Geometric Complexity Theory: abstract

Dedicated to Sri Ramakrishna

Ketan D. Mulmuley *
The University of Chicago

http://ramakrishnadas.cs.uchicago.edu

Technical report TR-2007-12,
Comp. Sci. Dept., The University of Chicago,
September, 2007

September 4, 2007

This article gives a nontechnical abstract of geometric complexity theory (GCT), an approach to the P vs NP and related problems in complexity theory via algebraic geometry and representation theory. This, followed by [GCTflip1] and [GCTintro], should provide an introduction to GCT for computer scientists who wish to get a high-level picture before going any further. In this article, the underlying field of computation is taken be $\mathbb{C}$. No familiarity with algebraic geometry or representation theory is assumed.

The basic principle underlying GCT is called the *flip* [GCTflip1]. It, in essence, reduces the negative hypotheses (lower bound problems) in complexity theory, such as the $P \neq ? NP$ problem in characteristic zero, to positive hypotheses in complexity theory (upper bound problems): specifically, to showing that a series of decision problems in representation theory and algebraic geometry belong to the complexity class P. This constitutes a flip from *hard, nonexistence* to *easy existence*. It was motivated by the *classical flip*–from the undecidable (negative) to the decidable (positive)–that occurs in Gödel's incompleteness theorem.

*Part of this work was done while the author was visiting I.I.T. Mumbai

1 The flip

There are actually two flips within this flip: (1) from nonexistence to existence, and (2) from hard to easy.

The flip from nonexistence to existence is addressed in [GCT1, GCT2]. Here the nonexistence (lower bound) problem is reduced to an existence problem-specifically, to the problem of proving existence of *obstructions*, which serve as "proofs" or "witnesses" for nonexistence of efficient computational circuits for the explicit hard function in the lower bound problem under consideration–just as existence of a forbidden Kurotowoski minor in a graph serves as an obstruction, i.e., a "proof" for nonexistence of a planar embedding. The explicit hard functions in the lower bound problems under consideration have to be chosen in a very special way for GCT to work. For the P vs. NP problem, such a special (co)-NP complete function is the one called $E(X) = E(x_1, \ldots, x_n)$ in [GCT1]. Thus existence of an obstruction in this context for given input size n and circuit size m would imply that $E(X)$ cannot be computed by a circuit of size m over $\mathbb{C}$ (actually, a minor variant of this).

The obstructions in GCT are representation-theoretic gadgets with algebro-geometric significance. The main algebro-geometric results and arguments in [GCT2, GCT10] roughly say that such obstructions should exist in the context of the P vs. NP problem, assuming that $P \neq NP$; similarly, for other related lower bound problems. This addresses the easier half of the flip from nonexistence to existence.

But how should one prove that obstructions actually exist? The main hypothesis governing the flip is the following:

Hypothesis 1.1 (PHflip) *[GCTflip1] Consider the P vs. NP problem over $\mathbb{C}$. Let $E(X)$ be the explicit function in [GCT1] mentioned above. Then the following problems are "easy"; i.e., belong to P.*

(a) Verification of an obstruction: given input size n, circuit size m, and a combinatorial classifying label (name) of a representation-theoretic gadget, decide if that gadget is an obstruction for computation of $E(X)$ by a circuit of size m for input size n. The goal is an algorithm that takes time polynomial in n, m and the bitlength of the label.

(b) Search and construction of an obstruction: Decide if there exists an obstruction–i.e. a representation-theoretic gadget of the kind under consideration–for given input size n, and circuit size m. Also construct one, if it does. The

goal is an algorithm that takes time polynomial in n and m.

(c) The associated decision problems in algebraic geometry and representation theory.

Each of the decision problems in (c) is of the form: Given a nonnegative structural constant in representation theory or algebraic geometry, decide if it is nonzero (positive). These structural constants are akin to the permanent of a nonnegative integer matrix. Nonvanishing of the permanent can be decided in polynomial time, using any polynomial time algorithm for deciding if a bipartite graph has a perfect matching. PHflip (c) says that the situation is similar for all these (much harder) structural constants in algebraic geometry and representation theory.

