Geometric Complexity Theory
Milind Sohoni¹

An approach to complexity theory
via
Geometric Invariant Theory.

¹joint work with Ketan Mulmuley
Talk Outline

- Mainly Valiant
- Mainly stability and obstructions
- Mainly Representations
- Largely hard
The satisfiability problem

- Boolean variables $x_1, \ldots, x_n$
- Term $t_1 = (\neg x_1 \lor x_3 \lor x_7)$, and so on up to $t_m$.
- Formula $t_1 \land t_2 \land \ldots \land t_m$

Question: Decide if there is a satisfying assignment to the formula.

There is no known algorithm which works in time polynomial in $n$ and $m$.

Harder Question: Count the number of satisfying assignments. Thus we have the decision problem and its counting version.
Matchings

**Question**: Given a bipartite graph on $n$, $n$ vertices, check if the graph has a complete matching.

This problem has a known polynomial time algorithm.

**Harder Question**: Count the number of complete matchings.

- There is no known polynomial time algorithm to compute this number.
- Even worse, there is no proof of its non-existence.

Thus, there are decision problems whose counting versions are hard.
The permanent

If $X$ is an $n \times n$ matrix, then the permanent function is:

$$perm_n(X) = \sum_{\sigma} \prod_{i} x_{i,\sigma(i)}$$

The relationship with the matching problem is obvious. When $X$ is 0-1 matrix representing the bipartite graph, then $perm(X)$ counts the number of matchings.

- There is no known polynomial time algorithm to compute the permanent, and worse, no proof of its non-existence.
- The function $perm_n$ is #$P$-complete. In other words, it is the hardest counting problem whose decision version is easy to solve.
Our Thesis

- Non-existence of algorithm $\implies$ existence of a mathematical structure (obstructions)
- These happen to arise in the GIT and Representation Theory of Orbits.

**CAUTION**: There are plenty of NP-complete problems in Representation Theory. But that's not what we are saying.

**Example**

- **Hilbert Nullstellensatz**: Either polynomials $f_1, \ldots, f_n$ have a common zero, or there are $g_1, \ldots, g_n$ such that

  $$f_1g_1 + \ldots + f_ng_n = 1$$

- Thus $g_1, \ldots, g_n$ obstruct $f_1, \ldots, f_n$ from having a common zero.
Other #$P$-complete problems

- Compute the Kostka number $K_{\lambda \mu}$.
- Compute the Littlewood-Richardson number $c^\nu_{\lambda, \mu}$.

Note that there are polynomial time algorithms to check non-zero-ness.

We will stick with the permanent.

- homogeneous polynomial, i.e., in $\text{Sym}^n(X)$,
- Distinguished stabilizer within $\text{GL}(X)$:

$$\text{perm}(X) = \text{perm}(PXQ) \quad \text{perm}(X) = \text{perm}(D_1XD_2)$$

- $P, Q$ permutation matrices, $D_1, D_2$ diagonal matrices.
Let $p(X_1, \ldots, X_n)$ be a polynomial. A formula is a particular way of writing it using $\ast$ and $+$. 

$$
\text{formula} = \text{formula} \ast \text{formula} \mid \text{formula} + \text{formula}
$$

- Thus the same function may have different ways of writing it.
- The number of operations required may be different.

Example:

- $a^3 - b^3 = (a - b)(a^2 + a \ast b + b^2)$.
- Van-der-Monde $(\lambda_1, \ldots, \lambda_n) = \prod_{i \neq j}(\lambda_i - \lambda_j)$.

Formula size: the number of $\ast$ and $+$ operations.

- LHS1 is 5, RHS1 is 7, RHS2 is $2n$. 
Formula size

- A formula gives a formula tree.
- This tree yields an algorithm which takes time proportional to formula size.

