Geometric Complexity Theory

Patrick Lei

UMass CS Theory Seminar

October 22, 2019

Abstract

Geometric complexity theory, introduced by Ketan Mulmuley, relates complexity-theoretic problems to problems in representation theory and algebraic geometry. We present the basic ideas of GCT and discuss relationships to interesting problems in mathematics.

Notation and Basic Notions

Throughout, all geometry and algebra is over $\mathbb{C}$. Given a vector space V of finite dimension, the k-th symmetric power of V is $V^{\otimes k}/(a \otimes b - b \otimes a)$ and is denoted by $\operatorname{Sym}^k V$. The dual space $\operatorname{Hom}(V, \mathbb{C})$ is denoted by V^*.

Recall that projective space is denoted by $\mathbb{P}^n = Gr(1, n+1) = (\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^*$. Alternatively, $\mathbb{P}^n$ is the algebraic variety associated to the graded ring $\mathbb{C}[x_0, \ldots, x_n]$.

1 Complexity Theory and Logic Review

From the outside, the goal of complexity theory seems to be singularly focused on proving that P $\neq$ NP.[1] Part of the difficulty of solving this problem is that any proof technique that relativizes is not strong enough to resolve P vs NP. In fact, any so-called "natural proof" will not resolve P vs NP.

Now recall some standard facts from foundations:

Theorem 1 (Gödel's Incompleteness Theorem)**.** *Any consistenf formal system F that contains PA cannot prove its own consistency.*

Because P vs NP is a universal hardness statement, it can potentially preclude its own proof and thus be independent of ZFC. We will need to restate problems in complexity theory in a way that resolves the logical obstruction.

Specifically, we implement what Mulmuley calls a "flip." In addition, we will attempt to find explicit proofs of statements. Logically, we have

$$A \neq B \leftrightarrow \exists \text{ obstruction for } B \text{ w.r.t } A.$$

Definition 2. A technique for separating NP from *P/poly* (using a problem $f(X)$) is called a *flip* if there exists a family $\mathcal{O} = \{\mathcal{O}_{m,n}\}$ of obstruction labels satisfying:

F0 (short) Obstructions are polynomial in m, n.

F1 (easy to decode) Every obstruction $s \in \mathcal{O}_{m,n}$ gives a set $S_{m,n}(s)$ of small global obstructions to efficient computation of $f(X)$ that can be computed in polynomial time.

F2 (rich) For every $n, m = n^{O(1)}$, $\mathcal{O}_{m,n}$ contains at least $2^{\Omega(m)}$ disjoint obstructions.

F3 (easy to verify) Checking whether s is a valid obstruction string is in P.

F4 (easy to construct) Constructing an obstruction string $s_{m,n} \in \mathcal{O}_{m,n}$ can be done in polynomial time.

The following provides justification for attempting to find an explicit proof.

Theorem 3 (Flip Theorem)**.** *The arithmetic nonuniform P vs NP conjecture has an extremely explicit proof assuming that it is true and that polynomial identity testing can be derandomized.*

[1] Compare this to analytic number theory and the Riemann Hypothesis.

Proof of this is omitted and can be found in [GCTflip].

One problem with the logical statement above is that we translated the original problem into an equivalent positive hypothesis. We need to decompose our hard problem into subproblems that are easier. For an example, parity was shown to not be in AC^0 by proving two lemmas:

1. AC^0 is easy to approximate by low degree polynomials.
2. Parity cannot be approximated by low degree polynomials.

2 Constructing Geometric Obstructions

Our general approach is as follows:

1. To each complexity class, associate a complete problem for that class.
2. To each problem, associate a projective algebraic variety.
3. From each projective algebraic variety, extract representation-theoretic data.

I will explain what all of these terms mean later, but first we will perform this construction.

Our problems will be (1) computing the permanent and (2) computing the determinant.

Definition 4. Let $M \in M_n(\mathbb{C})$. Then the *permanent* $\operatorname{perm}(M)$ is defined by

$$\operatorname{perm}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} M_{i,\sigma(i)}.$$

Note the similarity to the definition of the determinant.

Our goal is to show that the permanent of A cannot be represented as the determinant of a larger matrix B whose entries are linear in the entries of A.