These decision problems in (c) are the crux of the matter. To decide if obstructions exist as in (b), one needs to decide if these structural constants are zero or nonzero (positive). Once there are easy algorithms as in (c) to decide this, the goal is to use them or rather their structure to show that obstructions indeed exist for all $n \to \infty$, when $m = n^{\log n}$ (say), by showing how to construct one such obstruction (label) $\lambda(n)$, more or less *explicitly*, for every large enough n. We shall call such a constructive proof of existence of obstructions a *P-constructive proof*, since it also yields an algorithm to construct an obstruction-label $\lambda(n)$ in poly(m) time for every n; here P stands for the complexity class P. Existence of such an explicit family $\{\lambda(n)\}$ of obstructions would imply that the specific function $E(X)$ cannot be computed by a circuit of size $n^{\log n}$, thereby implying that $P \neq NP$ over $\mathbb{C}$. This is what is meant by "reduction" from hard nonexistence problems to easy existence problems. This is not a formal Turing machine reduction. If it were, it would be relativizable. It will be discussed in Section 3 below. Assuming at the moment that it works, PHflip implies the flip that we sought: from the original hard nonexistence problem to an easy existence problem for obstructions.

2 The P-barrier and its crossing

But, by divine justice, the task of showing that the problems in PHflip are easy turned out to be extremely hard. Indeed, even the problem of verifying an obstruction, let alone constructing it, turned out to be extremely hard. Because the best algorithm for verification that one can get by using the general purpose algorithms in algebraic geometry and representation theory take space that is double exponential in m and time that is triple exponential in m. The gap between this triple exponential time bound and the poly(m) time bound sought in Hypothesis 1.1 is so huge, that, at the surface, PHflip may seem impossible. This was the main barrier, called the P-barrier, on this path towards the P vs NP problem, when the flip was briefly announced in [GCTconf].

It is crossed in [GCT6] subject to reasonable mathematical assumptions. Specifically, it is shown there that all decision problems in PHflip (c) are indeed in P, assuming certain mathematical positivity hypotheses, called PH1 and PH2 therein.

The positivity hypotheses PH1 roughly say that the structural constants occuring in the decision problems in PHflip (c) have *positive* $\#P$-formulae; i.e., formulae without any alternating signs akin the usual formula for the permanent (in contrast, the usual formula for the determinant has alternating signs). The positivity hypotheses PH2 say that some auxillary structural constants associated with these structural constants are all nonnegative.

The article [GCT6] also provides theoretical and experimental evidence for these positivity hypotheses, points out how their validity is intimately linked to the Riemann hypothesis over finite fields, proved in [Dl2], and the related works in algebraic geometry and the theory of quantum groups [BBD, KL2, Kas3, Lu1, Lu2], and, furthermore suggests a plan for proving them, which seems to need a substantial extension of these works; cf. Figure 1.

The algorithms in [GCT6] are conceptually extremely simple–just simple variations of linear programming. The quantum group and algebraic geometry machinery is needed only to prove that these extremely simple algorithms are actually correct.

To see what this means, let us consider the algorithm in [GCT6] for the deciding if there exists a simpler kind of obstruction called a *geometric obstruction* for given n and m; cf. PHflip (b). The main mathematical results in [GCT6] together with the positivity hypotheses PH1 and PH2 imply that there exist convex polytopes $P_{m,n}$ and $Q_{m,n}$ such that the relative difference $R_{m,n} = P_{m,n} \setminus Q_{m,n}$ is nonempty iff there exists a geometric obstruction to the computation of $E(X)$ for given n and m, and furthermore, the label of such an obstruction can be computed in polynomial time given a rational point in $R_{m,n}$. So it suffices to simply check if $R_{m,n}$ is nonempty, and construct a rational point in it, if so. This can be done in polynomial time using the convex (linear) programming algorithm in [GLS], if the the number of constraints of $Q(m,n)$ is polynomial in m. (The number of constraints in

$$\boxed{\text{Complexity theoretic negative hypotheses (lower bound problems)}}$$

$$\Big\downarrow \text{The flip}$$

$$\boxed{\text{Complexity theoretic positive hypotheses (upper bound problems)}}$$

$$\Big\downarrow \text{GCT6}$$

$$\boxed{\text{Mathematical positivity hypotheses}}$$

$$\Big\downarrow \text{?}$$

$$\boxed{\text{(?): Extension of the Riemann hypothesis over finite fields, and related work}}$$

