The GCT program towards the P vs. NP problem

Dedicated to Sri Ramakrishna

Ketan D. Mulmuley
The University of Chicago

(To appear in CACM)

ABSTRACT

This article gives an informal overview of the geometric complexity theory (GCT) program towards the P vs. NP and related problems.

Categories and Subject Descriptors

F.1.3 [**Computation by Abstract Devices**]: Complexity Measures and Classes—*Relations among complexity classes*

General Terms

Theory

Keywords

Geometric complexity theory, P, NP

1. INTRODUCTION

Geometric complexity theory (GCT) is an approach via algebraic geometry and representation theory towards the P vs. NP and related problems [9, 13, 15, 29]. It was proposed in a series of papers [18, 21, 25, 26, 24, 4, 22, 19, 20] and was developed further in [7, 8, 14]. This article gives an informal overview of GCT. It is meant to be an update on the status of the P vs. NP problem as reported in [11]. See [23] for a more detailed and formal overview of GCT.

Let us begin by recalling an algebraic variant of the P vs. NP problem introduced in the seminal paper [29]. It can formulated in a very concrete form as the *permanent vs. determinant* problem. Here the permanent of an $n \times n$ variable matrix X is defined just like the determinant but without signs. Specifically:

$$\begin{array}{lcl} \det(X) & = & \sum_\sigma \mathrm{sign}(\sigma) \prod_{1 \le i \le n} x_{i\sigma(i)}, \quad \text{and,} \\ \mathrm{perm}(X) & = & \sum_\sigma \prod_{1 \le i \le n} x_{i\sigma(i)}, \end{array}$$

where x_{ij}'s denote the entries of X and σ ranges over all permutations of the integers from 1 to n. Let K, the base field or ring of computation, be either $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, or a finite field F_p of p elements, p an odd prime. We say that $\mathrm{perm}(X)$ can be *linearly represented* as the determinant of an $m \times m$ matrix if $\mathrm{perm}(X) = \det(Y)$ for some $m \times m$ matrix Y whose entries are linear combinations (possibly nonhomogeneous) over K of the variable entries of X. The permanent vs. determinant conjecture in [29] is that $\mathrm{perm}(X)$ cannot be linearly represented as the determinant of an $m \times m$ matrix when m is small. This means when m is polynomial in n, or more generally, when it is $O(2^{\log^a n})$ for some constant $a > 0$.

It is known [3, 29] that this conjecture, when K is $\mathbb{Z}$ or F_p, and m is polynomial in n, is implied by a stronger (nonuniform) version[1] of the $P \neq NP$ conjecture or even the weaker $\#P \not\subseteq NC$ conjecture. Here $\#P$ denotes the class of functions, like the number of satisfying assignments of a boolean formula, that count the number of solutions of the problems in NP, and NC denotes the class of functions[2], like the determinant, that can be computed efficiently in parallel in polylogarithmic time using polynomially many processors. The implication of the permanent vs. determinant conjecture from the (nonuniform) $\#P$ vs. NC conjecture is based on the fact that the permanent is $\#P$-complete [29] (in the spirit of the well-known NP-completeness) and that the determinant is (almost) NC-complete. It is also known that the permanent vs. determinant conjecture, when K is a large enough finite field F_p and $m = O(2^{c \log^2 n})$ for some large enough constant $c > 0$, implies the $\#P \not\subseteq NC$ conjecture. As such the permanent vs. determinant conjecture is, strictly speaking, an algebraic analogue of the $\#P$ vs. NC conjecture, not the P vs. NP conjecture. There is also an analogous algebraic analogue of the P vs. NP conjecture (cf. [21, 25]) which, when K is a large enough finite field, implies the usual $P \neq NP$ conjecture. But its story is similar to that of the permanent vs. determinant conjecture. Hence, for simplicity, we only focus on the permanent vs. determinant conjecture here.

By the arithmetic case of this conjecture, we mean the case when $K = \mathbb{Z}, \mathbb{Q}$, or $\mathbb{C}$. This case for $K = \mathbb{Z}$ is implied by the case when $K = F_p$, and also, as already mentioned, by the (nonuniform) $\#P$ vs. NC conjecture. The arithmetic case is easier than the case when $K = F_p$ because it avoids complications in algebra that arise in the case of finite fields.

Hence let us first discuss the arithmetic case when $K = \mathbb{C}$, which implies the cases when $K = \mathbb{Z}$ or $\mathbb{Q}$. The advantage of

[1]This version says that NP contains functions that cannot be computed by polynomial size circuits.

[2]This definition of NC is broader than the usual definition that allows only 0-1 functions.

dealing with the arithmetic conjecture over $\mathbb{C}$, in contrast to the original boolean conjectures, is that this arithmetic conjecture is a statement about multivariate polynomials over $\mathbb{C}$. Hence we can use techniques from algebraic geometry, which is the study of the common zeroes of sets of multivariate polynomials. These techniques work best when the base field is algebraically closed of characteristic zero, such as $\mathbb{C}$. Since the permanent and the determinant are characterized by their symmetries (Section 2), we can also use techniques from representation theory, which is the study of groups of symmetries. As such the GCT approach that goes via algebraic geometry and representation theory is very natural in the arithmetic setting.

The articles [25, 26] reduce the arithmetic permanent vs. determinant conjecture to proving existence of *geometric obstructions* (Section 2) that are proof certificates of hardness of the permanent. The very existence of these obstructions for given n and m implies that the permanent of an $n \times n$ variable matrix cannot be linearly represented as the determinant of an $m \times m$ matrix. The geometric obstructions are objects that live in the world of algebraic geometry and representation theory. Their dimensions can be large, exponential in n and m. But they have short classifying labels. The basic strategy of GCT, called the *flip* [22, 21] (Section 3), is to construct the classifying label of some geometric obstruction *explicitly* in time polynomial in n and m when m is small. It is called the flip because it reduces the lower bound problem under consideration to the upper bound problem of constructing a geometric obstruction label efficiently. The flip basically means proving lower bounds using upper bounds. Its basic idea in a nutshell is: (1) understand the the theory of upper bounds (algorithms) first, and (2) use this theory to prove lower bounds later. But one may wonder why we are going for explicit construction of obstructions, when proving existence of an obstruction even nonconstructively suffices in principle. This is because of the flip theorem in [23, 21] which says that in the problem under consideration we are essentially *forced* to construct some proof certificate of hardness explicitly.

