

On P vs. NP , Geometric Complexity Theory, Explicit Proofs, and The Complexity Barrier

Ketan D. Mulmuley

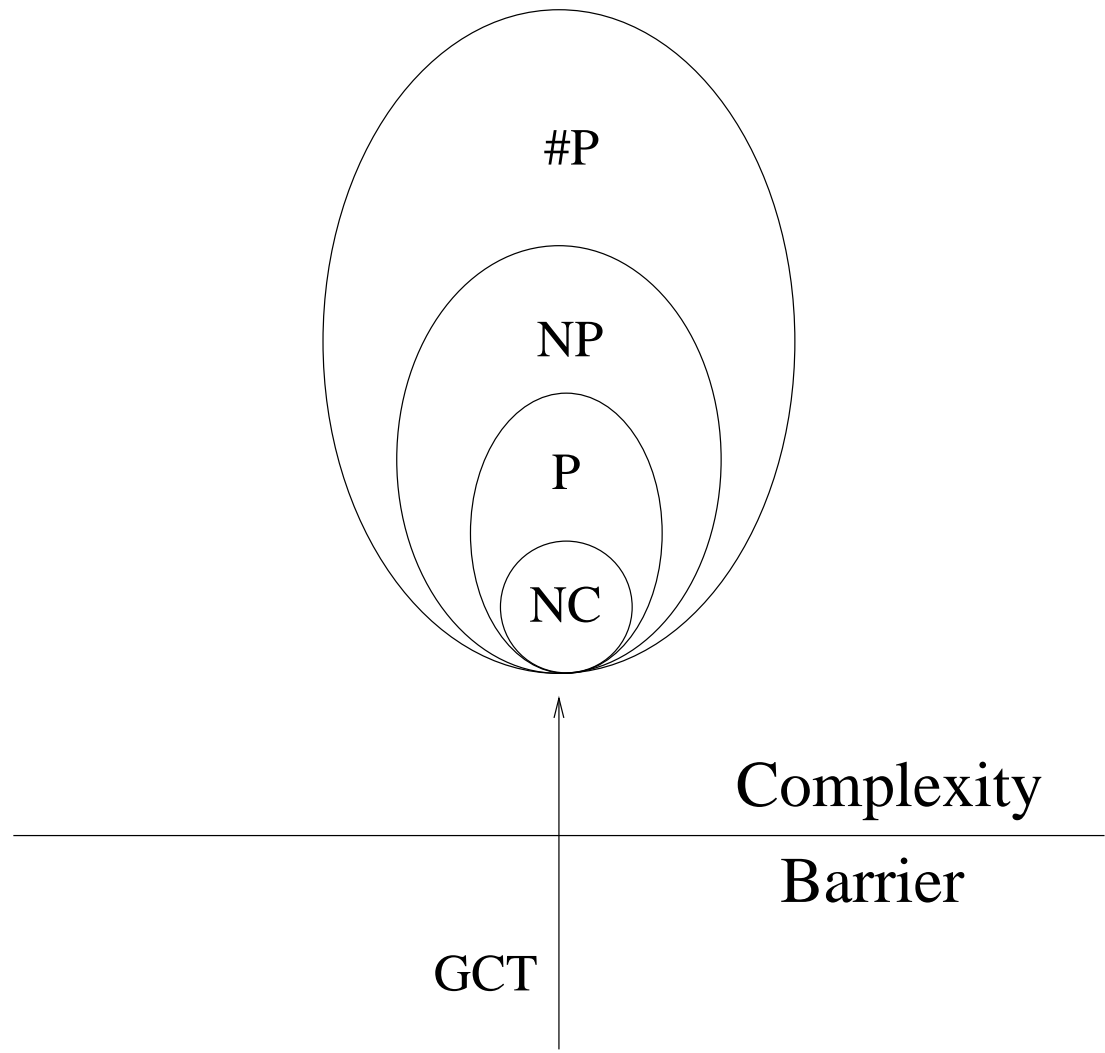
The University of Chicago

References

1. On P vs. NP , Geometric Complexity Theory (GCT), Explicit Proofs and The Complexity Barrier, 2009.
2. GCTlocal: Lower bound in a parallel model without bit operations, SICOMP 99.
3. GCT1-8:
 - (a) GCT1-4: Joint with Milind Sohoni
 - (b) GCT5: Joint with Hari Narayanan

All papers available on the speakers home page.