Figure 1: Crossing the P-barrier

the actual problem can be exponential in m, but that is not a serious issue [GCTflip1]). Furthermore, it is expected, for the mathematical reasons given in [GCT6], that there exists a genuinely simple, i.e., purely combinatorial algorithm for this problem that does not even need linear programming. That is, the story is expected to be the same as for the min-cost flow problem in combinatorial optimization, for which a linear-programming-based polynomial-time algorithm was found first [Ta], to be followed by several genuinely simple and purely combinatorial polynomial time algorithms; e.g. cf. [O].

The story is expected to be similar for a more complex kind of obstruction, called *modular obstruction* [GCT6].

3 Transformation of easy algorithms into easy proof

Assuming this, let us now explain what is meant by "reduction" from lower bounds to upper bounds in the flip, as shown in the topmost arrow of Figure 1. The goal is to use the structure of the easy algorithms for the basic decision problems in PHflip (c) to get a P-constructive proof of existence of an obstruction for every $n \to \infty$, when $m = n^{\log n}$.

To illustrate how to do this, let us not worry about modular obstructions, and just imagine that all obstructions are of the geometric kind. Furthermore, as an analogy, let us imagine than the polytope $P_{m,n}$, which arises in the context of geometric obstructions, is actually the perfect matching polytope of a bipartite graph $G_{m,n}$ and that the polytope $Q_{m,n}$ is empty. Then $R_{m,n} = P_{m,n} \setminus Q_{m,n} = P_{m,n}$ is nonempty iff $G_{m,n}$ has a perfect matching, which then can be thought of as an obstruction in this analogy. Let us assume that we have a simple polynomial-time algorithm–say the Hungarian method-for deciding if $R_{m,n}$ is nonempty, i.e, if $G_{m,n}$ has a perfect matching, and the goal is to show, using structure and techniques underlying this algorithm that $G_{m,n}$ always has a perfect matching, as expected, when $m = n^{\log n}$, as $n \to \infty$. In other words, we have to give an algorithmic (constructive) proof of existence of a perfect matching in every such $G_{m,n}$.

This may be done as follows. Using the structure of the Hungarian algorithm, we can prove a structure theorem, namely, Hall's marriage theorem. This says that every bipartite graph H, in which every subset on any side of the graph has at least as many neighbours as the size of that subset, has a perfect matching. Using this structure theorem, we then have to show that $G_{m,n}$ indeed has a perfect matching whenever $m = n^{\log n}$, $n \to \infty$. This will then yield an an algorithmic (constructive) proof for existence of an obstruction for every large enough n, assuming $m = n^{\log n}$. Furthermore, this constructive proof technique also yields an easy (polynomial time) procedure to get an explicit obstruction $\lambda(n)$ for every $n \to \infty$. Hence it is a P-constructive proof.

Now the polyhedral set $P_{m,n}$ that actually arises in our setting is not a perfect matching polytope. But it can be expected to be as nice, in fact, even nicer than the perfect matching polytope. For example, the hive polytope [KT1] which arises in the context of the simplest basic prototype of the decision problems in PHflip (c) (called the Littlewood-Richardson problem in representation theory) are known to be extremely regular and well behaved polytopes with remarkable representation-theoretic and algebraic geometric properties. The situation is expected to be the same for the polytopes $P_{m,n}$ and $Q_{m,n}$ that arise in our setting. Hence, it is reasonable to assume that the easy algorithm as above for deciding if a geometric obstruction exists (PHflip(b)) would lead to the sought P-constructive proof of existence of obstructions.