The upper bound problems that arise in the context of the flip turn out to be formidable problems at the frontier of algebraic geometry. The flip theorem mentioned above also says that stronger versions of the permanent vs. determinant conjecture and a standard derandomization conjecture [12] in complexity theory imply together solutions to the upper bound problems in algebraic geometry that are akin to the ones that arise in the flip. Furthermore the article [22] gives evidence that even the upper bound problems that arise in the flip may be essentially implications of these conjectures in complexity theory. This suggests a *law of conservation of difficulty*, namely, that problems comparable in difficulty to the ones encountered in GCT would be encountered in *any* approach to the (nonuniform) P vs. NP problem (of which the arithmetic permanent vs. determinant conjecture over $\mathbb{Z}$ is an implication). This does not say that any approach to the P vs. NP problem has to necessarily go via algebraic geometry. But it does suggest that avoiding algebraic geometry may not be pragmatic since it would essentially amount to reinventing in some guise the wheels of this difficult field that have been developed over centuries.

There is also another reason why the explicit construction of geometric obstruction labels turns out to be hard. At the surface it seems that for such efficient construction one may need to compute the permanent itself efficiently, thereby contradicting the very hardness of the permanent that we are trying to prove. By the flip theorem in [23, 21], this *self referential difficulty* (Section 3.4), akin to that in Gödel's Incompleteness Theorem, is also not specific to GCT. Any approach would have to cope with it. The article [22] shows how it can be tackled in GCT by decomposing the lower bound problem under consideration into subproblems without this difficulty (Section 3.5). Conceptually, this is the main result of GCT in the arithmetic setting.

Finally, let us discuss the permanent vs. determinant conjecture over finite fields that implies the $\#P \not\subseteq NC$ conjecture, the story for the algebraic variant of the P vs. NP problem in [25] that implies the usual (boolean) P vs. NP conjecture being similar. Here the GCT plan is to prove the arithmetic case via algebraic geometry over $\mathbb{C}$ as outlined above first, and then extend this proof to finite fields by proving additional results in algebraic geometry over $\mathbb{C}$, or rather, algebraically closed fields of characteristic zero such as $\mathbb{C}$. At the surface, this plan may seem counterintuitive. After all, how one can hope to prove statements about finite fields using algebraic geometry over $\mathbb{C}$? A basic prototype for this plan is the analogue of the usual Riemann hypothesis for finite fields proved in [10] using algebraic geometry over algebraically closed fields of characteristic zero such as $\mathbb{C}$. The proof of this result, a crowning achievement in mathematics, shows that difficult statements about finite fields can be proved using algebraic geometry over algebraically closed fields of characteristic zero. In the same spirit, the GCT approach in the arithmetic setting can be extended so that it applies to the usual (boolean) $\#P$ vs. NC and P vs. NP conjectures. But this story is beyond the scope of this article. It will be described in a later paper [17]. In this paper we confine ourselves to the arithmetic permanent vs. determinant problem, which captures the crux of the P vs. NP problem.

The rest of this article is organized as follows. In Section 2 we describe the notion of geometric obstructions for the arithmetic permanent vs. determinant problem. In Section 3, we describe the *flip* strategy that goes towards *explicit* construction of geometric obstruction labels in polynomial time. We state the upper bound problems in algebraic geometry that arise in this context. We also describe the self-referential difficulty in the problem under consideration and how GCT tackles it by decomposing the problem into subproblems without this difficulty. In Section 4, we address some frequently asked questions.

The subsections marked with ♠ in this article contain technical material. They may be skipped by the readers not interested in technical details.

2. GEOMETRIC OBSTRUCTIONS

We now describe the GCT approach to the arithmetic permanent vs. determinant problem [29] over $\mathbb{C}$ based on the notion of geometric obstructions (proof certificates of hardness).

The starting point of the approach is the classical result that the permanent and determinant are completely characterized by their symmetries in the following sense [25].

(D): Let Y be a variable $m \times m$ matrix. Then $\det(Y)$ is the unique polynomial (up to a constant multiple) of degree m in the variable entries of Y such that, for any $m \times m$

invertible complex matrices A and B with $\det(A)\det(B) = 1$, $\det(Y) = \det(AY^*B)$, where Y^* is Y or its transpose.
(P): Let X be a variable $n \times n$ matrix. Then $\text{perm}(X)$ is the unique polynomial (up to a constant multiple) of degree n in the variable entries of X such that, for any diagonal or permutation matrices A and B, $\text{perm}(X) = \text{perm}(AX^*B)$, where X^* is X or its transpose, and the product of the entries of A is one, when A is diagonal, and similarly for B.

The goal is to solve the problem under consideration exploiting these properties. Towards this end, [25] constructs algebraic varieties $\Delta[\text{perm}, n, m]$ and $\Delta[\det, m]$ such that if $\text{perm}(X)$, where X is an $n \times n$ variable matrix, can be linearly represented as the determinant of an $m \times m$ matrix, then

$$\Delta[\text{perm}, n, m] \subseteq \Delta[\det, m]. \quad (1)$$

Here by an algebraic variety we mean the set of common solutions of a system of multivariate polynomial equations over $\mathbb{C}$. These are generalizations of the usual curves and surfaces. For example, the set of common solutions in $\mathbb{C}^4$ of two polynomial equations

$(1) : x_1^2/a^2 + x_2^2/b^2 + x_3^2/c^2 + x_4^2/d^2 = 0,\ a, b, c, d > 0,$ and,
$(2) : x_1^2/a'^2 + x_2^2/b'^2 + x_3^2/c'^2 = x_4,\ a', b', c' > 0,$

is a two-dimensional variety Z formed by intersecting the 3-dimensional ellipsoid corresponding to the first equation with the 3-dimensional paraboloid corresponding to the second equation. By the coordinate ring of a variety we mean the space of polynomial functions on it. This is obtained by restricting to the variety the polynomial functions on the ambient vector space containing the variety. For example, the coordinate ring of Z here is the space of polynomial functions on C^4 restricted to Z.

The varieties $\Delta[\det, m]$ and $\Delta[\text{perm}, n, m]$ are formally defined in Section 2.1 below. Intuitively, the points in the variety $\Delta[\det, m]$ correspond to the functions in the arithmetic analogue of NC called VP [29] or the "limits" of such functions, and the points in $\Delta[\text{perm}, n, m]$ correspond to the functions in the arithmetic analogue of $\#P$ called VNP [29] or the "limits" of such functions. Since the permanent vs. determinant conjecture is the arithmetic analogue of the $\#P$ vs. NC conjecture, it thus suffices to show that the inclusion (1) does not hold when m is small.