The root difficulty



A special case of the $P \neq NC$ conjecture

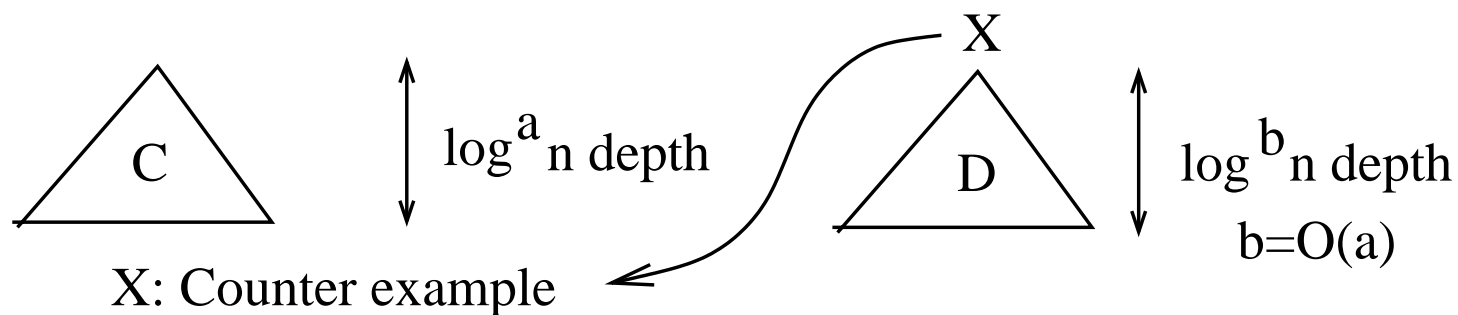
Theorem[GCTlocal] [$P \neq NC$ result without bit operations]

Max flow cannot be computed in $\text{polylog}(N)$ time using $\text{poly}(N)$ processors in the PRAM model without bit operations.

A: Superpolynomial lower bound that is a special case of a fundamental separation problem in a natural and realistic model of computation.

Proof

1. Classical algebraic geometry
2. **Locally explicit**: produces a counterexample for a circuit of polylog depth with a circuit of polylog depth.



In contrast, lower bound proofs for constant depth or monotone circuits or algebraic decision trees are nonconstructive.

Algebraic degree barrier

[GCTlocal]: Low degree techniques will not work.

Algebraic degree barrier

[GCTlocal]: Low degree techniques will not work.

Basic idea for bypassing the algebraic degree barrier

[GCTlocal]: Use geometric invariant theory.

[GCT1,2]: An approach via geometric invariant theory.

Mathematical form of the $\#P \neq NC$ conjecture

Defn: A polynomial $p(X_1, \dots, X_k)$, $\dim(X_i) = n$, is called a hybrid symmetric function if it has the same symmetries as the determinant on the left and the permanent on the right.

Mathematical form of the $\#P \neq NC$ conjecture

Defn: A polynomial $p(X_1, \dots, X_k)$, $\dim(X_i) = n$, is called a hybrid symmetric function if it has the same symmetries as the determinant on the left and the permanent on the right.

Thm [GCT1,2,6]: No hybrid symmetric function can be expressed as a polynomial in the traces of monomials in $\bar{X}_i = BX_iC$, for any possibly singular matrices B and C , if $n > 1$. [characteristic zero]

Mathematical form of the $\#P \neq NC$ conjecture

Defn: A polynomial $p(X_1, \dots, X_k)$, $\dim(X_i) = n$, is called a hybrid symmetric function if it has the same symmetries as the determinant on the left and the permanent on the right.

