
G algebraic	$K[V]^G$ normal	?	?	Müller-Quade/ Beth/Ke (1999/2007)	?
G reductive	$K[X]^G$ finitely generated	Ke (2003)	Derksen/Ke (2008)	see above	Ke (2003)
G linearly reductive	$\mathcal{R}$: $K[X] \twoheadrightarrow K[X]^G$	Derksen (1999)	Derksen (1999)	see above	see above
G finite	$K[X]$ integral over $K[X]^G$	Sturmfels/Ke (1993/1999)	see above	Fleischmann/ Ke/Woodcock (2007)	Derksen/Ke (2002)

The Derksen ideal

Let G act on a K-algebra R. Let $x_1, \ldots, x_n \in R$, and take $y_1, \ldots, y_n$ indeterminates.
The *Derksen ideal* $D \subseteq R[y_1, \ldots, y_n]$ comes in three guises:

Algebraic: $D := \bigcap_{\sigma \in G} \Big(y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n)\Big)_{R[y_1,\ldots,y_n]}$.

Geometric: If $R = K[V] = K[x_1, \ldots, x_n]$, then D is the vanishing ideal of the set

$$\Big\{(x, y) \in V \times V \Big| \, G(x) = G(y)\Big\}.$$

Computational: If $G \subseteq K^m$ is given by its vanishing ideal $I_G \subseteq K[t_1, \ldots, t_m]$, and $\sigma(x_i) = f_i(\sigma)$ with $f_i \in R[t_1, \ldots, t_m]$, then

$$D = \Big(I_G \cup \{y_1 - f_1, \ldots, y_n - f_n\}\Big)_{R[\underline{t},\underline{y}]} \cap R[y_1, \ldots, y_n]$$

(elimination ideal).

Derksen's algorithm

Input: - a linearly reductive algebraic group G;

- a G-module V.

Output: Generators of $K[V]^G = K[x_1, \ldots, x_n]^G$.

(1) Compute the Derksen ideal $D \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_n]$.

(2) Set $y_i := 0$ in all generators of D. Obtain polynomials $g_i \in K[V]$. **Theorem**: The g_i generate the *Hilbert ideal* $\left(K[V]^G_+\right)_{K[V]}$.

(3) Apply the *Reynolds operator*: The $\mathcal{R}(g_i)$ generate $K[V]^G$. Alternative: Compute invariants of the same degrees as the g_i from scratch.

Derksen's algorithm in MAGMA

We compute the invariants of $G = \mathrm{O}_2$ acting on three vectors.

```
Magma V2.16-5
> Kt<t11,t12,t21,t22>:=PolynomialRing(Rationals(),4);
> I:=ideal<Kt | [t11^2+t12^2-1,t21^2+t22^2-1,t11*t21+t12*t22]>;
> // this defines the orthogonal group
> A:=Matrix([[t11,t12],[t21,t22]]);
> // this defines the natural action
> A:=TensorProduct(MatrixAlgebra(Kt,3)!1,A);
> A;
[t11 t12   0   0   0   0]
[t21 t22   0   0   0   0]
[  0   0 t11 t12   0   0]
[  0   0 t21 t22   0   0]
[  0   0   0   0 t11 t12]
[  0   0   0   0 t21 t22]
> // this defines the action on 3 points
> R:=InvariantRing(I,A: LinearlyReductive:=true);
> // This only sets up the data structure
> Kx<x11,x12,x21,x22,x31,x32>:=PolynomialRing(R);
```

Derksen's algorithm in MAGMA

```
> time FundamentalInvariants(R);
[
    x31^2 + x32^2,
    x21*x31 + x22*x32,
    x21^2 + x22^2,
    x11*x31 + x12*x32,
    x11*x21 + x12*x22,
    x11^2 + x12^2
]
Time: 0.130
```

These are indeed the scalar products!