The goal is to show using algebraic geometry and representation theory that the inclusion (1) is impossible, as conjectured in [25], when m is polynomial in n. We call this *the strong permanent vs. determinant conjecture*. It implies the original conjecture and is almost equivalent to it in the sense that if (1) holds then $\text{perm}(X)$ can be approximated infinitesimally closely by a linear representation of the form $\det(Y')$, with $\dim(Y') = m$. The following is a partial result towards the above stronger conjecture.
Theorem[14] The inclusion (1) is impossible if $m \leq n^2/2$.

This implies the earlier quadratic lower bound [16] for the permanent, but is a bit stronger.

As an aid to prove the strong permanent vs. determinant conjecture in general, [26] defines the notion of a *geometric obstruction* to the inclusion (1). Informally, a geometric obstruction is a representation-theoretic object that lives on $\Delta[\text{perm}, n, m]$ but not on $\Delta[\det, m]$; cf. Figure 1. The very existence of such an obstruction serves as a guarantee that the inclusion as in (1) is not possible, because otherwise the obstruction would be living on $\Delta[\det, m]$ as well.

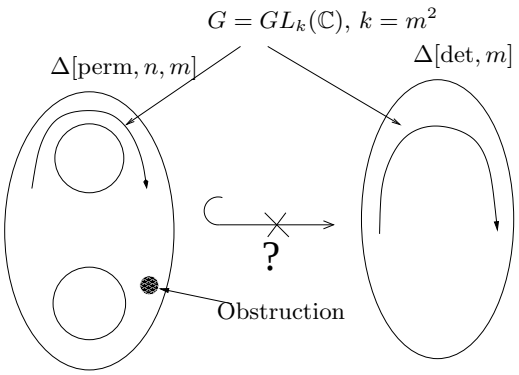

Figure 1: A geometric obstruction

To define geometric obstructions precisely, we need to recall some basic facts from representation theory. Let $G = GL_k(\mathbb{C})$ be the general linear group of $k \times k$ complex invertible matrices. We call a vector space W a representation of G if there is a homomorphism from G to the group of invertible linear transformations of W. For example, $\mathbb{C}^k$ with the usual action of G is its standard representation. There are, of course, far more complex representations of G. Their building blocks were classified by Hermann Weyl [30]. He showed that irreducible (polynomial) representations of G are in one-to-one correspondence with nonnegative integer sequences (called partitions) $\lambda = (\lambda_1, \cdots, \lambda_l)$, where $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_l \geq 0$, and $l \leq k$. An irreducible representation of G in correspondence with λ is denoted by $V_\lambda(G)$. It is called a *Weyl module* of G. For example, the standard representation $\mathbb{C}^k$ of G mentioned above is the Weyl module corresponding to the partition (1) consisting of just one integer 1. The Weyl module $V_\lambda(G)$, when $\lambda = (r)$, is simply the space $\text{Sym}^r(z_1, \ldots, z_k)$ of all homogeneous polynomials of degree r in the variables $z_1, \ldots, z_k$ with the following action of G. Given a polynomial $f(\bar{z}) = f(z_1, \ldots, z_k) \in \text{Sym}^r(z_1, \ldots, z_k)$ and $\sigma \in G$, map $f(\bar{z})$ to

$$f^\sigma(\bar{z}) = f(\bar{z}\sigma). \quad (2)$$

Each finite dimensional representation of G is like a complex building that can be decomposed into the building blocks– the Weyl modules. Fundamental significance of Weyl's classification result from the complexity theoretic perspective is the following. The dimension of each Weyl module $V_\lambda(K)$ is in general exponential in the bitlength of λ. But it has a compact (polynomial size) specification, namely, the labelling partition λ. Existence of such compact specifications of irreducible representations of G plays a crucial role in what follows.

If W is a representation of G, then the elements of G act on W moving its points around via invertible linear transformations. More generally, a group can similarly act on a variety too. As a simple example, consider the ellipsoid $E \subseteq \mathbb{R}^3$ with the equation $x_1^2 + x_2^2 + x_3^3/a = 0$, $a > 0$. Let U be the unit circle. It becomes an additive group if we identify each point in U with its polar coordinate θ and let the usual addition of angles play the role of the group composition. The group U has a natural action on E: let $\theta \in U$ act on E by rotating E around the x_3 axis by the angle θ; cf. Figure 2. Let $\mathbb{R}[E]$ be the coordinate ring of E. This

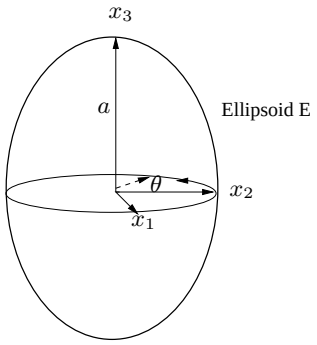

Figure 2: An ellipsoid

is the space of polynomial functions on $\mathbb{R}^3$ restricted to E. Then this action of U on E also makes $\mathbb{R}[E]$ a representation of U: given $\theta \in U$ just map any polynomial function $f(\bar{x}) = f(x_1, x_2, x_3)$ on E to $f(\theta \cdot \bar{x})$, where $\theta \cdot \bar{x} \in E$ denotes the point obtained by rotating $\bar{x} \in E$ around the x_3 axis by the angle θ.

Similarly, the group $G = GL_k\mathbb{C}$, with $k = m^2$, acts on the varieties $\Delta[\det, m]$ and $\Delta[\text{perm}, n, m]$ moving their points around (cf. Figure 1) and this action of G on the varieties makes their coordinate rings (the spaces of polynomial functions on them) representations of G. A formal definition of the action of G and the representation structures of the coordinate rings of $\Delta[\det, m]$ and $\Delta[\text{perm}, n, m]$ is given in Section 2.1 below.

These representation structures turn out [26] to depend critically on the properties (D) and (P) respectively. Specifically, the properties (D) and (P) put strong restrictions on which irreducible representations of G can occur as G-subrepresentations of these coordinate rings.

Formally, a geometric obstruction to the inclusion (1) for given n and m is an irreducible representation $V_\lambda(G)$ of G (a Weyl module) that occurs as a G-subrepresentation in the coordinate ring of $\Delta[\text{perm}, n, m]$ but not in the coordinate ring of $\Delta[\det, m]$ [3]; cf. Figure 1. The partition λ here is called a *geometric obstruction label*. The existence of such an obstruction guarantees that the inclusion as in (1) is impossible because otherwise the obstruction would occur as a G-subrepresentation in the coordinate ring of $\Delta[\det, m]$ as well.

Thus to solve the (strong) permanent vs. determinant conjecture, it suffices to show that:

Geometric obstruction hypothesis (GOH) (cf. [26]): A geometric obstruction exists when m is polynomial in n.