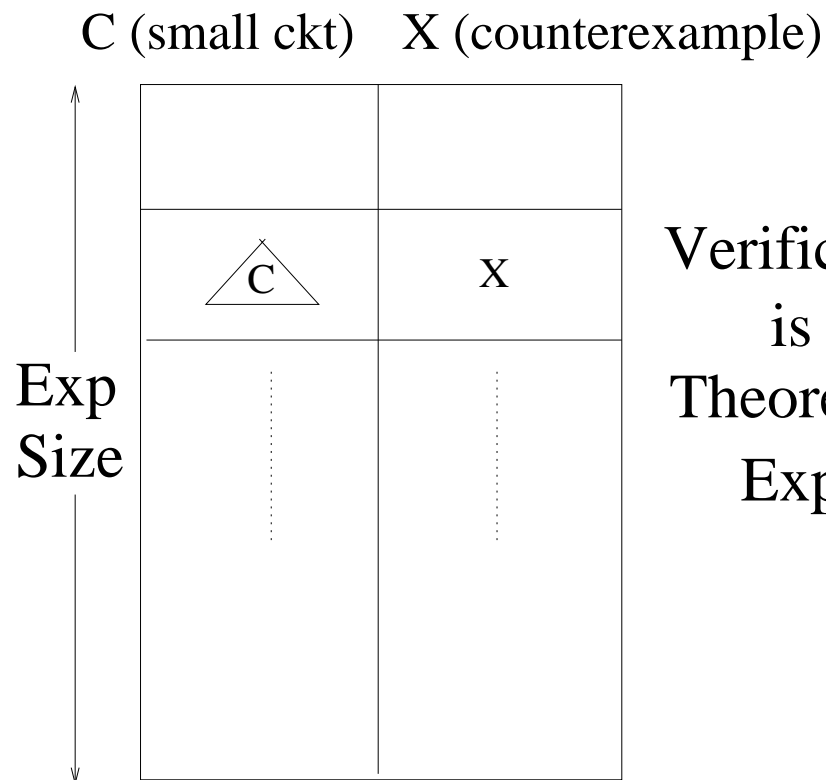
Thm [GCT1,2,6]: No hybrid symmetric function can be expressed as a polynomial in the traces of monomials in $\bar{X}_i = BX_iC$, for any possibly singular matrices B and C , if $n > 1$. [characteristic zero]

Proof: Geometric invariant theory

B: Bypasses the relativization, natural proof and algebraic degree barriers simultaneously.

Nonuniform P vs. NP problem

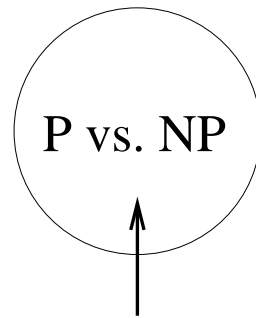
Infeasible Obstruction Hypothesis [IOH]: There exists a trivial obstruction (proof certificate of hardness) for any NP -complete $f(X) = f(x_1, \dots, x_n)$.



Verification and Discovery
is Hard, i.e.,
Theoretically Infeasible:
Exp Time

The complexity barrier

Fundamental Folklore Question: Why should any given proof technique be even **theoretically feasible**?



Complexity barrier [break the circle]: Answer the question **formally**:

1. Formalize the question.
2. Answer the formalized question.

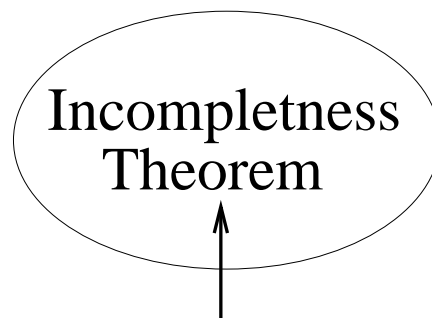
The computability barrier

Incompleteness Theorem [G]: Number theory is undecidable.

Fundamental Folklore Question: What is **decidable**, i.e., **computable**?

Computability barrier: Formalize the question.

Computability Hypothesis [CT]: Formalization of the computability barrier.