Does $perm_n$ have a formula of size polynomially bounded in $n$? (This also implies a polynomial time algorithm)

Valiant’s construction: converts the tree into a determinant.
Valiant’s Construction

If $p(Y_1, \ldots, Y_k)$ has a formula of size $m/2$ then,

- There is an inductively constructed graph $G_p$ with at most $m$ nodes, with edge-labels as (i) constants, or (ii) variable $Y_i$.
- The determinant $\det(A_p)$ of the adjacency matrix of $G_p$ equals $p$.

A simple formula. The general case. Addition
The Matrix

In other words:

\[ p(Y_1, \ldots, Y_k) = \text{det}_m(A) \]

where \( A_{ij}(Y) \) is a degree-1 expression on \( Y \).

For our example, we have:

\[
A = \begin{bmatrix}
0 & 1 & 0 \\
0 & 1 & y \\
1 & 0 & 0
\end{bmatrix}
\]

\( \text{det}(A) = y \)

- Note that in Valiant’s construction \( A_{ij} = Y_r \) or \( A_{ij} = c \).

formula size = \( m/2 \) \( \implies \) \( p(Y) = \text{det}_m(A) \)
The homogenization

Lets homogenize the above construction:
- Add an extra variable $Y_0$.
- Let $p^m(Y_0, \ldots, Y_k)$ be the degree-$m$ homogenization of $p$.
- Homogenize the $A_{ij}$ using $Y_0$ to $A'_{ij}$.

We then have: $p^m(Y_0, \ldots, Y_k) = \det_m(A')$

For our small example:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & y \\ 1 & 0 & 0 \end{bmatrix} \quad A' = \begin{bmatrix} 0 & y_0 & 0 \\ 0 & y_0 & y \\ y_0 & 0 & 0 \end{bmatrix} \quad \det(A') = y_0^2 y$$
If a form $p(Y)$ has a formula of size $m/2$ then

- There is an $m \times m$-matrix $A$ with linear entries
  \[ \det(A) = p(Y) \]

- There is an $m \times m$-matrix $A'$ with homogeneous linear entries
  \[ \det(A') = p^m(Y) \]

where $p^m$ is the $m$-homogenization of $p$. 
The $\preceq_{hom}$

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

For two form $f, g \in \text{Sym}^d(X)$, 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.
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 \( perm^m_n \in Sym^m(X) \).

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

Thus \( perm_n \) has been inserted into \( Sym^m(X) \), of which \( det_m(X) \) is a special element.
The "inserted" permanent

For $m > n$, we construct a new function $\text{perm}_n^m \in \text{Sym}^m(X)$.

- Let $Y$ be the principal $n \times n$-matrix of $X$.
- $\text{perm}_n^m = x^m_{mm} \text{perm}_n(Y)$

Thus $\text{perm}_n$ has been inserted into $\text{Sym}^m(X)$, of which $\text{det}_m(X)$ is a special element.

- formula of size $m/2$ implies $\text{perm}_n = \text{det}_m(A)$
- Use $x_{mm}$ as the homogenizing variable

Conclusion

$\text{perm}_n^m = \text{det}_m(A')$

$\text{perm}_n^m \preceq_{\text{hom}} \text{det}_m$
Group Action and $\leq_{\text{hom}}$

Let $V = \text{Sym}^m(X)$. 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: $O(g) = \{g_T \mid T \in SL(X)\}$.
- The projective orbit closure $\Delta(g) = \text{cone}(O(g))$.

If $f \leq_{\text{hom}} g$ 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 $A$ is approximated by elements of $GL(X)$.

Thus, in either case,

$$f \leq_{\text{hom}} g \implies f \in \Delta(g)$$
Thus, we see that if \( \text{perm}_n \) has a formula of size \( m/2 \) then \( \text{perm}_n^m \in \Delta(\text{det}_m) \).

On the other hand, \( \text{perm}_n^m \in \Delta(\text{det}_m) \) implies that for every \( \epsilon > 0 \), there is a \( T \in GL(X) \) such that \( \|(\text{det}_m)_T \) \( - \text{perm}_n^m \| < \epsilon \). This yields a poly-time approximation algorithm for the permanent.