Derksen's algorithm in MAGMA

. . . Now compute moment-invariants.

```
> B:=Matrix([[t11^2,2*t11*t12,t12^2],[t11*t21,t11*t22+t21*t12,t12*t22],
> [t21^2,2*t21*t22,t22^2]]);
> // the action on the moments with index-sum 2
> R:=InvariantRing(I,B: LinearlyReductive:=true);
> Ka<a20,a11,a02>:=PolynomialRing(R);
> time FundamentalInvariants(R);
[
    a20 + a02,
    a20*a02 - a11^2
]
Time: 0.010
```

Algorithms: the state of the art

	facts	$K[V]^G$	$K[X]^G$	$K(X)^G$	separating
G algebraic	$K[V]^G$ normal	?	?	Müller-Quade/ Beth/Ke (1999/2007)	?
G reductive	$K[X]^G$ finitely generated	Ke (2003)	Derksen/Ke (2008)	see above	Ke (2003)
G linearly reductive	$\mathcal{R}$: $K[X] \twoheadrightarrow K[X]^G$	Derksen (1999)	Derksen (1999)	see above	see above
G finite	$K[X]$ integral over $K[X]^G$	Sturmfels/Ke (1993/1999)	see above	Fleischmann/ Ke/Woodcock (2007)	Derksen/Ke (2002)

Computing invariant fields: easier than expected!

Assume G acts on $N = K(x_1, \ldots, x_n)$. Compute a reduced Grbner Basis $\mathcal{B}$ of

$$D = \bigcap_{\sigma \in G} \Big\langle y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n) \Big\rangle_{N[y_1,\ldots,y_n]}.$$

Set $L := K\Big(\textit{all coefficients appearing in } \mathcal{B}\Big) \subseteq N$.

Theorem (Müller-Quade, Beth; Ke): $\boxed{N^G = L.}$

The algorithm is implemanted in MAGMA (for the case of linear actions).

We do give a proof!

1. D is G-stable. Uniqueness of reduced Gröbner bases: $\sigma(\mathcal{B}) = \mathcal{B}$ for all $\sigma \in G$, so $\sigma(g) = g$ for $g \in \mathcal{B}$. This implies $L \subseteq N^G$.

2. Let $a \in N^G$, write

$$a = \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$$

with $f, g \in K[y_1, \ldots, y_n]$. Then $f - ag \in D$, so have normal form

$$0 = \mathsf{NF}_{\mathcal{B}}(f - ag) = \mathsf{NF}_{\mathcal{B}}(f) - a\,\mathsf{NF}_{\mathcal{B}}(g). \qquad (*)$$

But $\mathcal{B} \subseteq L[y_1, \ldots, y_n]$, $f, g \in L[y_1, \ldots, y_n]$, so $\mathsf{NF}_{\mathcal{B}}(f), \mathsf{NF}_{\mathcal{B}}(g) \in L[y_1, \ldots, y_n]$. Hence (*) implies $a \in L$.

An example

Daigle and Freudenburg gave a "small" example of a G_a-action with non-finitely generated invariant ring. Action:

$$x_1 \mapsto x_1, \quad x_2 \mapsto x_2 + tx_1^3, \quad x_3 \mapsto x_3 + tx_2 + \frac{t^2}{2}x_1^3,$$
$$x_4 \mapsto x_4 + tx_3 + \frac{t^2}{2}x_2 + \frac{t^3}{6}x_1^3, \quad x_5 \mapsto x_5 + tx_1^2.$$

MAGMA computes $\mathcal{B}$ in 0.01 seconds. Picking out coefficients yields generators f_i of $\mathbb{C}(x_1, \ldots, x_5)^{G_a}$:

$$f_1 = x_1, \quad f_2 = x_1x_5 - x_2, \quad f_3 = 2x_2x_5 - 2x_1^2x_3 - x_1x_5^2,$$

$$f_4 = 6x_3x_5x_1^2 + x_1x_5^3 - 3x_2x_5^2 - 6x_1^4x_4.$$

$\mathbb{C}(x_1, \ldots, x_5)^{G_a}$ is isomorphic to a rational function field!

