Stability in Geometric Complexity Theory

Milind Sohoni
Indian Institute of Technology-Bombay

at

The Intractability Institute
Princeton University

8th July, 2010

Talk Outline

- A historical perspective
- Group representations and orbits
- Invariant Theory and Orbit Separation
- Stability and rings of invariants
- Calculus of 1-parameter subgroups
- Stability of permanent and determinant
- Further role of stability and geometric invariants

Groups and Action

- G a group and V a vector space over $\mathbb{C}$.
- $GL(V)$: the group of linear transformations on V.

- Representation : $\rho : G \to GL(V)$.
- Action : $G \times V \to V$
  - (i) $1_G \cdot v = v$ (ii) $(g \cdot g') \cdot v = g \cdot (g' \cdot v)$
  - (iii) $\alpha(g \cdot v) = (g \cdot \alpha v)$, $g \cdot (v + v') = g \cdot v + g \cdot v'$

Example 1 : G is the finite group of isometries of the cube. V is the space generated by the formal linear combinations of the *edges* of the cube.

$$|G| = 24 \qquad dim(V) = 12$$

Example 2 : $G = GL_m$ and $V = \mathbb{C}^m$, the standard action, i.e., given $v \in \mathbb{C}^m$ and $A \in G$, $A \cdot v = Av$.

Example 3 : $G = GL_m$ and $V = M_m$, square matrices of size m. Given $A \in G, X \in M_m$ we have $A \cdot X = AXA^{-1}$, the adjoint representation.

Example 4 : $G = GL_m$ and $V = Sym^d(\mathbb{C}^m)$, collection of homogenous polynomials of degree d in the variables $X = X_1, \ldots, X_m$. Given $A \in GL_m$ and $f(X) \in V$, we have $(A \cdot f)(X) = f(A^{-1}X)$.

Orbit : $v \in V$ then

$$O(v) = \{v' | \exists g \in G \; s.t. \; v' = g \cdot v\}$$

Enduring Question

Given ρ, v, v' **Is** $v' \in Orbit(v)$**?**

Is there a Tractable answer to the question

Given ρ, v, v' Is $v' \in Orbit(v)$?

- G finite and ρ perumation representation: Polya Theory.
- When G is *Galilean Group* $\times$ *Time*: Classical Mechanics.
- In fact, many more examples. Hilbert's 3rd : Can the tetrahedron be cut and pasted to a cube?

Approach I : Inspection or explicit solution.

- When G is finite, try all.
- Otherwise, try and get $g \in G$ by solving a set of equations. E.g., given $P = Ax^2 + Bxy + C$ and $P' = A'x^2 + B'xy + C'y^2$, is there

$$\begin{aligned} x &\leftarrow aX + bY \\ y &\leftarrow cX + dY \end{aligned}$$

such that $P(x, y) = P'(X, Y)$?

continued

Expanding P and comparing with P' gives us the equations:

$$\begin{aligned} a^2A + acB + c^2C &= A' \\ 2abA + (ad+bc)B + 2cdC &= B' \\ b^2A + bdB + d^2C &= C' \end{aligned}$$

This is hard to solve. In general, the orbit problem is highly non-linear in the group variables and usually intractable.

Approach II

Canonical Forms : -*without loss of generality*

- Locate a special element in each orbit.
- Move both v and v' to this canonical form and then compare.

Very popular

- $A \in GL_m$: $X \to AXA^{-1}$: *Jordan canonical form*.
- For quadratic, cubic and quartic polynomials.
- LU, SVD and polar decomposition.

- Will give g such that $g \cdot v = v'$.
- Very few actions have canonical forms!

Invariants

A function $f : V \to \mathbb{C}$ is called an **invariant** if $f(v) = f(g^{-1} \cdot v)$ for all $g \in G$ and for all $v \in V$.

- More generally, there is a character $\chi : G \to \mathbb{C}$ so that $f(g^{-1} \cdot v) = \chi(g^{-1})f(v)$
- Most interesting groups have very few characters, e.g., SL_m has just the identity.
- The action of GL_m is a simple extension of the action of SL_m.
- Clear then that $f(v) \neq f(v') \implies v' \notin O(v)$.