Thus, we have an almost faithful algebraization of the formula size construction.
The Obstruction and its existence

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

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

In other words:

- $\mathcal{V}$ is a $GL(X)$-module.
- $f$ and $g$ are special points.
- What is the witness to $f \notin \Delta(g)$?

It is clear that such witnesses or obstructions exist in the coordinate ring $k[\mathcal{V}]$.

What is the structure of such obstructions?
The Obstruction

So let $g, f \in V = Sym^d(X)$. How do we show that $f \notin \Delta(g)$.

- Exhibit a homogeneous polynomial $\mu \in Sym^r(V^*)$ which vanishes on $\Delta(g)$ but not on $f$.

This $\mu$ is then the required obstruction. We would need to show that:

- $\mu(f) \neq 0$.
- $\mu(g_T) = 0$ for all $T \in SL(X)$.

Check $\mu$ on every point of $\text{Orbit}(g)$

False start: Use the $SL(X)$-invariant elements of $Sym^d(V^*)$ for constructing such a $\mu$. 
Invariants

- $V$ is a space with a group $G$ acting on $V$.
- $\text{Orbit}(v) = \{ g.v | G \in G \}$.
- Invariant is a function $f : V \to \mathbb{C}$ which is constant on orbits.

Existence and constructions of invariants has been an enduring interest for over 150 years.

Example:
- $V$ is the space of all $m \times m$-matrices.
- $G = GL_m$ and $g.v = gvg^{-1}$.
- Invariants are the coefficients of the characteristic polynomial.
Invariants and orbit separation

To show that $f \not\in \Delta(g)$

Exhibit a homogeneous invariant $\mu$ which vanishes on $g$ but not on $f$. This $\mu$ would then be the desired obstruction.

- Easy to check if a form is an invariant.
- Easy to construct using age-old recipes.
- Easy to check that $\mu(g) = 0$ and $\mu(f) \neq 0$.

$$\mu(g) = 0 \implies \mu(g_T) = 0 \implies \mu(\Delta(g)) = 0$$

Important Fact

If $g$ and $f$ are stable and $f \not\in \Delta(g)$, then there is a homogeneous invariant $\mu$ such that $\mu(g) \neq \mu(f)$. 

April 19, 2007 22 / 47
Stability

- $g$ is stable iff $SL(X)$-Orbit($g$) is Zariski-closed in $V$.

- Most polynomials are stable.

- It is difficult to show that a particular form is stable.

**Hilbert**: Classification of unstable points.

- For matrices under conjugation, precisely the diagonal matrices are stable.

  $perm_m$ and $det_n$ are stable.

**Proof**:

- Kempf’s criteria.

- Based on the stabilizers of the determinant and permanent.
Rich Stabilizers

The stabilizer of the determinant:
- The form $\text{det}_m(X)$:
  - $X \rightarrow AXB$
  - $X \rightarrow X^T$
- $\text{det}_m \in \text{Sym}^m(X)$ determined by its stabilizer.

The stabilizer of the permanent:
- The form $\text{perm}_m(X)$:
  - $X \rightarrow PXQ$
  - $X \rightarrow D_1XD_2$
  - $X \rightarrow X^T$
- $\text{perm}_m \in \text{Sym}^m(X)$ determined by its stabilizer.

Tempting to conclude that the homogeneous obstructing invariant $\mu$ now exists.
The Main Problem

Recall we wish to show

\[ perm_n^m \notin \Delta(det_m) \]

where

\[ perm_n^m = x_{mm}^{m-n} perm(Y). \]

\( perm_n^m \) is unstable, in fact in the null-cone, for very trivial reasons.