Extensions, applications

Obtain an algorithmic version of
Rosenlicht's Theorem: "Almost all G-orbits can be separated by rational invariants."

Tobias Kamke (2009): Assume $K(X)^G = \text{Quot}\left(K[X]^G\right)$ (e.g., G unipotent). By controlling denominators, obtain $0 \neq f, g_1, \ldots, g_m \in K[X]^G$ such that

$$K[X]_f^G = K[f^{-1}, g_1, \ldots, g_m]$$

From this, obtain a "pseudo-algorithm" for computing $K[X]^G$ if finitely generated.

Algorithms: the state of the art

	facts	$K[V]^G$	$K[X]^G$	$K(X)^G$	separating
G algebraic	$K[V]^G$ normal	?	?	Müller-Quade/ Beth/Ke (1999/2007)	?
G reductive	$K[X]^G$ finitely generated	Ke (2003)	Derksen/Ke (2008)	see above	Ke (2003)
G linearly reductive	$\mathcal{R}$: $K[X] \twoheadrightarrow K[X]^G$	Derksen (1999)	Derksen (1999)	see above	see above
G finite	$K[X]$ integral over $K[X]^G$	Sturmfels/Ke (1993/1999)	see above	Fleischmann/ Ke/Woodcock (2007)	Derksen/Ke (2002)

Second lucky case: separating invariants

G reductive, $x, y \in X$:

$$\exists\ f \in K[X]^G \text{ with } f(x) \neq f(y) \quad \Longleftrightarrow \quad \overline{G(x)} \cap \overline{G(y)} = \emptyset.$$

(So for $|G| < \infty$, invariants separate all orbits!)

G nonreductive: ???

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" is weaker than "generating"!

Separating invariants: example

$G = Z_3$ acts in $\mathbb{C}[x, y]$ by $x \mapsto \omega x$, $y \mapsto \omega y$ with $\omega = e^{2\pi i/3}$.

$$\mathbb{C}[x, y]^G = \mathbb{C}[\underbrace{x^3}_{f_1}, \underbrace{x^2y}_{f_2}, \underbrace{xy^2}_{f_3}, \underbrace{y^3}_{f_4}]$$

(minimal generating set).

But $S := \{f_1, f_2, f_4\}$ is separating since

$$f_3 = f_2^2/f_1, \quad \text{and} \quad f_1(v) = 0 \;\Rightarrow\; f_3(v) = 0.$$

Second lucky case: separating invariants

- $K[X]^G$ always has a finite separating subset.
- $|G| < \infty \Rightarrow$ Noether's degree bound holds for separating invariants in $K[V]^G$: $\beta_{\mathsf{sep}}\left(K[V]^G\right) \leq |G|$.

Proof. $K[V] = K[x_1, \ldots, x_n]$. With additional indeterminates T and U, set

$$f(T,U) := \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} \sigma(x_i) U^{i-1} \right) \in K[V]^G[T,U].$$

The coefficients of $f(T,U)$ form a separating set: Let $v, w \in V$ such that all coefficients of $f(T,U)$ coincide on v and w. Then

$$\prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} x_i \left(\sigma^{-1}(v)\right) U^{i-1} \right) = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} x_i \left(\sigma^{-1}(w)\right) U^{i-1} \right).$$

This shows that $\exists\ \sigma \in G$ with $\sigma(v) = w$. $\square$

Second lucky case: separating invariants

- $K[X]^G$ always has a finite separating subset.
- $|G| < \infty \Rightarrow$ Noether's degree bound holds for separating invariants in $K[V]^G$: $\beta_{\mathsf{sep}}\left(K[V]^G\right) \leq |G|$.
- If $|G| < \infty$ and there exist $n = \dim(V)$ separating invariants in $K[V]^G$, then G is generated by reflections (Dufresne 2009).
- Weyl's polarization theorem holds for separating invariants in all characteristics (Draisma, Ke, Wehlau 2008).
- But: For many non-Cohen-Macaulay invariant rings, there is no Cohen-Macaulay separating subalgebra (Dufresne, Elmer, Kohls 2009).