Definition 5. Define the *padded permanent* of an $n \times n$ matrix M by

$$\operatorname{perm}_n^m(M) = z^{m-n}\operatorname{perm}(M).$$

Let $Y = M_m(\mathbb{C}) \simeq \mathbb{C}^{m^2}$. We will identify $X = M_n(\mathbb{C}) \simeq \mathbb{C}^{n^2}$ with the bottom right corner of Y. Consider the vector space $V = \mathbb{C}[Y]_m = \operatorname{Sym}^m Y^*$, which is the space of degree m homogeneous polynomials in the coordinates of Y. This has a natural $G = GL_{m^2}(\mathbb{C})$-action given by $\sigma(f(y)) = f(\sigma^{-1}y)$.

Also observe that both $\det, \operatorname{perm}_n^m \in V$. Now we consider the projective space $\mathbb{P}(V)$, which contains points corresponding to $\det, \operatorname{perm}_n^m$. Now we construct the two varieties

$$\chi(\det_m) = \overline{GL_n(\mathbb{C}).\det_m} \subset \mathbb{P}(V)$$
$$\chi(\operatorname{perm}_n^m) = \overline{GL_n(\mathbb{C}).\operatorname{perm}_n^m} \subset \mathbb{P}(V).$$

Here, the closure is taken in the *Zariski topology.*

Definition 6. Let $I \subset \mathbb{C}[x_0, \ldots, x_n]$ be a homogeneous ideal. Then the *vanishing set* $\mathcal{Z}(I) \subset \mathbb{P}^n$ is defined by

$$\mathcal{Z}(I) = \{x \in \mathbb{P}^n \mid f(x) = 0 \forall f \in I\}.$$

Definition 7. The *Zariski topology* on $\mathbb{P}^n$ is defined by the closed sets being the vanishing sets of homogeneous ideals.

Proof that this forms a topology can be found in any standard introductory text in algebraic geometry.

Proposition 8. *If the permanent can be represented as the determinant of a larger, related matrix, then* $\chi(\operatorname{perm}_n^m) \subset \chi(\det_m)$.

This suggests the following conjecture:

Conjecture 9. *If $m = n^{O(1)}$, then*

$$\chi(\text{perm}_n^m) \not\subseteq \chi(\underset{m}{\det}).$$

These geometric objects appear to be completely intractable to compute with. This is a problem if we are to construct a geometric obstruction to the permanent vs determinant problem. Fortunately, to our algebraic varieties, we can associate algebraic information, namely a homogeneous ideal and a graded ring.

Definition 10. For any projective algebraic variety $X \subset \mathbb{P}^n$, its *ideal* $I(X)$ is defined to be the ideal generated by the set of homogeneous polynomials that vanish on X.

Definition 11. The *homogeneous coordinate ring* $R(X)$ of a projective variety $X \subset \mathbb{P}^n$ is given by $R(X) = \mathbb{C}[x_0, \ldots, x_n]/I(X)$. Equivalently, $X = \text{Proj}\,\mathbb{C}[x_0, \ldots, x_n]/I(X)$.

Observe that the varieties $\chi(\text{perm}_n^m), \chi(\det_m)$ both have a natural action by G. This action lifts to their homogeneous coordinate rings. In addition, the action of G respects the gradings of the two rings. This allows us to use the following theorem:

Theorem 12. *Let G be a reductive algebraic group over $\mathbb{C}$. Then any finite-dimensional representation of G splits as a direct sum of irreducible representations.*

Because $G = GL_n(\mathbb{C})$ is reductive, we can attempt to find a geometric obstruction.

Definition 13. A *geometric obstruction* is an irredicible representation V_λ that contained in $R(\chi(\text{perm}_n^m))^*$ but not in $R(\chi(\det_m))^*$.

By more recent results, this is very unlikely to exist. We attempt to find a weaker geometric obstruction:

Definition 14. A *relaxed geometric obstruction* is an irreducible representation V_λ that occurs as a subrepresentation of G in $I(\det_m)/(I(\det_m) \cap I(\text{perm}_n^m))$.