It is conjectured in [22] that GOH, or rather its slightly relaxed form, is *equivalent* to the strong permanent vs. determinant conjecture. We shall discuss why GOH should hold a bit more in Section 3.2.

2.1 ♠:Formal definition of the varieties

For the interested readers, we now formally define the varieties $\Delta[\det, m]$ and $\Delta[\text{perm}, n, m]$ and the action of G on them.

Let Y be an $m \times m$ variable matrix. Let X be an $n \times n$ submatrix of Y, say its lower-right $n \times n$ subminor. Let z be any entry of Y outside X. Let V be the vector space of homogeneous polynomials of degree m in the variable entries of Y. Thus $\det(Y)$ is an element of V. Let $\tilde{\Delta}[\det, m]$ be the set of elements in V of the form $\det(Y')$, where Y' is an $m \times m$ matrix whose entries are complex homogeneous linear combinations of the variable entries of Y. Then $\Delta[\det, m] \subseteq V$ is the closure of $\tilde{\Delta}[\det, m]$ in V in the usual complex topology of V. It can be shown to be an algebraic variety. The variety $\Delta[\text{perm}, n, m] \subseteq V$ is constructed similarly using the homogeneous polynomial $z^{m-n}\text{perm}(X) \in V$ in place of the determinant. It can be shown (cf. [25]) that these varieties have the required property mentioned in (1) [4].

The action of $G = GL_k(\mathbb{C})$, $k = m^2$, on these varieties is defined as follows. First, observe that the space V is a representation of G by a natural action which, for any matrix $\sigma \in G$, maps any point (homogeneous polynomial) $p(Y) \in V$ to the point $p(\sigma^{-1}Y)$. Here we think of Y as an m^2-vector by straightening it, say, rowwise. It can be shown that $\Delta[\det, m]$ and $\Delta[\text{perm}, n, m]$ are invariant under this action of G on V. This induces a natural action of G on these varieties as well. Under this action, each matrix in G acts on a variety by moving its points around and thereby inducing an automorphism. With this action, the coordinate ring of $\Delta[\det, m]$, by which we mean the space of polynomial functions on V restricted to $\Delta[\det, m]$, becomes a representation of G: just map a polynomial function $f(v)$ to $f(\sigma^{-1} \cdot v)$ for any $\sigma \in G$ and $v \in \Delta[\det, m]$. Here $\sigma^{-1} \cdot v$ denotes the point in $\Delta[\det, m]$ obtained by letting $\sigma^{-1} \in G$ act on v. The coordinate ring of $\Delta[\text{perm}, n, m]$ is similarly a representation of G.

3. THE FLIP

With the help of GOH, we have reduced the nonexistence problem under consideration to an existence problem. For general varieties, such an existence problem is hopeless. But we can hope to prove existence of a geometric obstruction using the characterization by symmetries provided by the properties (P) and (D). We turn to this story in this section.

The strategy is to construct, for any n and m polynomial in n, a geometric obstruction label λ *explicitly* in time polynomial in n and m exploiting the properties (P) and (D). We call this strategy the *flip* because it reduces the nonexistence problem under consideration to the problem of proving existence of a geometric obstruction, and furthermore, the lower bound problem is reduced to the upper bound problem of constructing a geometric obstruction label in polynomial time.

The following is a stronger and precise explicit form of GOH which says that geometric obstructions can indeed be constructed *explicitly*.

Flip Hypothesis (FH) (cf. [22, 23]) The geometric obstruction family is *explicit* in the sense that it satisfies the following properties:

FH[Short]: A short geometric obstruction label λ, with bit length polynomial in n and m, exists if m is polynomial in n.

FH[Verification]: Given n, m, and a partition λ, whether λ is a valid geometric obstruction label can be verified in time polynomial in n, m and the bit length of λ.

FH[Discovery and construction]: Given n and m, whether a

[3]Strictly speaking, we have to use the duals of the coordinate rings here.

[4]Actually the varieties here are the affine cones of the projective varieties defined in [25].

geometric obstruction exists can be decided in time polynomial in n and m. If an obstruction exists, one such geometric obstruction label λ can also be constructed in the same time. By FH[Short], this discovery algorithm always succeeds if m is polynomial in n.
FH[Det]: For given m and λ, whether $V_\lambda(G)$ occurs as a G-subrepresentation in the coordinate ring [5] of $\Delta[\det, m]$ can be verified in time polynomial in m and the bit length of λ.
FH[Perm]: For given n, m and λ, whether $V_\lambda(G)$ occurs as a G-subrepresentation in the coordinate ring of $\Delta[\mathrm{perm}, n, m]$ can be verified in time polynomial in n, m and the bit length of λ.

The flip strategy can now be elaborated further into three steps: (1) Prove FH[Det] and FH[Perm]. This clearly implies an efficient criterion for verifying a geometric obstruction label as in FH[Verification]. (2) Use this criterion to design an efficient algorithm for discovering an obstruction as in FH[Discovery]. (3) Prove that this discovery algorithms always succeeds if m is polynomial in n. For this strategy to succeed, it is not enough if the verification and discovery algorithms are only efficient in theory. They should also have simple enough mathematical structure to carry out the step (3). Otherwise, they have to be made simpler and simpler until (3) succeeds.

We shall discuss why FH should hold later in Section 3.2. There is a huge gap between FH and what can be proved at present. Currently the best algorithms for verification and construction of a geometric obstruction label based on general purpose algorithms in algebraic geometry and representation theory take at least double exponential time in n and m. FH says that this time bound can be brought down to a polynomial. This may seem impossible.

3.1 Why go for explicit proofs?

If so, one may ask why we should go for explicit construction of obstructions when proving existence of obstructions even nonconstructively suffices in principle. The reason is provided by the strong flip theorem in [21, 23] described in Section 3.3 below. It says that any proof of the arithmetic (strong) permanent vs. determinant conjecture can be converted into an explicit proof assuming a stronger form of a standard derandomization hypothesis [12] in complexity theory (described below) that is generally regarded as easier than the target lower bound. By an explicit proof, we mean that the proof also yields an algorithm for efficient construction of some proof certificate of hardness of the permanent, called an *obstruction*, that is analogous to the geometric obstruction above in the following sense: (1) its very existence for given n and m guarantees that the inclusion (1) is impossible, and (2) the family of obstructions satisfies analogues of FH[short], FH[verify], and FH[construction]; cf. Section 3.3 for a formal definition. Thus, by the strong flip theorem, the strong permanent vs. determinant conjecture essentially *forces* an explicit proof, modulo derandomization.