So far we are assuming that all obstructions are geometric. In the presence of modular obstructions the story should be more complex but similar [GCT6].

It may be remarked that for such a transformation of an easy algorithm into an easy (feasible) constructive proof to work it is crucial that the algorithm to be transformed works in polynomial-time and, has, furthermore, reasonably simple structure. The underlying informal principle here, which cannot be proved, is that the mathematical complexity of an algorithmic constructive proof is intimately linked with the computational complexity of the algorithm on which it is based. This is why there is no nontrivial result (comparable to Hall's marriage theorem) for Hamiltonian paths–because the problem of finding such a path is NP-complete.

Assuming that the transformation works as above, [GCT6] has, "in essence", reduced the positive complexity theoretic hypotheses to mathematical positivity hypotheses (see the middle arrow in Figure 1).

4 Obstructions vs. expanders

Before we can describe the plan in [GCT6] to prove these mathematical positivity hypotheses, we should explain why the obstructions in GCT are in a sense generalizations of expanders [LPS, Ma] from constant depth circuits to superpolynomial depth circuits. Specifically, obstructions are to superpolynomial depth circuits what expanders are to constant depth, in fact, depth two circuits. In view of this relationship, explicit construction of obstructions that GCT goes for would be to superpolynomial depth circuits what explicit construction of expanders is to constant depth circuits.

To see this relationship, let us recall the hardness-vs-randomness principle [IW, KI, NW]. It says that some restricted forms of lower bounds can be obtained by good derandomization techniques, or in other language, by designing efficient pseudo-random generators. At present, we do not have pseudo-random generators that are good enough to yield a lower bound result for constant depth circuits. But for the sake of discussion, let us imagine that the expander in, say [LPS, Ma], can be generalized further to obtain a hypothetical structure, which we shall call a *strong expander*, using which one can obtain an efficient pseudo-random generator, whose existence implies separation of the class NC^1 from AC^0, where NC^1 is the class of problems that can be solved by circuits of logarithmic depth, and AC^0 the class of problems that can be solved by circuits of constant depth. This would provide an explicit-construction-based proof of separation of NC^1 from AC^0 in contrast to the known proofs [BS] based on probabilistic methods. We also assume here that the problem of constructing such a strong expander belongs to (nonuniform) AC^0. That is, such a strong expander can be constructed by a nonuniform circuit of constant depth, just like the expander in [LPS, Ma]. Now the existence of such a family $\{E_n\}$ of strong expanders, for each n, would imply that an explicit function in NC^1, depending on the pseudo-random generator, cannot be computed by a circuit of constant depth. Hence such strong expanders can now be regarded as obstructions for computation of an explicit NC^1-function by constant depth circuits. It is in this sense that GCT obstructions are to superpolynomial depth circuits what strong expanders are to constant depth circuits.

The article [RR] says that nonconstructive probabilistic techniques, akin to those used in the constant-depth lower bound results, would not work in the context of the P vs. NP problem. Hence we go explicit construction of obstructions in GCT in the spirit of explicit construction of expanders in [LPS, Ma, RVW], because the naturalizability barrier in [RR] would not apply to explicit-construction-based techniques.

It is may be remarked that the expander in [LPS, Ma] can actually be constructed by a nonuniform (algebraic) circuit of depth two. So an expander (as against the hypothetical strong expander) actually belongs to depth two circuits. Hence, it can serve as an obstruction for computation by a circuit of depth at most two (really, just one). But there is no nontrivial lower bound problem of this kind. This is why the present expanders cannot be used in lower bound problems.

The discussion in this section is summarized in Figure 2.

$$\begin{array}{c} \uparrow \\ \text{depth} \\ | \\ \boxed{\text{Superpolynomial depth circuit: Obstruction in GCT}} \\ \uparrow \\ | \\ \boxed{\text{Constant depth circuit: Strong expander}} \\ \uparrow \\ | \\ \boxed{\text{Depth two circuit: expander}} \end{array}$$

Figure 2: The relationship between obstructions and expanders

5 Mathematical positivity hypotheses and the Riemann hypothesis

Using the analogy between obstructions and expanders we shall now explain the relationship between the mathematical positivity hypotheses PH1 and PH2 in [GCT6] with the Riemann hypothesis over finite fields.