- Added an extra degree equalizing variable.
- Treated as a polynomial in a larger redundant set of variables.
Two Questions

Thus every invariant $\mu$ will vanish on $\text{perm}^m_n$.
There is no invariant $\mu$ such that $\mu(\det_m) = 0$ and $\mu(\text{perm}^m_n) \neq 0$.

Homogeneous invariants will never serve as obstructions.

Two Questions:

Is there any other system of functions which vanish on $\Delta(\det_m)$?
Can anything be retrieved from the superficial instability of $\text{perm}^m_n$?
Part II

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

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

Representations as obstructions
Stabilizers
Question 1

Is there any other system of functions which vanish on $\Delta(det_m)$ and enter the null-cone?

- We use the stabilizer $H \subseteq SL(X)$ of $det_m$.
- For a representation $V_\lambda$ of $SL(X)$, we say that $V_\lambda$ is $H$-admissible iff $V_\lambda^*|_H$ contains the trivial representation $1_H$.

For $g$ stable:

**Fact**: $k[\text{Orbit}(g)] \cong k[G/H] \cong \sum_\lambda H$-admissible $n_\lambda V_\lambda$

**Thankfully**: $k[\Delta(g)] \cong \sum_\lambda H$-admissible $m_\lambda V_\lambda$

Thus a fairly restricted class of $G$-modules will appear in $k[\Delta(g)]$. We use this to generate some elements of the ideal for $\Delta(g)$. 
Consider next the $G$-equivariant surjection:

$$\phi : k[V] \to k[\Delta(g)]$$

We see that (i) $\phi$ is a graded surjection, and (ii) if $V_\mu \subseteq k[V]^d$ is not $H$-admissible, then $V_\mu \in \ker(\phi)$.

Let $\Sigma_H$ be the ideal generated by such $V_\mu$ within $k[V]$. Clearly $\Sigma_H$ vanishes on $\Delta(g)$.

How good is $\Sigma_H$?
The Local Picture

**G-separability:** We say that $H \subseteq G$ is $G$-separable, if for every non-trivial $H$-module $W_\alpha$ such that:

- $W_\alpha$ appears in some restriction $V_\lambda|_H$.

then there exists a $H$-non-admissible $V_\mu$ such that $V_\mu|_H$ contains $W_\alpha$.

**Theorem:** Let $g$ and $H$ be as above, with (i) $g$ stable, (ii) $g$ only vector in $V$ with stabilizer $H$, and (iii) $H$ is $G$-separable. Then for an open subset $U$ of $V$, $U \cap \Delta(g)$ matches $(k[V]/\Sigma_H)_U$. 
Applying this ...

The conditions: (i) stability of $g$, (ii) $V^H = \langle g \rangle$ and (iii) $G$-separability of $H$.

- $det_m$ and $perm_n$ satisfy conditions (i) and (ii) above.
- For $n = 2$, stabilizer of $det_2$ is indeed $SL_4$-separable.
- For $V = \bigwedge^d$ and $g$ the highest weight vector, $\Delta(g)$ is the grassmanian. For this $\Sigma_H$ generates the ideal.
- For $g = det_m$, the data $\Sigma_H$ does indeed enter the null-cone.

Still open:

- Look at $H = SL_n \times SL_n$ sitting inside $G = SL_{n^2}$. Is $H$ $G$-separable?
- Does $\Sigma_H$ determine $\Delta(det_m)$?
To conclude on Question 1

- Stabilizer yields a rich set $\Sigma_H$ of relations vanishing on $\Delta(det_m)$.
- Given $G$-separability, $\Sigma_H$ does determine $\Delta(det_m)$ locally.

Now suppose that $\text{perm}_n^m \in \Delta(det_m)$ then:

- Look at the surjection $k[\Delta(det_m)] \rightarrow k[\Delta(\text{perm}_n^m)]$.

$V_\mu \subseteq k[\Delta(\text{perm}_n^m)]$ and $V_\mu$ non-$H$-admissible, then $V_\mu$ is the required obstruction.