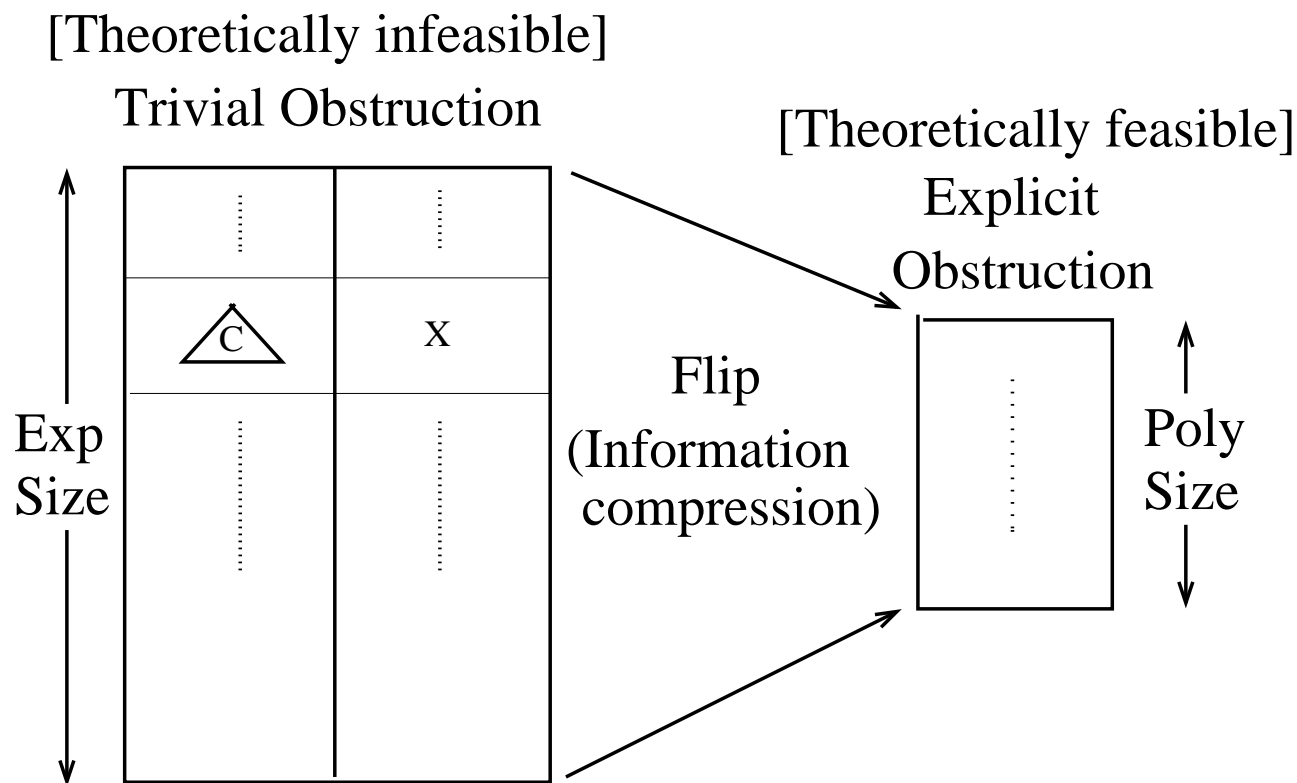
The main result of GCT

Theorem [GCT6]:

C: Formalization of the complexity barrier

1. Gives formal meaning to **theoretically feasibility of GCT**.
2. Formalizes the complexity barrier in the same spirit that the Computability Hypothesis formalizes the computability barrier.

The flip



(Strongly) Explicit means:

1. **Short:** $\text{poly}(n)$ size.
2. **Easy to verify (and discover):** $\text{poly}(n)$ time.

The flip (cont.)

1. Come up with a new obstruction that is **explicit**:
 - a Short: For given n and m if there exists an obstruction, there exists a short obstruction with specification of $\text{poly}(n)$ bit length.
 - b Easy to verify: For given n and $m < 2^n$, whether a given string x is a specification of an obstruction can be verified in $\text{poly}(n, \langle x \rangle)$ time.

The flip (cont.)

1. Come up with a new obstruction that is **explicit**:
 - a Short: For given n and m if there exists an obstruction, there exists a short obstruction with specification of $\text{poly}(n)$ bit length.
 - b Easy to verify: For given n and $m < 2^n$, whether a given string x is a specification of an obstruction can be verified in $\text{poly}(n, \langle x \rangle)$ time.
2. [Optional] **Strongly explicit**: This means easy to discover. That is, for given n and $m < 2^n$ whether there exists an obstruction can be decided in $\text{poly}(n)$ time.

3: Practical feasibility

Using the “easy” (**theoretically feasible**) criterion for verification (and discovery) show that:

OH (Obstruction Hypothesis): For any n and $m = \text{poly}(n)$, there exists a new obstruction.

We will say that the complexity barrier is crossed once steps 1 and 2 are carried out.