For this let us observe that, though the explicit construction of expanders is “extremely easy” (nonuniform AC^0), its correctness is based on a nontrivial mathematical positivity hypothesis:

PHspectral: The spectral gap of an expander is bounded below by a positive constant.

The mathematical positivity hypotheses PH1 and 2 in [GCT6] can be regarded as (nonspectral) analogues of PHspectral in the setting of superpolynomial depth circuits.

The proof of PHspectral in [LPS] in the case of expanders depends on the Riemann hypothesis over finite fields (for curves) [Dl2], which is again a deep positive statement. We say that the Riemann Hypothesis (over finite fields) is positive, because its usual statement is, after all, a positive statement, and furthermore, it can also be reformulated as stipulating positivity (nonnegativity) of some mathematical quantities (cf. page 458 in [Ha]). It should not be a surprise then that what is needed to prove to the positivity hypotheses PH1, PH2 mentioned above is, in essence, an extension of the Riemann hypothesis over finite fields, and the results surrounding it. But given the big gap between constant depth circuits and superpolynomial depth circuits it would have been a great surprise if the existing *standard* Riemann Hypothesis over finite field were to suffice. And it does not, as expected. What seems to be needed are *nonstandard extensions* of the Riemann hypothesis over finite fields [Dl2], and the related results [BBD, KL2, Kas3, Lu1, Lu2].

We shall now briefly indicate what is meant by nonstandard extensions. Specifically, in GCT6 certain positivity hypotheses, called *PH0*, are formulated, and it is pointed out how and why these may lead to the proof of the required PH1 and PH2 (or rather its weaker form called SH, saturation hypothesis, which is sufficient for our purposes). These PH0 hypotheses are generalized forms of a deep positivity statement in the theory of *standard quantum groups* [Dri, Ji, RTF], namely: their representations and coordinate rings have *canonical bases* [Kas2, Lu1, Lu2], whose structural constants, determining their representation-theoretic and multiplicative structure, are all nonnegative. But the theory of standard quantum groups does not work, as expected, in the context of GCT. In [GCT4, GCT7], a basic theory of nonstandard quantum groups as needed for GCT is set up, with its conjectural further extension, as needed, pointed out in [GCT10]. Furthermore [GCT8] gives a conjecturally correct algorithm for constructing the required canonical bases of the irreducible representations and coordinate rings of the nonstandard quantum groups in [GCT4, GCT7]. These are natural generalizations of the canonical bases mentioned above due to Kashiwara and Lusztig [Kas2, Lu1, Lu2] for the irreducible representations and coordinate rings of the standard quantum group. Furthermore, [GCT8] also gives an analogous conjecturally correct algorithm to construct canonical bases of the nonstandard deformations of the symmetric group ring, which are dually paired with the nonstandard quantum groups. These generalize the Kazhdan-Lusztig basis [KL1] of the Hecke algbra.

The only known proof of correctness [Lu1, Lu2] of the canonical basis construction in the theory of standard quantum groups that also proves simultaneously the required positivity properties of the associated structural constants is based on the (standard) Riemann Hypothesis over finite fields [Dl2], and the related work [BBD]. So what seems to be needed [GCT8] for proving correctness of the algorithms for constructing canonical bases in [GCT8] and PH0 are *nonstandard extensions* of the Riemann hypothesis over finite fields and the related work. We, personally, do not have the mathematical expertize to even formulate these hypotheses, let alone prove them. But theoretical and experimental evidence in [GCT4, GCT7, GCT8] suggests that such extensions exist, and that they ought to be provable by a systematic extension of the theory of standard quantum groups to nonstandard quantum groups. Hence it is reasonable to hope now that the experts will be able to formulate and prove such nonstandard Riemann Hypotheses in due course, which would lead to the proof of PH0 hypotheses, and in turn to the proof of the $P \neq NP$ conjecture over $\mathbb{C}$. The whole picture is summarized in Figure 3. The arrows with question marks are conjectural, the double arrow is unconditional. The ? signs indicate the main open problems at the heart of this approach.