Separating invariants: algorithms

Let G be reductive.

- Have an algorithm (involving the Derksen ideal) for computing separating invariants in $K[X]^G$.
- Let $S \subseteq K[V]^G$ be a graded, separating subalgebra $\Rightarrow$
  - char$(K) = 0$: $K[V]^G$ is the normalization of S;
  - char$(K) > 0$: $K[V]^G$ is the inseparable closure of S in $K[V]$.
- Obtain an algorithm for computing $K[V]^G$ (Ke 2003).
- Have an extension that computes $K[X]^G$ (Derksen & Ke 2008).

Algorithms: the state of the art

	facts	$K[V]^G$	$K[X]^G$	$K(X)^G$	separating
G algebraic	$K[V]^G$ normal	?	?	Müller-Quade/ Beth/Ke (1999/2007)	?
G reductive	$K[X]^G$ finitely generated	Ke (2003)	Derksen/Ke (2008)	see above	Ke (2003)
G linearly reductive	$\mathcal{R}$: $K[X] \twoheadrightarrow K[X]^G$	Derksen (1999)	Derksen (1999)	see above	see above
G finite	$K[X]$ integral over $K[X]^G$	Sturmfels/Ke (1993/1999)	see above	Fleischmann/ Ke/Woodcock (2007)	Derksen/Ke (2002)

Open problems

G nonreductive:

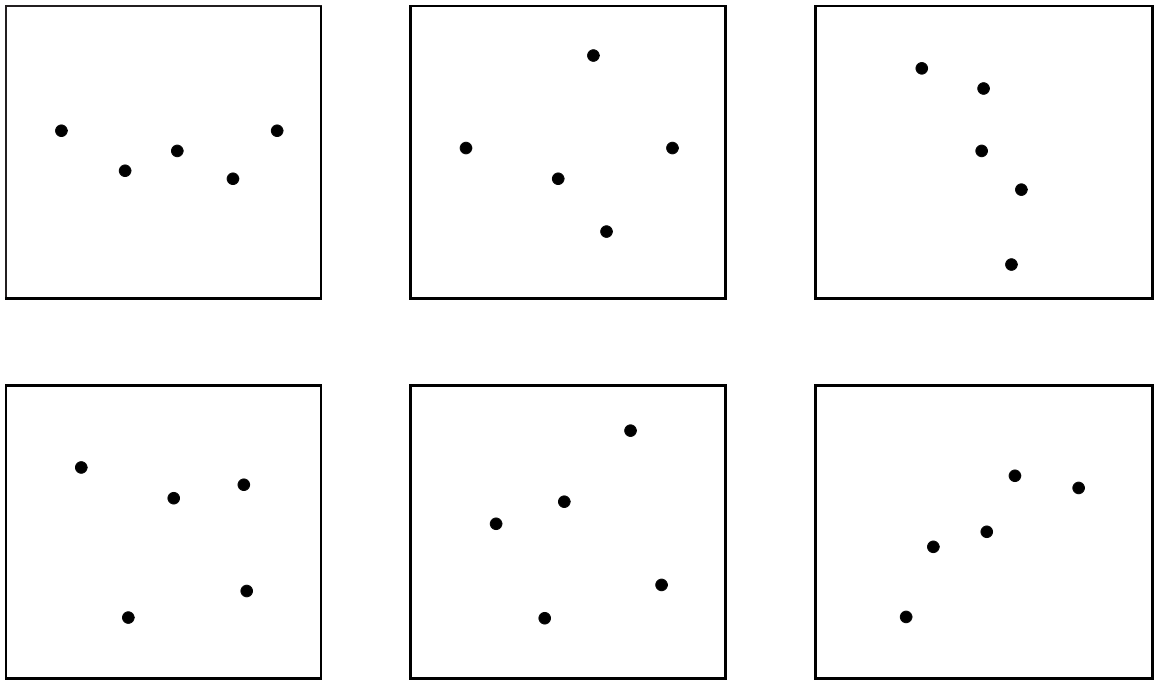
- Find a separating subset of $K[X]^G$.
- Test finite generation of $K[X]^G$; in case "yes", compute generators.
- Compute a quasi affine variety Y with $K[X]^G = K[Y]$.