We will say that OH and the approach is **theoretically feasible** once the complexity barrier is crossed.

Explicit proofs

A proof is **explicit** if it is based on the flip. **Locally explicit** if it produces a counter example X for each small C in polynomial time.

Circuit lower bounds	Proof techniques
Constant depth, Monotone ckts	Nonconstructive
A: P vs. NC result without bit ops	Locally explicit
B: Mathematical form of the #P vs. NC problem	Strongly explicit

Towards
P vs. NP

The permanent vs. determinant problem

Can $\text{perm}(X)$, $\dim(X) = n$, be linearly represented as $\det(Y)$, $\dim(Y) = m$, if $m = \text{poly}(n)$? [Characteristic zero]

The permanent vs. determinant problem

Can $\text{perm}(X)$, $\dim(X) = n$, be linearly represented as $\det(Y)$, $\dim(Y) = m$, if $m = \text{poly}(n)$? [Characteristic zero]

Observation [GCT1]: The determinant and the permanent are **exceptional**, i.e., **characterized by their symmetries**:

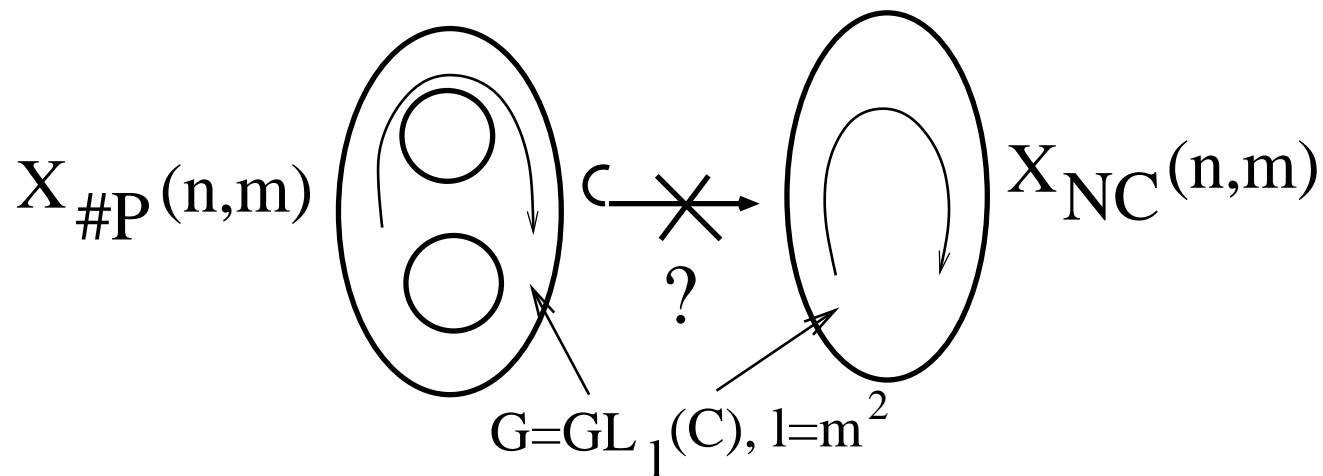
(D): The determinant is the only polynomial in Y of degree m such that for all A, B with $\det(AB) = 1$, $\det(AYB) = \det(Y)$.

(P): The permanent is the only polynomial in X of degree n such that for all permutation and/or diagonal matrices (with determinant one) $\text{perm}(AXB) = \text{perm}(X)$.