The proof over $\mathbb{C}$ may eventually extend to finite fields (as in the usual form of the conjecture) along the lines suggested in [GCT11]. Thus the ultimate goal of the GCT flip is to deduce the ultimate negative hypothesis of mathematics, the $P \neq NP$ conjecture, in essence, from the ultimate positive hypotheses in mathematics, the (nonstandard) Riemann Hypotheses, thereby giving the ultimate flip; see Figure 4.

Logical dependence dependence among the GCT papers and a suggested reading sequence is shown in Figure 5.

Acknowledgement

The author is deeply grateful to Madhav Nori, who taught him algebraic geometry, Milind Sohoni, who collaborated in GCT 1-4, and Manju the source of energy behind this work.

(?): Nonstandard Riemann Hypotheses for the quantum groups in [GCT4, GCT7], and their conjectural extensions in [GCT10]

?

$\downarrow$

PH0 (?): Existence of canonical bases; cf. [GCT6, GCT8]

?

$\downarrow$

PH1,SH (PH2)

GCT6

$\Downarrow$

Polynomial time algorithms for the decision problems in PHflip (c)

The flip (The reduction mentioned in Section 3)

?

$\downarrow$

Explicit construction of obstructions

$\downarrow$

$P \neq NP$ over $\mathbb{C}$

Figure 3: The basic plan for implementing the flip

References

[A2] M. Agrawal, Proving lower bounds via pseudo-random generators, Proceedings of FSTTCS 2005, 92-105, 2005.

[BBD] A. Beilinson, J. Bernstein, P. Deligne, Faisceaux pervers, Astérisque 100, (1982), Soc. Math. France.

[BS] R. Boppana, M. Sipser: The complexity of finite functions, Handbook of Theoretical Computer Science, vol. A, Edited by J. van Leeuwen, North Holland, Amsterdam, 1990, 757–804.

[Co] S. Cook: The complexity of theorem-proving procedures. Proceedings of the third annual ACM Symposium on Theory of Computing. 151-158. (1971).

[Dl2] P. Deligne, La conjecture de Weil II, Publ. Math. Inst. Haut. Étud. Sci. 52, (1980) 137-252.

[Dri] V. Drinfeld, Quantum groups, Proc. Int. Congr. Math. Berkeley, 1986, vol. 1, Amer. Math. Soc. 1988, 798-820.

[GCTconf] K. Mulmuley, M. Sohoni, Geometric complexity theory, P vs. NP and explicit obstructions, in "Advances in Algebra and Geometry", Edited by C. Musili, the proceedings of the International Conference on Algebra and Geometry, Hyderabad, 2001.

[GCTflip1] K. Mulmuley, On P. vs. NP, geometric complexity theory, and the flip I: a high-level view, Technical Report TR-2007-13, Computer Science Department, The University of Chicago, September 2007. Available at: http://ramakrishnadas.cs.uchicago.edu

[GCTflip2] K. Mulmuley, On P vs. NP, geometric complexity theory, and the flip II, under preparation.

[GCTintro] K. Mulmuley and M. Sohoni, Geometric complexity theory: introduction, technical report TR-2007-16, computer science dept., The university of Chicago, Sept. 2007. Available at: http://ramakrishnadas.cs.uchicago.edu.

[GCT1] K. Mulmuley, M. Sohoni, Geometric complexity theory I: an approach to the P vs. NP and related problems, SIAM J. Comput., vol 31, no 2, pp 496-526, 2001.