G reductive:

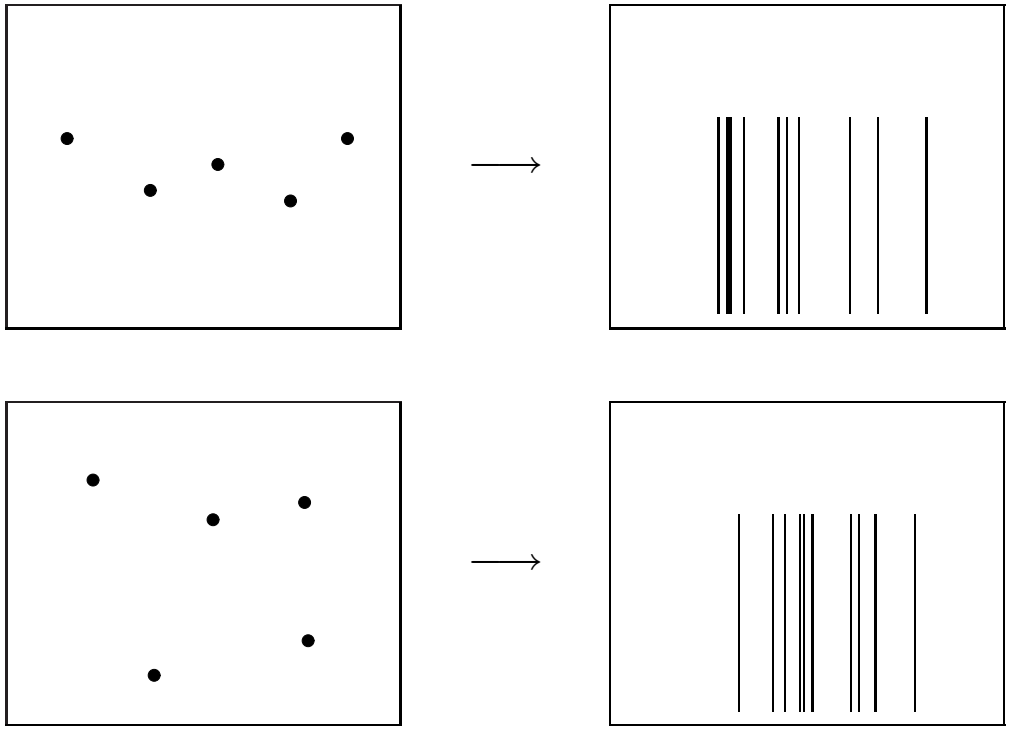
- R nonreduced K-algebra with G-action: Compute R^G.
- Implementations! (MAGMA, SINGULAR, MAPLE . . .)

Application: point configurations

Which objects are "equal?"