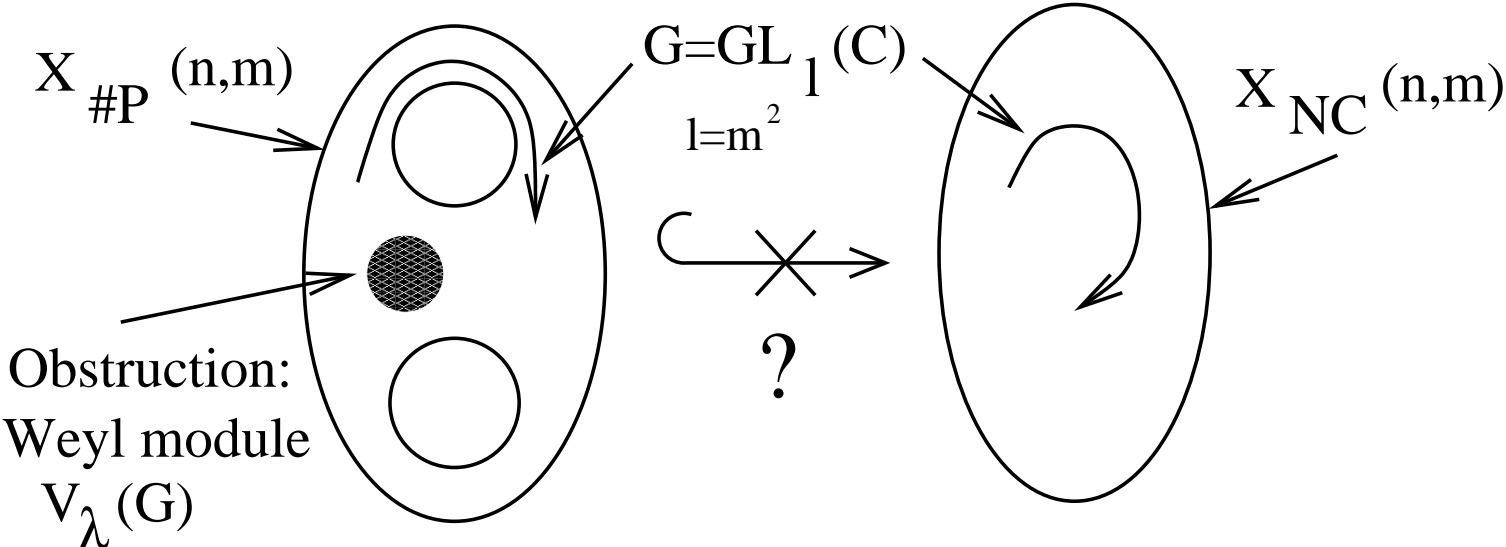
The class varieties

[GCT1,2]: Associates with the complexity classes $\#P$ and NC **exceptional class varieties** $X_{\#P}(n, m)$ and $X_{NC}(n, m)$ such that if $\text{perm}(X)$ can be linearly represented as a determinant of an $m \times m$ matrix then:

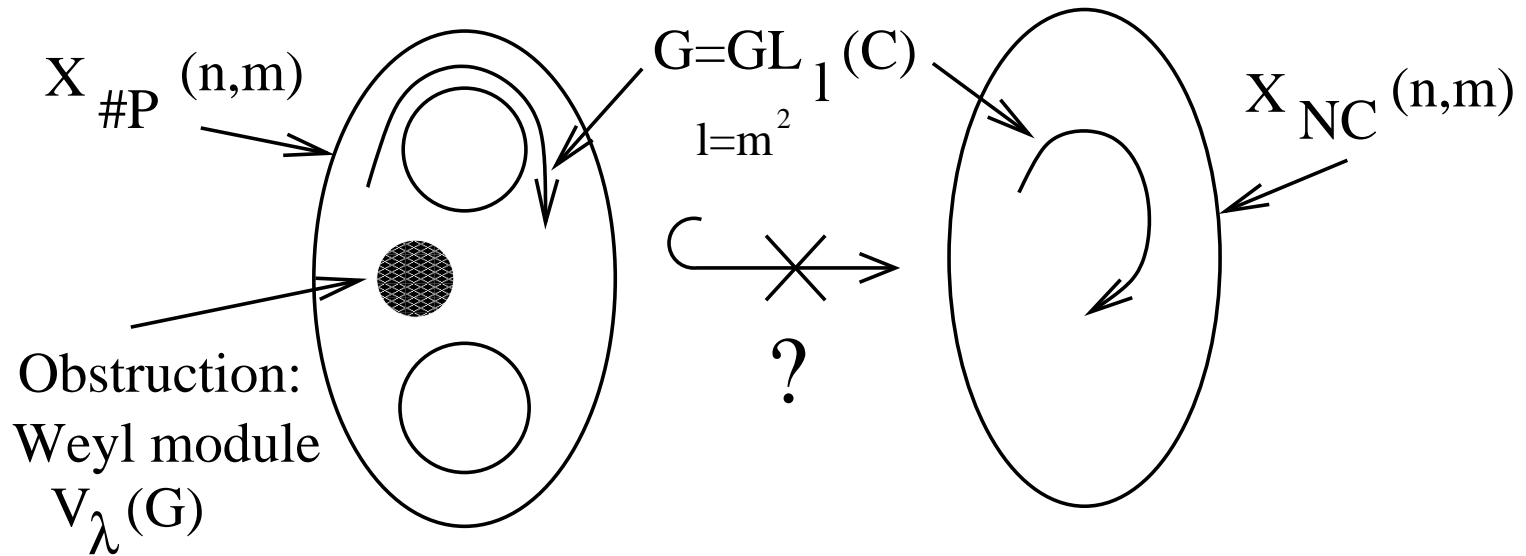
$$X_{\#P}(n, m) \subseteq X_{NC}(n, m).$$