Question 1 : How are such invariants to be constructed?
Question 2 : Are there enough of them?

Example 1 : GL_m acting on $\mathbb{C}^{m\times m}$ by conjugation: $A \cdot X = AXA^{-1}$. $\mathbb{C}[X] = \mathbb{C}[X_{11}, \ldots, X_{mm}]$ is the ring of functions. Invariants are $trace(X^k)$, and *these are the only ones*.

Example 2 : GL_m acting on $\mathbb{C}^{m\times n}$ by left multiplication; $A \cdot X = AX$. Invariants are the $m \times m$-minors of X, and *these are the only ones*.

Example 3 : GL_2 acting on $Sym^2(\mathbb{C}^2)$, i.e., $aX_1^2 + bX_1X_2 + cX_2^2$. In $\mathbb{C}[a, b, c]$, the discriminant $b^2 - 4ac$ is an invariant and *it is the only one*.

Example 4 : GL_m acting on $(X_1, \ldots, X_k)$ by simultaneous conjugation:

$$(X_1, X_2, \ldots, X_k) \rightarrow (AX_1A^{-1}, \ldots, AX_kA^{-1})$$

The invariants are $Tr(X_{i1} \ldots X_{id})$ for all tuples $(i_1, \ldots, i_d)$.

The invariants and orbit space

Hilbert (1898), Mumford, Nagata and others: For rational actions of reductive groups the ring of polynomial invariants is a finitely generated $\mathbb{C}$-algebra.

If $\mathbb{C}[V]$ is the ring of functions on V, and $C[V]^G$ is denoted as the ring of invariants, then there are $f_1, \ldots, f_r \in \mathbb{C}[V]$, homogeneous, such that $\mathbb{C}[V]^G = \mathbb{C}[f_1, \ldots, f_r]$.

Also note that if $\mathbb{C}[V]^G = \mathbb{C}[f_1, \ldots, f_r]$, then in general the f_i *are not algebraically independent*.

This explains the limitation of the canonical form approach.

Invariants

The Reynolds Operator: : $R : \mathbb{C}[V] \to \mathbb{C}[V]^G$.

- *Cayley process, symbolic method, restitution*

This answered the construction of invariants question.

But are there enough of them?

That is, if $v' \notin O(v)$ then is there an $f \in \mathbb{C}[V]^G$ such that $f(v) \neq f(v')$?

If $\mathbb{C}[V]^G = \mathbb{C}[f_1, \ldots, f_r]$ then consider the map $V \to \mathbb{C}^r$:

$$v \to (f_1(v), \ldots, f_r(v))$$

So, if $v \notin O(v')$ then is $f(v) \neq f(v')$?

Rings and Spaces

Variety X and $\mathbb{C}[X]$, ring of functions on X.

$$\text{maximal ideals of } \mathbb{C}[X] \Leftrightarrow \text{points of } X$$

Lets apply this to $\mathbb{C}[V]^G$:

$$\text{maximal ideals of } \mathbb{C}[V]^G \overset{?}{\Leftrightarrow} \text{orbits in } V$$

Example 2 : GL_m acting on $\mathbb{C}^{m\times n}$ by left multiplication; $A \cdot X = AX$. Invariants are the $m \times m$-minors of X, and *these are the only ones*.

NO

$$m\text{-dimensional subspaces of } \mathbb{C}^n \overset{?}{\Leftrightarrow} \text{all subspaces of dimension} \leq m$$

Separation

Let $\mathbb{C}[V]^G = \mathbb{C}[f_1, \ldots, f_r]$.

The closure

$$[v] = \{v' | f_i(v) = f_i(v') \text{ for all } f_i\}$$

Clear that:

- $[v]$ is a closed set and that $O(v) \subseteq [v]$.
- If $O(v)$ is not closed, *invariants do not separate.*

Example : Consider $X \rightarrow AXA^{-1}$. Let $A(t) = diag(t, t^{-1})$ and X be as follows:

$$A(t)XA(t)^{-1} = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} 1 & t^2 \\ 0 & 1 \end{bmatrix}$$

X cannot be separated from I by any invariant.