There are similar flip theorems (cf.[21]) for other lower bound problems, such as the usual permanent vs. determinant and the arithmetic P vs. NP problems, and a certain average case stronger form of the boolean P vs. NP problem. These results are the main reason why we are going towards explicit proofs, i.e. towards explicit construction of obstructions, right from the beginning.

[5]Actually its dual; and similarly in FH[Perm].

The derandomization hypothesis mentioned above is the following. It importance is based on the fundamental result in [12] that derandomization means proving circuit lower bounds. Let $Y(X)$ be an $m \times m$ matrix, whose each entry is a complex linear combination (possibly nonhomogeneous) of the variable entries of X. The problem is to decide if $\det(Y(X))$, for given $Y(X)$, is an identically zero polynomial in the variable entries of X. There is a simple and efficient randomized algorithm for this test. Let A be a matrix obtained from X by substituting for each entry of X a large enough random integer of bit length polynomial in n and m. Evaluate $\det(Y(A))$ modulo a large enough random integer b. If it is nonzero then $\det(Y(X))$ is certainly a nonzero polynomial. If it is zero, then $\det(Y(X))$ is an identically zero polynomial with a high probability. This randomized test is a black-box test in the sense that it only needs to know the value of $\det(Y(X))$ for a given specialization of X to A. It does not need to know $Y(X)$. The derandomization hypothesis mentioned above is essentially that this randomized black-box determinant identity test can be efficiently derandomized so as to get an efficient deterministic black box determinant identity testing algorithm. (The required hypothesis is actually a bit stronger; cf. [21].) This derandomization hypothesis, which is somewhat different from the one in [12], is essentially equivalent to proving a determinantal lower bound for a multilinear function that can be evaluated in exponential time; cf. [1]. This is generally regarded as easier than proving a determinantal lower bound for the permanent since $\#P$ is conjecturally smaller than EXP, the class of functions that can be computed in exponential time.

3.2 Why should GOH and FH hold?

The strong flip theorem [21, 23] described in Section 3.3 below actually shows something much more. It shows that stronger forms of the permanent vs. determinant and derandomization conjectures together imply an analogue of FH in algebraic geometry of comparable difficulty. This reveals that formidable upper bound problems in algebraic geometry are hidden underneath the fundamental hardness and derandomization conjectures in complexity theory. This may explain why these conjectures, which look so elementary at the surface, have turned out to be so formidable. In view of the strong flip theorem, problems of comparable difficulty can be expected in *any* approach, even if the approach does not go via algebraic geometry. We refer to this as the *"law of conservation of difficulty"*.

The article [22] gives an evidence based on the strong flip theorem and additional results in algebraic geometry which suggests that FH itself may be in essence an *implication* of the strong permanent vs. determinant and derandomization conjectures together. At present this is the main evidence for FH, and hence, GOH. Further evidence is provided by a recent article [7] which constructs explicit geometric obstructions in the analogous setting for the lower bound problem for matrix multiplication, albeit for a problem of very modest size. Explicit computation for any larger example is difficult at present due to the difficulty of the problems that arise.

The strong flip theorem for the permanent vs. determinant conjecture and analogous results in [21] for other fundamental hardness conjectures in complexity theory, such as the arithmetic P vs. NP conjectures, show a fundamental difference between such hardness conjectures that

are at least as hard as the derandomization conjectures and the known lower bound results in the restricted models of computation such as constant depth [5] or monotone [27] circuits. The lower bounds in these restricted models are statements about the *weakness* of these models. In contrast, by the strong flip theorem, the permanent vs. determinant problem is a statement about the *strength* of the complexity class NC (or rather its arithmetic analogue [29] VP) for which the determinant is essentially complete. It does not say that NC (or rather VP) is small and weak, but rather that it is big and strong–strong enough to assert that "I am different from $\#P$" (or rather its arithmetic analogue VNP [29]), for the permanent is complete. Similarly, by an analogous flip theorem for the (arithmetic) P vs. NP problem, this problem is a statement about the strength of the complexity class P. It does not say that P is weak and small but rather that it is big and strong–strong enough to assert that "I am different from NP".

It should also be remarked that FH will almost never hold for functions not characterized by their symmetries (in place of the determinant and the permanent), since, as we shall in Section 3.3 below, the characterization by symmetries plays a crucial role in the proof of the strong flip theorem that forms the crux of the justification of FH. This is why the characterization by symmetries is so crucial for the flip strategy. It is indeed a fortunate coincidence that the fundamental complexity classes such as $\#P$ and NC have complete functions characterized by their symmetries.

3.3 ♠: The strong flip theorem

To the state the strong flip theorem, we need a few definitions. Let $\Delta[\det, m]$, $\Delta[\mathrm{perm}, n, m]$, and V be as in Section 2.1.

By a *global obstruction set* for given n and small m polynomial in n, we mean a set $S_{n,m} = \{X_1, \ldots, X_l\}$ of nonnegative integral $n \times n$ matrices with the following property. Fix any point (homogeneous polynomial) $p(Y) \in \Delta[\det, m] \subseteq V$. Let $p'(X)$ denote the polynomial obtained from $p(Y)$ by substituting zero for all variables in Y other than z and X, and 1 for z. Then, for any such $p(Y) \in \Delta[\det, m]$, there exists a counterexample $X_i \in S_{n,m}$ such that $p'(X_i) \neq \mathrm{perm}(X_i)$. Thus $S_{n,m}$ contains a counterexample against every point in $\Delta[\det, m]$ that shows that the point does not specialize to $\mathrm{perm}(X)$. This guarantees that the inclusion as in (1) is not possible for given n and m. We say that $S_{n,m}$ is small if l is polynomial in n.

We call a proof of the strong permanent vs. determinant conjecture *extremely explicit* if, for each n and small m polynomial in n, it shows existence of a set of bit strings called *obstructions*, which serve as proof certificates of hardness of $\mathrm{perm}(X)$, with the following properties E0-E3.

E0 [Short]: For every n and small m polynomial in n, there exists a short obstruction of bitlength polynomial in n.

E1 [Easy to decode:] Given any such short obstruction s for given n and small m polynomial in n, one can construct in time polynomial in n a small *global obstruction set* $S_{n,m}(s)$. Thus each short obstruction s denotes a small global obstruction set.

E2 [Easy to verify]: Given a bit string s and n and m, whether s is the specification of an obstruction for n and m can be decided in time polynomial in n and m, and the bitlength of s.

E3 [Easy to construct]: For each n and small m polynomial in n, a valid obstruction can be constructed in time polynomial in n.