Geometric obstructions

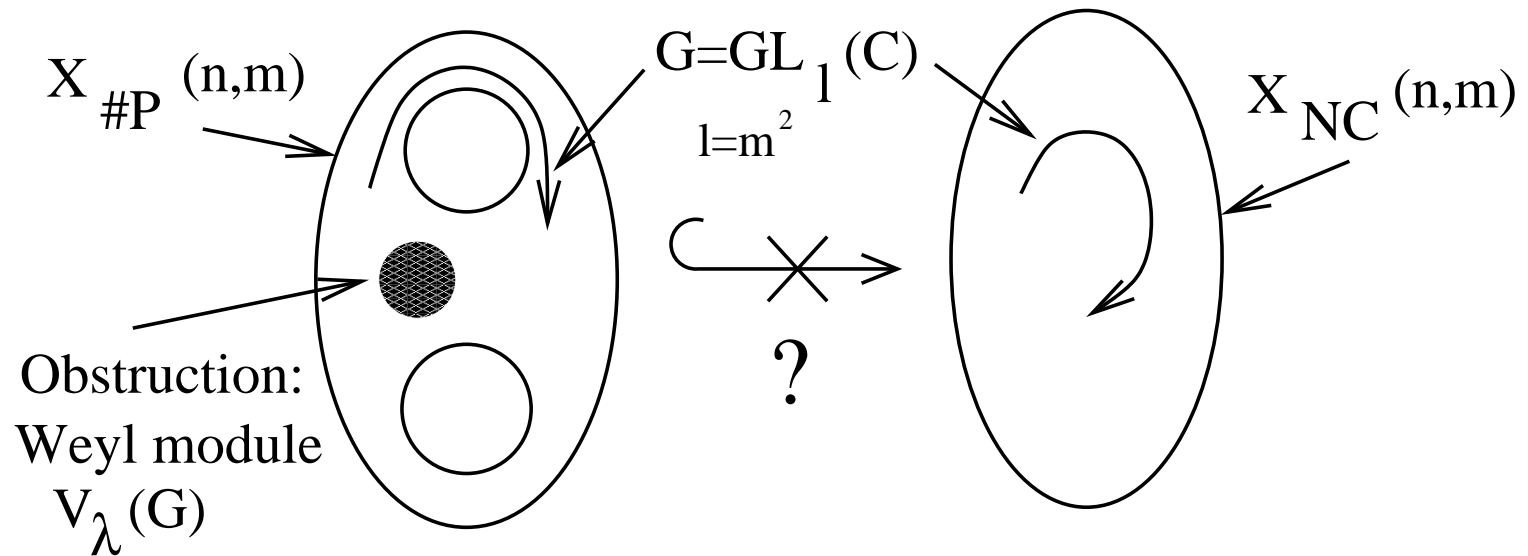


Geometric obstructions



Defn: [GCT1,2] A geometric obstruction for given n and m is an irreducible representation of $G = GL_l(\mathbb{C})$, $l = m^2$, [Weyl module $V_\lambda(G)$] that lives on $X_{\#P}(n, m)$ but not on $X_{NC}(n, m)$.

Geometric obstructions



Defn: [GCT1,2] A geometric obstruction for given n and m is an irreducible representation of $G = GL_l(\mathbb{C})$, $l = m^2$, [Weyl module $V_\lambda(G)$] that lives on $X_{\#P}(n, m)$ but not on $X_{NC}(n, m)$.