If $k[\Delta(\text{perm}_n^m)]$ is understood then this sets up the representation-theoretic obstruction.
Can anything be retrieved from the superficial instability of $\text{perm}_n^m$?

Let’s consider the simpler function $f = \text{perm}(Y) \in \text{Sym}^n(X)$, i.e., with useful variables $Y$ and useless $X - Y$.

- Let parabolic $P \subseteq \text{GL}(X)$ fix $Y$.
- $P = LU$, with $U$ the unipotent radical.

We see that:
- $f$ is fixed by $U$.
- $f$ is $L$-stable.
The form $f$

Recall $f = perm(Y) \in V = Sym^n(X)$ and $P$ fixing $Y$. We see that $f$ is partially stable with $R = L = GL(Y) \times GL(X - Y)$.

With $W = Sym^n(Y)$, we have the $P$-equivariant diagrams:

$$
\begin{array}{ccc}
W & \overset{\iota}{\rightarrow} & V \\
\Delta_W(f) & \overset{\iota}{\rightarrow} & \Delta_V(f) \\
\downarrow & & \downarrow \\
k[W]^d & \overset{\iota^*}{\leftarrow} & k[V]^d \\
k[\Delta_W(f)]^d & \overset{\iota^*}{\leftarrow} & k[\Delta_V(f)]^d
\end{array}
$$

where $\Delta_W(f)$ is the projective closure of the $GL(Y)$-orbit of $f$, and $\Delta_V(f)$ is that of the $GL(X)$-orbit of $f$. 

**The Theorem**

### Lifting

- The $GL(X)$-module $V_\mu(X)$ occurs in $k[\Delta_V(f)]^{d*}$ iff $(V_\mu(X))^U$ is non-zero. Thus the $GL(Y)$-module $V_\mu(Y)$ must exist.

- Next, the multiplicity of $V_\mu(X)$ in $k[\Delta_V(f)]^{d*}$ equals that of $V_\mu(Y)$ in $k[\Delta_W(f)]^{d*}$.

Now recall that $f = perm_m(Y)$, and let $K = stabilizer(f) \subseteq GL(Y)$.

**But $f$ is $GL(Y)$-stable, and**

- the $GL(Y)$-modules which appear in $k[\Delta_W(f)]^d$ must be $K$-admissible.
The Grassmanian

Consider $V = V_{1k}(\mathbb{C}^m) = \wedge^k(\mathbb{C}^m)$ and the highest weight vector $v$.

- $v$ is stable for the $GL_k \times GL_{m-k}$ action.
- $\Delta_V(v)$ is just the grassmanian.
- $v$ is partially stable with the obvious $P$.
- $W = \mathbb{C}^k \subseteq \mathbb{C}^m$ and $\Delta_W(v)$ is the line through $v$.
- Whence
  \[
  k[\Delta_W(v)] = \sum_d \mathbb{C}
  \]
- The above theorem subsumes the Borel-Weil theorem:
  \[
  k[\Delta_V(v)] \cong \sum_d V_{dk}(\mathbb{C}^m)
  \]
The general partially stable case

Recall: Let $V$ be a $G$-module. Vector $v \in V$ is called partially stable if there is a parabolic $P = LU$ and a regular $R \subseteq L$ such that:
- $v$ is fixed by $U$, and
- $v$ is $R$-stable.

In the general case, there is a regular subgroup $R \subseteq L$, whence the theory goes through

$$\Delta_W(v) \rightarrow \Delta_Y(v) \rightarrow \Delta_V(v)$$

- The first injection goes through a Pieri branching rule.
- The second injection follows the lifting theorem.
In Summary

The General Conclusion

In other words, the theory of partially-stable $\Delta_V(f)$ lifts from that of the stable case $\Delta_W(f)$.