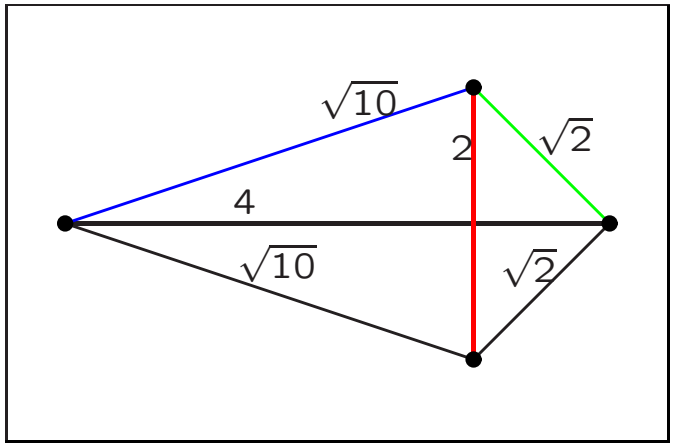
Distribution of distances

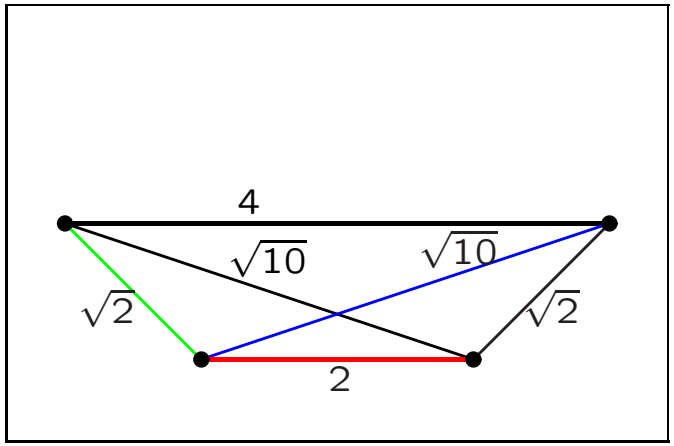


Further applications: finger print identification, archaeological sherds, DNA-strands.

Reconstructibility

Question: Are point configurations determined uniquely (up to the action of von $S_n \times \mathrm{AO}_m$) by their distribution of distances?





Reconstructibility

For $P_1, \ldots, P_n \in \mathbb{R}^m$, set $d_{i,j} := ||P_i - P_j||^2$,

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

The coefficients of $F_{P_1,\ldots,P_n}(X)$ are invariant under $G = S_n \times \mathrm{AO}_m$.

Definition: We call the 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 $g \in \mathrm{AO}_m$ and $\pi \in S_n$ such that

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

The wrong group!

The coefficients of $F_{P_1,\ldots,P_n}(X)$ are invariants of the group $S_{\binom{n}{2}}$ (instead of S_n)!

But there are relations between the $d_{i,j}$. E.g., for $m = 2$, $n = 4$ have:

$$\begin{aligned} & d_{12}d_{13}d_{23} - d_{12}d_{14}d_{23} - d_{13}d_{14}d_{23} + d_{14}^2d_{23} + d_{14}d_{23}^2 \\ & - d_{12}d_{13}d_{24} + d_{13}^2d_{24} + d_{12}d_{14}d_{24} - d_{13}d_{14}d_{24} - d_{13}d_{23}d_{24} \\ & - d_{14}d_{23}d_{24} + d_{13}d_{24}^2 + d_{12}^2d_{34} - d_{12}d_{13}d_{34} - d_{12}d_{14}d_{34} \\ & + d_{13}d_{14}d_{34} - d_{12}d_{23}d_{34} - d_{14}d_{23}d_{34} - d_{12}d_{24}d_{34} - d_{13}d_{24}d_{34} \\ & + d_{23}d_{24}d_{34} + d_{12}d_{34}^2 = 0. \end{aligned}$$

Good news

Theorem (Boutin, Ke 2004): Almost all point configurations are reconstructible.
More precisely: Let $V = \mathbb{R}^m$, $n > m + 1$. Then there is a polynomial $f \in \mathbb{R}[V^n]$, $f \neq 0$, such that every point configuration $(P_1, \ldots, P_n) \in V^n$ with

$$f(P_1, \ldots, P_n) \neq 0$$

is reconstructible.

Open question: Is every point configuration in $\mathbb{R}^2$ reconstructible (up to the action of $S_n \times \mathrm{AO}_2$) from the distribution of all $\binom{n}{3}$ subtriangles?