There are some additional technical properties that an extremely explicit proof has to satisfy; cf. [23, 21] for its details. The properties E0, E2 and E3 are analogues of the properties FH[Short], FH[Verification], and FH[Construction] of geometric obstruction labels (which we identify with geometric obstructions). The geometric obstruction labels also conjecturally satisfy the analogue of E1 for decoding (though this was not stated in the statement of FH above).

We call a proof *extremely explicit in a stronger NC-sense*, if the various algorithms in the conditions E1-E3 work in polylogarithmic time using polynomial number of processors instead of sequential polynomial time.

We say that a technique for proving the strong permanent vs. determinant conjecture is a *flip* if it leads to an extremely explicit proof of the conjecture. It is called a flip because it reduces the nonexistence problem to the problem of proving existence of obstructions and the lower bound problem to the upper bound problem of finding efficient algorithms to verify, construct and decode obstructions.

For similar definitions of explicit proofs for other lower bound problems, such as the usual permanent vs. determinant and P vs. NP problems, see [23, 21].

The strong flip theorem [23, 21]

Suppose the strong permanent vs. determinant conjecture holds, and that black box determinant identity testing [12] described in Section 3.1 can be derandomized (in a stronger form as specified in [21]). Then the strong permanent vs. determinant conjecture has an extremely explicit proof in the stronger NC-sense. In particular, for any m polynomial in n, an explicit global obstruction set $S_{n,m}$ can be constructed in time polynomial in n, and more strongly, in polylogarithmic time (in n) using polynomial number of processors.

The proof of the strong flip theorem depends critically on the characterization by symmetries of the permanent as per the property (P). Alternatively, one can also use downward self-reducibility of the permanent that has several other applications in complexity theory [3].

Currently the best algorithms for the construction of a global obstruction set $S_{n,m}$ based on general purpose algorithms in algebraic geometry take at least double exponential time in n and m and the bit length of the constructed obstruction set is also double exponential in general. Bringing this time down to polynomial may seem impossible at the surface. This situation is very similar to that for FH (cf. the remarks after the statement of FH). Thus the difficulty of proving E0, E0, E2 and E3 for global obstruction sets is comparable to the difficulty of proving FH for geometric obstructions. The strong flip theorem says that the time bound can indeed be brought down to polynomial for geometric obstruction sets assuming the strong permanent vs. determinant conjecture and the derandomization hypothesis.

3.4 ♠: Self-referential difficulty

The strong flip theorem above also reveals the self-referential difficulty in the permanent vs. determinant conjecture.

To see this, let us examine closely the properties E1-E3 of an explicit proof (cf. Section 3.3) that any proof of this conjecture can be converted into, modulo derandomization, by the strong flip theorem. Let $S_{n,m}(s)$ be a global obstruction set denoted by an obstruction string s. To verify if $S_{n,m}(s)$

indeed contains a counterexample against a given point (homogeneous polynomial) $p(Y) \in \Delta[\det, m]$, we have to check if $p'(X) \neq \text{perm}(X))$ for some $X \in S_{n,m}(s)$. Assuming that the permanent is hard to compute, we cannot check efficiently if $p'(X) \neq \text{perm}(X))$ for general X. Yet, by E2 (in the stronger NC-sense), whether $S_{n,m}(s)$ contains a counterexample against *every* $p(Y) \in \Delta_V[g, m]$ can be checked efficiently (even in parallel). This seems to contradict the very hardness of the permanent that we are trying to prove.

This self-referential paradox is only an *apparent* paradox because assuming the permanent vs. determinant conjecture and an additional derandomization hypothesis we can construct an extremely explicit proof by the strong flip theorem. But this is a circular argument. The main difficulty is to make headway in the construction of an explicit proof *without making an assumption in any guise* that is as hard as or harder than the target lower bound assumption.

Analogous flip theorems in [21] reveal similar self-referential difficulty in other variants of the P vs. NP problem harder than derandomization, such as the arithmetic P vs. NP problem [25]. Intuitively, the apparent self-referential paradox arises because the P vs. NP conjecture, being a universal statement about mathematics which says that discovery is hard, can *potentially* make the discovery of its own proof hard.

The situation here is akin to (but far harder than) the situation for another universal statement about mathematics, Gödel's Incompleteness Theorem. This result says that there are true statements which cannot be proved. This does not say that this universal statement itself cannot be proved. As we know now, it can be proved. But the crux of this proof is the resolution of this *apparent* self-referential paradox by the construction of a statement that says "I cannot be proved". Similarly, the root difficulty in the P vs. NP (and the permanent vs. determinant) problem is the resolution of the *apparent self-referential paradox* in the construction of the statement that says "I am different from NP ($\#P$)".

In view of this self-referential paradox, the main conceptual difficulty in proving the permanent vs. determinant conjecture is to *break the circle* of self-reference by decomposing the conjecture into subproblems without the self-referential difficulty.

3.5 ♠: The decomposition

We now describe how this is achieved in GCT.

Towards this end, observe that FH[Det] does not have the self-referential difficulty in the sense that (1) m is not required to be a small function of n in its statement, and (2) it only depends on the properties of the determinant, and not on the relationship between the permanent and the determinant (or equivalently, between the complexity classes $\#P$ and NC). The case of FH[Perm] is similar.

FH[Det] and FH[Perm] together imply FH[verification], which says that geometric obstructions in GOH are easy to verify. We saw in Section 3.4 that the self-referential difficulty is the main obstacle to efficient verification of obstructions as needed in E2. Hence, once FH[Det] and FH[Perm] are proved, GOH does not have the self-referential difficulty in verification any more. This decomposes the strong permanent vs. determinant conjecture into three subproblems without the self-referential difficulty in verification, namely, FH[Det], FH[Perm], and GOH. Pictorially:

$$\begin{array}{c}\text{Strong perm. vs. det.} \stackrel{\cdots>}{\longleftarrow} \\ FH[Det] + FH[Perm] + GOH.\end{array} \quad (3)$$

Here the solid arrow $\longleftarrow$ denotes the formal implication–this follows trivially since GOH itself implies the strong permanent vs. determinant conjecture. The dotted arrow $\cdots>$ indicates the evidence given in [22] for the plausible converse based on the strong flip theorem (cf. Section 3.3). This decomposition breaks the circle of self-reference for verification. Intuitively, the circle is broken here because the task of verifying a geometric obstruction naturally breaks into two independent tasks, one depending only on the permanent (i.e. the complexity class $\#P$) and the other only on the determinant (i.e. the complexity class NC). This is the fundamental difference between geometric obstructions and the global obstruction sets in the strong flip theorem.