Stability

Nagata, Mumford

- $v \in V$ is called **stable** is $O(v)$ is closed.
- $[v]$ **has a unique stable orbit.**

Part of the proof:

- Suppose $[v]$ has two closed disjoint G-invariant sets C_1 and C_2.
- There is an $f \in \mathbb{C}[V]$ such that $f(C_1) = 0$ and $f(C_2) = 1$.
- (rationality of action) There are a finite number of translates $f_1 = g_1 \cdot f, \ldots, f_k = g_k \cdot f$ such that all translates $g \cdot f$ are linear combinations of the above. In other words

$$M = \mathbb{C}f_1 \oplus \ldots \oplus \mathbb{C}f_k$$

is a G-module.

- Finally, let $p \in C_2$ and define:

$$eval_p : M \to \mathbb{C}$$

given by $h \to h(p)$. This is equivariant (with the trivial action of G on $\mathbb{C}$).

- Thus the kernel of $eval_p$ is a G-module.
- (reductivity) There is an invariant $h \in M$ such that $h(p) = 1$.

Thus $h(C_1) = 0$ and $h(C_2) = 1$ and h separates C_1 from C_2.

- Thus $V/[\cdot]$ is the collection of orbits separable by invariants.

Question : So, how big is $[v]$ for a $v \in V$?

- The biggest and most complicated $[v]$ is $[0]$, the *Null Cone*, an important feature of every group action. The 0-Orbit is the unique closed orbit in $[0]$.
- For the $X \rightarrow AXA^{-1}$, $[0]$ is precisely the collection of *Nilpotent Matrices* $\mathcal{N}$. For all $N \in \mathcal{N}$, $Tr(N^k) = 0$.
- Most points are stable, *but few tests to prove stability* .
- diagonal matrices are stable.
- $perm_n(X), det_n(X)$ as elements of $Sym^n(X)$ (on $n \times n$-matrices) are stable!

This is through the use of theory of one-parameter subgroups of G for taking limits, initiated by Hilbert, and then by Mumford and refined by Kempf.

$$\lambda : \mathbb{C}^* \rightarrow G$$

When $G = SL_m$ or GL_m, λ is conjugate to:

$$\lambda(t) = \begin{bmatrix} t^{n_1} & 0 & 0 & 0 \\ 0 & t^{n_2} & 0 & 0 \\ 0 & 0 & \vdots & 0 \\ 0 & 0 & 0 & t^{n_m} \end{bmatrix}$$

Hilbert: $v \in [0]$ iff there is a λ so that $\lim_{t \to 0} \lambda(t) \cdot v = 0$.

For example, when $X = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ for the action $X \to AXA^{-1}$:

$$\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} 0 & t^2 \\ 0 & 0 \end{bmatrix}$$

Thus $\lim_{t \to 0} \lambda(t) \cdot X = 0 \implies X \in [0]$.

Hilbert and 1-PS

- $v \in [0] \implies 0 \in \overline{O(v)}$, the orbit-closure. Easy.
- This implies that there is a *curve* $\lambda(t) \subset G$ such that $\lim \lambda(t) \cdot v = 0$. moderate.
- This implies there is a subgroup $\lambda(t)$! Tricky.

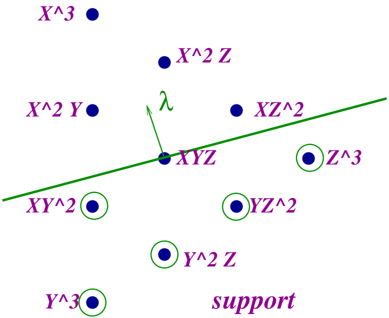
Hilbert used this most effectively to understand the null-cone for the action of GL_m on $Sym^d(X)$.

If $f \in [0]$ then there is a $g \in G$ and a $\lambda \in \mathbb{Z}^m$ so that $g \cdot f = \sum_d a_d X^d$ such that

- $\sum \lambda = 0$ (λ is code for $diag(t^{\lambda_1}, \ldots, t^{\lambda_m})$)and
- $\lambda \cdot d \leq 0 \implies a_d = 0$.