Conj: [GCT6] Geometric obstructions are **strongly explicit**, i.e., **short, easy to verify and discover [theoretically feasible]**.

Positivity Hypothesis (PH1)

Let $F_{\lambda,n,m}(k)$ be the number of copies of $V_{k\lambda}(G)$ on $X_{\#P}(n, m)$, and $G_{\lambda,n,m}(k)$ on $X_{NC}(n, m)$.

Positivity Hypothesis (PH1)

Let $F_{\lambda,n,m}(k)$ be the number of copies of $V_{k\lambda}(G)$ on $X_{\#P}(n, m)$, and $G_{\lambda,n,m}(k)$ on $X_{NC}(n, m)$.

PH1: For any n and m there exist an explicit (parametrized) polytope

$$P_{\lambda,n,m}(k) : Ax \leq kb + c,$$

and a similar explicit polytope $Q_{\lambda,n,m}(k)$ such that

$$F_{\lambda,n,m}(k) = \#(P_{\lambda,n,m}(k)) \text{ and } G_{\lambda,n,m}(k) = \#(Q_{\lambda,n,m}(k)).$$

Positivity Hypothesis (PH1)

Let $F_{\lambda,n,m}(k)$ be the number of copies of $V_{k\lambda}(G)$ on $X_{\#P}(n, m)$, and $G_{\lambda,n,m}(k)$ on $X_{NC}(n, m)$.

PH1: For any n and m there exist an explicit (parametrized) polytope

$$P_{\lambda,n,m}(k) : Ax \leq kb + c,$$

and a similar explicit polytope $Q_{\lambda,n,m}(k)$ such that

$$F_{\lambda,n,m}(k) = \#(P_{\lambda,n,m}(k)) \text{ and } G_{\lambda,n,m}(k) = \#(Q_{\lambda,n,m}(k)).$$

Dimensions of the polytopes guaranteed to be polynomial.

C: Formalization of the complexity barrier

Thm: [GCT6] There exists an **explicit family** $\{O_{n,m} = V_{\lambda_{n,m}}(G)\}$ of obstructions assuming

1. PH1, and
2. Obstruction Hypothesis (OH): If $m = \text{poly}(n)$, there exists $\lambda_{n,m}$ such that for every large enough k :

$$[LP] : P_{\lambda,n,m}(k) \neq \emptyset \text{ and } Q_{\lambda,n,m}(k) = \emptyset.$$

Explicit means the bit specification $\langle \lambda \rangle$ is short and easy to verify.

C: Formalization of the complexity barrier

Thm: [GCT6] There exists an **explicit family** $\{O_{n,m} = V_{\lambda_{n,m}}(G)\}$ of obstructions assuming

1. PH1, and
2. Obstruction Hypothesis (OH): If $m = \text{poly}(n)$, there exists $\lambda_{n,m}$ such that for every large enough k :

$$[LP] : P_{\lambda,n,m}(k) \neq \emptyset \text{ and } Q_{\lambda,n,m}(k) = \emptyset.$$

Explicit means the bit specification $\langle \lambda \rangle$ is short and easy to verify.

Proof: 1) Geometric invariant theory, 2) Resolution of singularities, and 3) Cohomology.

Why should positivity hold?

$GCT_{6,7,8} : PH_1 \text{ --- } > PH_0.$

PH0 [GCT8]: Structural parameters of representations of nonstandard quantum groups in GCT4 and 7 are **positive**.

Supported by good experimental evidence.

PH0 is known to hold for standard quantum groups. The only known proof [KL,L] goes through the Riemann Hypothesis over finite fields [G,D].

Summary

GCT meets criteria A, B, and C.

Incompleteness Theorem	P vs. NP
Computability Barrier	Complexity Barrier
Formalization: Computability Hypothesis [CT]	Formalization: GCT6
Proof [G]	Program [GCT6,7,8]

Done: Easy initial step [Formalization]

Remains: Real hard work [Proof]

Final questions

1. Is there an alternative to GCT that meets the criteria A, B, and C?
2. Can a modest lower bound (e.g. superlinear) in the unrestricted model be proved without crossing the complexity barrier? **Unlikely.**
3. Has there been a progress on the P vs. NP problem?

This has to be judged by the two fields, mathematics and complexity theory, **together.**