The article [22] also describes an approach to prove FH assuming certain *positivity hypotheses* in algebraic geometry and representation theory. The first positivity hypothesis called PH1 basically says that, for given n, m and λ, the number of copies of the Weyl module $V_\lambda(G)$ that occur in the coordinate ring [6] of $\Delta[\det, m]$ (and similarly $\Delta[\text{perm}, n, m]$) has a positive ($\#P$) formula without alternating signs, akin to the usual positive formula for the permanent. We do not discuss other positivity hypotheses here. These hypotheses are again supported by the strong flip theorem, which suggests (cf. [22]) that these hypotheses too (like FH) may be in essence *implications* of the strong permanent vs. determinant and derandomization conjectures together. Furthermore, the self-referential difficulty is absent in these positivity hypotheses for the same reason that it is absent in FH[Det] and FH[Perm]. The decomposition theorem in [22, 23] decomposes the strong permanent vs. determinant conjecture in terms of these positivity hypotheses and a more refined form of GOH (called OH), which too is without the self-referential difficulty once the positivity hypotheses are proved. Unlike (3), this decomposition yields an approach to prove FH[Discovery] also in addition FH[Verification]. See [22, 23] for its details.

The positivity hypotheses above turn out to be formidable because as explained in [22] they encompass and go much further than the century-old plethysm problem in algebraic geometry and representation theory. Since in view of the strong flip theorem these may be essentially implications of the strong hardness and derandomization conjectures, problems of comparable difficulty can be expected in *any* approach. In this sense positivity (like explicit construction) is a hidden root difficulty underneath the fundamental hardness conjectures of complexity theory. This provides yet another reason (in addition to the strong flip theorem) for why these conjectures have turned out to be so hard though they look so elementary at the surface.

The articles [4, 22, 19, 20] suggest an approach to the positivity hypotheses via nonstandard quantum groups. But this story is beyond the scope of this article.

See [22] for the GCT approach to derandomization of determinant and polynomial identity testing [12] and the arithmetic P vs. NP problem.

4. FREQUENTLY ASKED QUESTIONS

[6] Strictly speaking, its dual.

Now we address frequently asked questions regarding GCT.

4.1 Can GCT be used to prove some modest lower bounds first?

Given the difficulty of the fundamental hardness conjectures, one may ask if GCT can be used to prove some modest lower bounds first. That is indeed so. Currently the best known lower bounds in the context of the P vs. NC and strong permanent vs. determinant problems are both based on GCT. The first lower bound is a special case of the $P \neq NC$ conjecture proved in [18]. It says that the P-complete max-flow problem cannot be solved in polylogarithmic time using polynomially many processors in the PRAM model without bit operations. This model is quite realistic and natural in contrast to the the constant depth [5] or monotone [27] circuit models used for proving lower bounds earlier. This lower bound is currently the only known superpolynomial lower bound that is a nontrivial implication of a fundamental separation conjecture like the $P \neq NC$ conjecture and holds unconditionally in a natural and realistic model of computation. Its proof is geometric and quasi-explicit. No combinatorial or elementary proof is known so far. This result was the beginning of the GCT approach to the fundamental hardness conjectures. The second lower bound based on GCT constructions, specifically the varieties $\Delta[\det, m]$ and $\Delta[\mathrm{perm}, n, m]$, is the quadratic lower bound [14] stated in Section 2 in the context of the strong permanent vs. determinant conjecture. It is a stronger form of the earlier quadratic lower bound [16] for the usual permanent vs. determinant problem. The proof in [16] is elementary and does not need GCT. The difference between the strong and usual versions of the permanent vs. determinant problem in [14] and [16] is akin to the difference between the tensor rank and usual versions of the lower bound problem for matrix multiplication [6].

See also the lower bounds for matrix multiplication based on the fundamental work [28] that introduced invariant theory in complexity theory.

4.2 Are explicit proofs necessary?

By the strong flip theorem (cf. Sections 3.1 and 3.3), we know that any proof of the strong permanent vs. determinant conjecture leads to an explicit proof modulo derandomization. This does not say that explicit proofs are necessary. There may be nonexplicit proofs that avoid derandomization all together. But this does suggest that, if derandomization is indeed easier than the fundamental hardness conjectures (cf. [12]) as the complexity theory suggests, then even such nonexplicit proofs would essentially have the necessary mathematical ingradients to construct proof-certificates of hardness efficiently a posteriori. If so, it makes sense to go towards this efficient construction right from the beginning. This allows us to use the theory of algorithms–the main tool of complexity theory–in the study of the fundamental lower bounds. Indeed, it is unrealistic to expect that we can prove $P \neq NP$ without understanding the complexity class P and the theory of algorithms in depth first, as the flip strategy suggests.

The situation here may be compared to that for the well known four colour theorem [2]. In principle, this theorem may be proved nonconstructively. Yet the fact remains that all known proofs of this theorem are explicit in the sense that they also yield efficient algorithms for finding a four colouring as a byproduct. The flip theorem suggests that the story of the fundamental hardness conjectures in complexity theory may be similar.

In this sense these conjectures are fundamentally different from other conjectures in mathematics such as the Riemann Hypothesis. Since there is no analogous flip theorem for the Riemann Hypothesis, it may have a nonconstructive proof that gives no hint on how to test efficiently if the n-th zero of the Riemann zeta function lies on the critical line.

4.3 Is algebraic geometry necessary?

By [29], the arithmetic permanent vs. determinant conjecture over $\mathbb{Z}$ is implied by the $\#P$ vs. NC conjecture. By the strong flip theorem [21, 23] (cf. Section 3.3), stronger forms of the fundamental hardness and derandomization hypotheses in the arithmetic setting imply an analogue of FH in algebraic geometry of comparable difficulty. We have already argued on the basis of these results in Section 1 why it is not pragmatic to avoid algebraic geometry, even though is not formally necessary.

Another concrete evidence for the power of algebraic geometry even in the boolean setting is provided by the proof of the special case of the $P \neq NC$ conjecture [18] (cf. Section 4.1). It has to be emphasized here that, unlike the earlier lower bounds in the algebraic model [6], this lower bound is boolean, not algebraic. This is because it is in terms of the bit length of the input, though the PRAM model in [18] does not allow bit operations. At present, to our knowledge, this is the only nontrivial implication of a fundamental hardness conjecture that can be proved unconditionally in a natural and realistic model of computation. If we cannot prove even this easier implication of the $P \neq NC$ conjecture by elementary techniques, it seems unrealistic to expect that we can prove the far harder $P \neq NC$ (or NP) conjecture by elementary techniques.