In other words, the polynomial may be arranged to have limited support.

Limiting support to a few monomials



Example : $f = 3X_1^2X_2^2 + X_1^3X_3 \in [0]$. We see that $d_1 = [220]$ and $d_2 = [301]$. The witness is $\lambda = [3, -2, -1]$.

Mumford and Kempf

Mumford : If v_0 is stable, and $v \in [v_0]$ then there is a $\lambda(t)$ such that (i) $\lim(\lambda(t) \cdot v)$ exists, and (ii) it is in $O(v_0)$.

$$\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} 1 & t^2 \\ 0 & 1 \end{bmatrix}$$

Thus $\lim_{t \to 0} \lambda(t) \cdot X = I \implies X \in [I]$.

Kempf : There is, in fact, *a unique most efficient* λ doing the job! Moreover:

- If H stabilizes v then $\lambda(t)$ commutes with H.

Proof: A quadratic programming formulation with integer entries. Optimum rational point is the answer.

Example revisited

Example : $f = 3X_1^2X_2^2 + X_1^3X_3 \in [0]$. We see that $d_1 = [220]$ and $d_2 = [301]$. One witness is $\lambda = [3, -2, -1]$.
λ is code for $X_1 \to t^3X_1, X_2 \to t^{-2}X_2$ and $X_3 \to t^{-1}X_3$. We have

$$X_1^2X_2^2 \to t^2X_1^2X_2^2 \qquad X_1^3X_3 \to t^8X_1^3X_3$$

Thus the *efficiency* is $2/\sqrt{3^2+2^2+1^2} \approx 0.6$.
Consider $[1, 0, -1]$ and we have efficiency as $2/\sqrt{2} > 1$. In fact, this is the most efficient λ.

Kempf

- Problem reduces to construction of a flag $0 \subseteq V_1 \subseteq \ldots \subseteq V_m = \mathbb{C}^m$.
- The flag with the most efficiency is "unique".
- Within a flag, problem is QP.

Stabilizers

$det_m(X)$ and $perm_m(X)$ are stable in $Sym^m(X)$, where X is the space of $m \times m$ matrices.

Stabilizers to the rescue.

- v unstable then there is λ_v most efficient.
- Clear that $g \cdot v$ unstable as well, also $\lambda_{g \cdot v} = g\lambda g^{-1}$.
- $h \cdot v = v$ implies h commutes with λ.
- λ_v commutes with stabilizer H.

det_m (and similarly $perm_m$) is stable

- But H for det_m includes $SL_m \times SL_m \to SL_{m^2} = SL(X)$.
- And $X = \mathbb{C}^m \otimes \mathbb{C}^m$ is H-irreducible.
- There is no *non-trivial* $\lambda \subseteq SL(X)$ commuting with H!

Groups and closed orbits

- Groups affect stability:
  - Orthogonal group: all orbits closed.
  - SL_m: some closed, GL_m: none closed.

- Cardboard polygons under translations and rotations: lengths, order
- Sets of coloured points in 3-space under permutation and translation and rotations: coloured distances
- Cardboard polygons under cut and paste: area
- 3-D polyhedra under cut and paste: length-angles

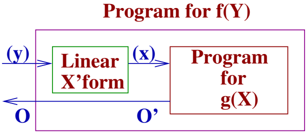
The $\preceq_{hom}$ and det_m and $perm_n$

Let $X = \{X_1, \ldots, X_r\}$.

For two form $f, g \in Sym^d(X)$, we say that $f \preceq_{hom} g$, if $f(X) = g(B \cdot X)$ where B is a fixed $r \times r$-matrix.

Note that:

- B may even be singular.
- $\preceq_{hom}$ is transitive.



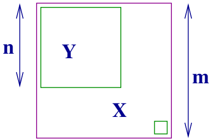
If there is an efficient algorithm to compute g then we have such for f as well.

- How is this related to orbits?
- How is this related to the usual 'reduction'?