Naturally, we make the following conjecture:

Conjecture 15. *A geometric obstruction exists if $m = n^{O(1)}$.*

We do have a lower bound:

Theorem 16. *An explicit relaxed geometric obstruction V_λ exists when $m \leq n^2/2$.*

3 Approach to Proof and Remarks

For general functions f, g, constructing an explicit obstruction is intractable because computing Gröbner bases is EXPTIME-complete. However, there is some hope because of the special nature of the permanent and the determinant. In particular,

Theorem 17 (Strong Flip)**.** *Suppose Conjecture 9 holds and that black box determinant identity testing can be derandomized. Then Conjecture 9 has an explicit proof satisfying the flip axioms and an additional property.*

Explicit separators of small dimension can be constructed, but only between very special kinds of varieties. This can be done using invariant theory, but they have very low complexity. The problem of explicit construction of separators seems beyond the reach of current algebraic geometry.

We can define analogues of the flip axioms for the permanent and determinant. Once we do this, the problem becomes the two flip hypotheses and Conjecture 15.[2]

How do we prove the flip hypotheses? Using representation theory. We recall some facts from representaiton theory.

Theorem 18 (Weyl)**.** *The irreducible representations of $GL_n(\mathbb{C})$ are given by sequences of integers $\lambda = (\lambda_1 \geq \cdots \geq \lambda_k > 0)$ for $k \leq n$, where k is the length of λ.*

Definition 19. Given sequences α, β, λ, the *Littlewood-Richardson coefficient* $c_{\alpha,\beta}^{\lambda}$ is the multiplicity of V_λ in the tensor product $V_\alpha \otimes V_\beta$.

[2]For a more detailed discussion, see Mulmuley's articles.

Define the associated stretching function $\widetilde{c}^{\lambda}_{\alpha,\beta}(k) = c^{k\lambda}_{k\alpha,k\beta}$. This is known to be a polynomial in k with nonnegative coefficients. Also, we know that

Proposition 20 (Littlewood-Richartson rule)**.** *There exists an explicit polytope P such that $\widetilde{c}^{ambda}_{\alpha,\beta}(k)$ is the number of integer points in the polytope kP.*

We also know that

Proposition 21. *Deciding nonvanishing of Littlewood-Richartson coefficients is in P.*

Now we need to lift this story to GCT. First we set$F_{\lambda,n,m}(k)$ to be the number of copies of $V_{k\lambda}$ that live on $\chi(\text{perm}_n^m)$. Also let $G(\lambda, m)(k)$ denote the number of copies of $V_{k\lambda}$ that live on $\chi(\det_m)$. Also, for a polytope P, let $f_P(k)$ denote the number of integer points in kP. The main conjecture towards GCT is the following:

Conjecture 22 (Positivity Hypothesis (PH1))**.**

1. *For every $\lambda, n, m \geq n$, there exists an explicit polytope $P_{\lambda,n,m}(k)$ such that $F_{\lambda,n,m}(k) = f_P(k)$.*
2. *For every λ, m, there exists an explicit polytope $Q_{\lambda,m}(k)$ such that $G_{\lambda,m}(k) = f_Q(k)$.*

Remark 23. If these polytopes exist, they have dimension polynomial in n as long as λ has polynomial length.

Assuming PH1 and a "saturation hypothesis", we can prove

Theorem 24. *Given λ, n, m, and k' sufficiently large, then nonvanishing of $F_{\lambda,n,m}(k')$ is decidable in polynomial time. A similar result holds for $G_{\lambda,m}(k)$.*

We state one final conjecture:

Conjecture 25. *For all $n \to \infty$, there exists λ, k such that*

1. *$P_{\lambda,n,m}(k) \neq \emptyset$ and the affine hull of $P_{\lambda,n,m}(k)$ contains an integer point.*
2. *The affine hull of $Q_{\lambda,m}(k)$ does not contain an integer point.*

In addition, we can run all of this for NP vs P/poly to obtain an analogous result. An approach to prove PH1 is suggested using quantum groups, which were introduced by Drinfeld.

References

[1] Mulmuley, K. D. *On P vs NP and Geometric Complexity Theory.* JACM, vol. 58, 2, April 2011.