4.4 When can we expect a hard lower bound?

The modest lower bounds based on GCT (Section 4.1) and the earlier modest lower bounds [3, 6] are separated from the fundamental hardness conjectures that are at least as hard as derandomization by the circle of self-referential difficulty (Section 3.4); cf. Figure 3. To break into this circle, we have to show (cf. Sections 3.2 and 3.3) that P contains formidable explicit construction problems in algebraic geometry and representation theory, such as the ones that arise in the strong flip theorem or FH. By the law of conservation of difficulty (cf. Section 3.2) based on the strong flip theorem, comparable understanding of P is needed in *any* approach. Unfortunately, our current understanding of P is very modest. Until we understand P (the theory of algorithms) and geometry in the required depth, we may not expect any further lower bounds that are fundamentally different from the modest lower bounds in Section 4.1.

5. CONCLUSION

GCT has broken the circle of self-reference around the fundamental hardness conjectures in the arithmetic setting and in the process has revealed deep explicit construction and positivity problems at the crossroads of algebraic geometry, representation theory, and complexity theory hidden underneath the fundamental hardness conjectures in complexity theory. Given the formidable nature of these problems, this is undoubtedly only the beginning.

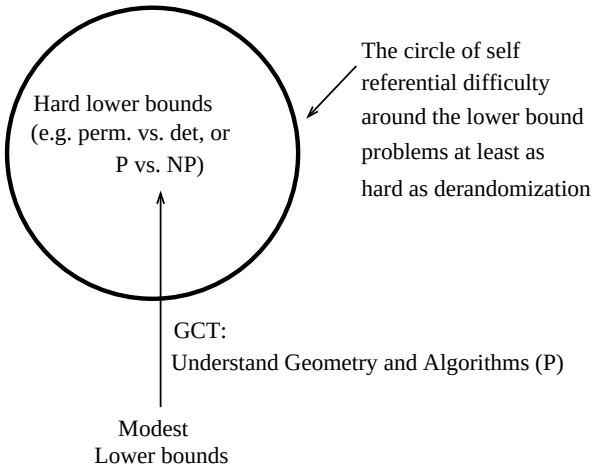

Figure 3: Division in the world of lower bounds by the circle of self-reference

6. ACKNOWLEDGMENTS

The author is grateful to Josh Grochow, Jimmy Qiao, Janos Simon and the referees for helpful comments. The work on this paper was supported by NSF grant CCF-1017760.

7. REFERENCES

[1] M. Agrawal. Proving lower bounds via pseudo-random generators. In *Proceedings of the FSTTCS*, pages 92–105, Berlin, Germany, 2005. Springer-Verlag.

[2] K. Appel, W. Haken, and J. Koch. Every planar map is four colourable. *Illinois Journal of Mathematics*, 21:439–567, 1977.

[3] S. Arora and B. Barak. *Computation complexity: a modern approach*. Cambridge University Press, Cambridge, England, 2009.

[4] J. Blasiak, K. Mulmuley, and M. Sohoni. Geometric complexity theory IV: nonstandard quantum group for the Kronecker problem. *cs. ArXiv preprint cs. CC/0703110*, 2011.

[5] R. Boppana and M. Sipser. The complexity of finite functions. *Handbook of Theoretical Computer Science, Volume A*, pages 757–804, 1990.

[6] P. Bürgisser, M. Clausen, and M. Shokrollahi. *Algebraic complexity theory*. Springer-Verlag, 1997.

[7] P. Bürgisser and C. Ikenmeyer. Geometric complexity theory and tensor rank. *arXiv:1011.1350 v1*, 2010.

[8] P. Bürgisser, J. Landsberg, L. Manivel, and J. Weyman. An overview of mathematical issues arising in the geometric complexity theory approach to $VP \neq VNP$. *arXiv: 0907.2850v1 [cs.CC]*, 2009.

[9] S. Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM Symposium on Theory of Computing*, pages 151–158, New York, NY, 1971. ACM.

[10] P. Deligne. La conjecture de weil II. *Publ. Math. Inst. Hau. Étud. Sci.*, 52:137–252, 1980.

[11] L. Fortnow. The status of the P versus NP problem. *CACM*, 52(9):78–86, 2009.

[12] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13:1–46, 2004.

[13] R. Karp. Reducibility among combinatorial problems. In *Complexity of computer computations*, pages 85–103, New York, 1972. Plenum Press.

[14] J. Landsberg, L. Manivel, and N. Ressayre. Hypersurfaces with degenerate duals and the geometric complexity theory program. *arXiv:1004.4802 v1 [math.AG]*, 2010.

[15] L. Levin. Universal sequential search problems. *Problems of information transmission*, 9:115–116, 1973.

[16] T. Mignon and N. Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notices*, pages 4241–4253, 2004.

[17] K. Mulmuley. Geometric complexity theory IX. Technical report, under preparation.

[18] K. Mulmuley. Lower bounds in a parallel model without bit operations. *The SIAM Journal On Computing*, 28(4):1460–1509, 1999.

[19] K. Mulmuley. Geometric complexity theory VII: Nonstandard quantum group for the plethysm problem. Technical Report TR-2007-14, Computer Science Department, The University of Chicago, 2007.

[20] K. Mulmuley. Geometric complexity theory VIII: On canonical bases for the nonstandard quantum groups. Technical Report TR 2007-15, Computer Science Department, The University of Chicago, 2007.

[21] K. Mulmuley. Explicit proofs and the flip. *arXiv:1009.0246 v1 [cs.CC]*, 2010.

[22] K. Mulmuley. Geometric complexity theory VI: The flip via positivity. Technical report, The Computer Science Department, The University of Chicago, 2010.

[23] K. Mulmuley. On P vs. NP and geometric complexity theory. *JACM*, 58(2), 2011.

[24] K. Mulmuley, H. Narayanan, and M. Sohoni. Geometric complexity theory III: on deciding nonvanishing of a Littlewood-Richardson coefficient. *Journal of Algebraic Combinatorics*, pages 1–8, November, 2011.

[25] K. Mulmuley and M. Sohoni. Geometric complexity theory I: an approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

[26] K. Mulmuley and M. Sohoni. Geometric complexity theory II: towards explicit obstructions for embeddings among class varieties. *SIAM J. Comput.*, 38(3):1175–1206, 2008.

[27] A. Razborov. Lower bounds on the monotone complexity of some boolean functions. *Doklady Akademii Nauk SSSR*, 281:798–801, 1985.

[28] V. Strassen. Rank and optimal computation of generic tensors. *Linear Algebra Appl.*, 53:645–685, 1983.

[29] L. Valiant. The complexity of computing the permanent. *TCS*, 8:189–201, 1979.

[30] H. Weyl. *Classical groups*. Princeton University Press, Princeton, NJ, 1946.