The insertion

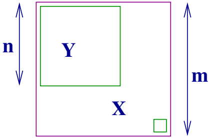
Suppose that $perm_n(Y)$ has a formula of size $m/2$. How is one to interpret Valiant's construction?

- Let Y be $n \times n$.
- Build a large $m \times m$-matrix X.
- Identify Y as its submatrix.



The "inserted" permanent

For $m > n$, we construct a new function $perm_n^m \in Sym^m(X)$.

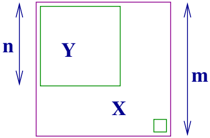


- Let Y be the principal $n \times n$-matrix of X.
- $perm_n^m = x_{mm}^{m-n} perm_n(Y)$

Thus $perm_n$ has been inserted into $Sym^m(X)$, of which $det_m(X)$ is a special element. Now, Valiant $\implies$ there is an $A(y)$ linear such that:

The "inserted" permanent

For $m > n$, we construct a new function $perm_n^m \in Sym^m(X)$.



- Let Y be the principal $n \times n$-matrix of X.
- $perm_n^m = x_{mm}^{m-n} perm_n(Y)$

Thus $perm_n$ has been inserted into $Sym^m(X)$, of which $det_m(X)$ is a special element. Now, Valiant $\implies$ there is an $A(y)$ linear such that:

- formula of size $m/2$ implies $perm_n = det_m(A(y))$
- Use x_{mm} as the homogenizing variable

Conclusion
$perm_n^m = det_m(A')$

$perm_n^m \preceq_{hom} det_m$

Group Action and $\preceq_{hom}$

Let $V = Sym^m(X)$. The group $GL(X)$ acts on V as follows. For $T \in GL(X)$ and $g \in V$

$$g_T(X) = g(T^{-1}X)$$

Two notions:

- The orbit: $O(g) = \{g_T | T \in SL(X)\}$.
- The projective orbit closure $\Delta(g) = \overline{cone(O(g))}$.

If $f \preceq_{hom} g$ then $f = g(B \cdot X)$, whence

- If B is full rank then f is in the $GL(X)$-orbit of g.
- If not, then B is approximated by elements of $GL(X)$.

Thus, in either case,

$$f \preceq_{hom} g \implies f \in \Delta(g)$$

The Δ

- Thus, we see that if $perm_n$ has a formula of size $m/2$ then $perm_n^m \in \Delta(det_m)$.

- On the other hand, $perm_n^m \in \Delta(det_m)$ implies that for every $\epsilon > 0$, there is a $T \in GL(X)$ such that $\|(det_m)_T - perm_n^m\| < \epsilon$. This yields a poly-time approximation algorithm for the permanent

Thus, we have an almost faithful algebraization of the formula size construction.

To show that $perm_5$ has no formula of size $20/2$, it suffices to show:

$$perm_5^{20} \notin \Delta(det_{20})$$

Naive Expectation : det_{20} is stable and so is $perm_5$. We have this great theory ... Invariants should do the job! OBSTRUCTION.

Problem 1 $perm_5$ may be stable, but $perm_5^{20}$ is NOT. It is in the null-cone.

$x_1^3 + x_2^3$ is stable in $Sym^2(\mathbb{C}^2)$ but $x_3^5(x_1^3 + x_2^3)$ is unstable in $Sym^8(\mathbb{C}^4)$.

Problem 2 $\Delta(det_{20})$ contains more than just the orbit and its scalar multiples.

Let $\lambda(t)$ be a 1-PS and let $\lambda(t) \cdot g = t^d f_d + t^{d+1} f_{d+1} + \ldots + t^m f_m$. Then $f_d, f_m \in \Delta(f)$. Thus, even for stable f, $\Delta(f)$ contains much more.

Two Questions

- Thus every invariant μ will vanish on $perm_n^m$.
- There is no invariant μ such that $\mu(det_m) = 0$ and $\mu(perm_n^m) \neq 0$.

Homogeneous invariants will never serve as obstructions. They dont even cut the null-cone

Two Questions:

- Is there any other system of functions which vanish on $\Delta(det_m)$?
- Can anything be retrieved from the superficial instability of $perm_n^m$?