The crucial problem therefore is to understand $\Delta_W(f)$ or $\Delta_V(g)$, i.e., the stable case. There, for its geometry, we have:

- Is the stabilizer $H$ of $g$, $G$-separable?
  - Larsen-Pink: do multiplicities determine subgroups?
- Does $\Sigma_H$ generate the ideal of $\Delta(g)$?
The Representation-theoretic Obstruction

Let $H \subseteq GL(X)$ stabilize $\det_m$ and $K \subseteq GL(Y)$ stabilize $\text{perm}_m^n$.

The representation-theoretic obstruction $V^*_\mu(X)$ for $\text{perm}_n^m \in \Delta(\det_m)$

- $V_\mu(X)|_H$ must have a $H$-fixed point.
- $V_\mu(X)^U$ is non-zero.
- $V_\mu(Y, y)|_R$ does not have a $K$-fixed point.
The lower-bounds?

Question: How does this relate \( m \) and \( n \)?

- \( V_\mu(X)|_H \) must have a \( H \)-fixed point.
- \( V_\mu(X)^U \) is non-zero.
- \( V_\mu(Y, y)|_R \) does not have a \( K \)-fixed point.

- The representation \( V_\mu(Y, y) \) is of width \( n^2 \) which is smaller than \( m^2 = |X| \).
- If \( m \gg n \) then \( \mu \) is really thin, and an obstruction may not exist.
The lower-bounds?

**Question**: How does this relate $m$ and $n$?

- $V_\mu(X)|_H$ must have a $H$-fixed point.
- $V_\mu(X)^U$ is non-zero.
- $V_\mu(Y, y)|_R$ does not have a $K$-fixed point.

- The representation $V_\mu(Y, y)$ is of width $n^2$ which is smaller than $m^2 = |X|$.
- If $m \gg n$ then $\mu$ is really thin, and an obstruction may not exist.
- and a formula may exist.
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 $det_m$. 
Any more geometry?

Is there any more geometry which will help?

- **The Hilbert-Mumford-Kempf flags**: limits for affine closures.
  - Extendable to projective closures?
  - Something there, but convexity of the optimization problem breaks down.

- **The Luna-Vust theory**: local models for stable points.
  - Extendable for partially stable points?
  - A finite limited local model exists, but no stabilizer condition seems to pop out.
Specific to Permanent-Determinant

**Negative Results**

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

**Positive results**

- **Jerrum-Sinclair-Vigoda**: The permanent can be approximated by a randomized algorithm
The Subgroup Restriction Problem

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

Similar(?) problems recently solved (in Littlewood-Richardson coefficients $c^\nu_{\lambda,\mu}$):

- **The PRV-conjecture** on the non-zeroness of certain $c^\nu_{\lambda,\mu}$.
  - The Drinfeld-Jimbo quantized Lie algebras.
  - The crystal bases for modules.

- **The saturation conjecture**: $c^{n\nu}_{n\lambda,n\mu} \neq 0 \implies c^\nu_{\lambda,\mu} \neq 0$.
  - A polynomial-time non-combinatorial algorithm to detect if $c^\nu_{\lambda,\mu} \neq 0$. 
The Kronecker Product  For $X = V \otimes W$, is there a quantized structure and an injection $H = GL_q(V) \times GL_q(W) \hookrightarrow GL_q(X) = G$ 

- For the standard quantizations, no such injection exists.
- However, there maybe a different quantization $GL_q(\overline{X})$ which:
  - for which the injection above is natural
  - is (co)-semisimple
  - which has a representation theory following $GL_q(X)$

This is investigated in GCT 4 (under preparation).
In Conclusion

- **Complexity Theory questions** and projective orbit closures.
  - stable and partially stable points.
  - obstructions
- **obstruction existence**
  - Representations as obstructions
  - Distinctive stabilizers
  - local definability of $\text{Orbit}(g)$
- **partial stability**
  - lifting theorems
- **subgroup restriction problem**
  - tests for non-zero-ness of group-theoretic data
Thank you.