Part II

- Is there any other system of functions which vanish on $\Delta(det_m)$?
  Yes. The Peter-Weyl argument.

- Can anything be retrieved from the superficial instability of $perm_n^m$?
  Yes. Partial or parabolic stability.

Two key ideas:

- **Representations as obstructions**
- **Stabilizers**

Philosophically-Two Parts

- Identifying structures where obstructions are to be found.
- Actually finding one and convincing others.

Two different types of problems:

- Geometric
  - Is the ideal of $\Delta(g)$ determined by representation theoretic data.
  - Does Σ_H generate the ideal of $\Delta(g)$?
  - Is the stabilizer H of g, G-separable?
    - ⋆ Larsen-Pink: do multiplicities determine subgroups?
  - More?
- Representation Theoretic
  - Is this G-module H-peter-weyl!

The subgroup restriction problem

- Given a G-module V, does $V|_H$ contain 1_H?
- Given an H-module W, does $V|_H$ contain W?

The Kronecker Product Consider $H = SL_r \times SL_s \to SL_{rs} = G$, when does $V_\mu(G)$ contain an H-invariant?

This, we know, is a very very hard problem. But this is what arises (with $r = s = m$) when we consider det_m and there may well be a hope...

The subgroup restriction problem

- Given a G-module V, does $V|_H$ contain 1_H?
- Given an H-module W, does $V|_H$ contain W?

The Kronecker Product Consider $H = SL_r \times SL_s \to SL_{rs} = G$, when does $V_\mu(G)$ contain an H-invariant?

This, we know, is a very very hard problem. But this is what arises (with $r = s = m$) when we consider det_m and there may well be a hope...

through Quantum Groups!

Any more geometry?

- The Hilbert-Mumford-Kempf flags: limits for affine closures.
  - Extendable to projective closures?
    $\lambda = [\lambda_1, \ldots, \lambda_m]$,

    $$f(t^{\lambda_1} X_1, \ldots, t^{\lambda_m} X_m) = t^d f_d + \ldots + t^e f_e$$

  - Kempf: if $d \geq 0$ then there is a unique best λ: convex programming.
  - general d?: Let $\Lambda(f, S, G) = \{\lambda \in G | ld(\lambda, f) \in S\}$.
  - Is there a best $\lambda \in \Lambda(f, S, G)$? in $\Lambda(f, S, T)$?
    Something there, but convexity of the optmization problem ...?

The Luna-Vust theory

Local models for stable points.

- Tubular neighbourhoods of stable orbits look like $G \times_H N$.
- Corollary: stabilizers of nearby points subgroups of H upto conjugation.
- Extendable for partially stable points, i.e., when H is not semisimple?
- $H = RU$ a Levi factorization and (i) N, an R-module, (ii) $\phi : N \times \mathcal{G} \to V$, an R-equivariant map.
- A finite lie-algebra local model exists but ...

Another problem-Strassen

Links invariant theory to computational issues.

- Consider the 2×2 matrix multiplication $AB = C$. To compute C, we seem to need the 8 bilinear forms $a_{ij} b_{jk}$.
- Can we do it in any fewer?

A bilinear form on A, B is rank 1 if its matrix is of rank 1. Let S denote the collection of all rank 1 forms.

- Let $S^k = S + S + \ldots + S$ (k times). These are the so called secant varieties.
- Strassen showed that S^7 contains all the above 8 bi-linear forms.

Consequence

There is an $n^{2.7}$-time algorithm to do matrix multiplication.

Specific to Permanent-Determinant

Negative Results

- von zur Gathen: $m > c \cdot n$
  - Used the singular loci of *det* and *perm*.
  - Combinatorial arguments.
- Raz: $m > p(n)$, but multilinear case.
- Ressayre-Mignon: $m > c \cdot n^2$
  - Used the curvature tensor.

For a point $p \in M$, hyper-surface $\kappa : TP_m \to TP_m$.

- For any point of det_m, $rank(\kappa(det_m)) \leq m$.
- For one point of $perm_n$, $rank(\kappa(perm_n)) = n^2$.
- A section argument.

Thank you.