[GCT2] K. Mulmuley, M. Sohoni, Geometric complexity theory II: towards explicit obstructions for embeddings among class varieties, to appear in SIAM J. Comput., cs. ArXiv preprint cs. CC/0612134, December 25, 2006. Available at: http://ramakrishnadas.cs.uchicago.edu

[GCT3] K. Mulmuley, M. Sohoni, Geometric complexity theory III, on deciding positivity of Littlewood-Richardson coefficients, cs. ArXiv preprint cs. CC/0501076 v1 26 Jan 2005.

[GCT4] K. Mulmuley, M. Sohoni, Geometric complexity theory IV: quantum group for the Kronecker problem, cs. ArXiv preprint cs. CC/0703110, March, 2007. Available at: http://ramakrishnadas.cs.uchicago.edu

[GCT5] K. Mulmuley, H. Narayanan, Geometric complexity theory V: on deciding nonvanishing of a generalized Littlewood-Richardson coefficient, Technical report TR-2007-05, Comp. Sci. Dept. The university of chicago, May, 2007.

[GCT6] K. Mulmuley, Geometric complexity theory VI: the flip via saturated and positive integer programming in representation theory and algebraic geometry, Technical report TR 2007-04, Comp. Sci. Dept., The University of Chicago, May, 2007. Available at: http://ramakrishnadas.cs.uchicago.edu. Revised version to be available here.

[GCT7] K. Mulmuley, Geometric complexity theory VII: a quantum group for the plethysm problem, technical report TR-2007-14, computer science dept., The university of Chicago, Sept. 2007. Available at: http://ramakrishnadas.cs.uchicago.edu.

[GCT8] K. Mulmuley, Geometric complexity theory VIII: On canonical bases for the nonstandard quantum groups, technical report TR-2007-15, computer science dept., The university of Chicago, Sept. 2007. Available at: http://ramakrishnadas.cs.uchicago.edu.

[GCT9] B. Adsul, M. Sohoni, K. Subrahmanyam, Geometric complexity theory IX: algbraic and combinatorial aspects of the Kronecker problem, under preparation.

[GCT10] K. Mulmuley, Geometric complexity theory X: On class varieties, and the natural proof barrier, under preparation.

[GCT11] K. Mulmuley, Geometric complexity theory XI: on the flip over finite or algebraically closed fields of positive characteristic, under preparation.

[GLS] M. Grötschel, L. Lovász, A. Schrijver, Geometric algorithms and combinatorial optimzation, Springer-Verlag, 1993.

[Ha] R. Hartshorne, Algebraic geometry, Springer, 1997.

[LPS] A. Lubotzky, R. Phillips, P. Sarnak: Ramanujan graphs, Combinatorica 8 (1988), 261-277.

[Ma] G. Margulis: Explicit constructions of concentrators, Problemy Inf. Trans. 9 (1973), 325-332.

[IW] R. Impagliazzo, A. Wigderson, P=BPP if E requires exponential size circuits: Derandomizing the XOR lemma, in proceedings of Annual ACM Symposium on the Theory of Computing, pages 220-229, 1997.

[Ji] M. Jimbo, A q-difference analogue of $U(\mathcal{G})$ and the Yang-Baxter equation, Lett. Math. Phys. 10 (1985), 63-69.

[KI] V. Kabanets, R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds, in proceedings of Annual ACM Symposium on the Theory of Computing, 355-364, 2003.

[Ka] R. Karp: Reducibility among combinatorial problems. R. E. Miller and J. W. Thatcher (eds.) Complexity of computer computations, Plenum Press, New York, 1972, 85-103.

[Kas2] M. Kashiwara, On crystal bases of the q-analogue of universal enveloping algebras, Duke Math. J. 63 (1991), 465-516.

[Kas3] M. Kashiwara, Global crystal bases of quantum groups, Duke Mathematical Journal, vol. 69, no.2, 455-485.

[KL1] D. Kazhdan, G. Lusztig, Representations of Coxeter groups and Hecke algebras, Invent. Math. 53 (1979), 165-184.

[KL2] D. Kazhdan, G. Lusztig, Schubert varieties and Poincare duality, Proc. Symp. Pure Math., AMS, 36 (1980), 185-203.

[KT1] A. Knutson, T. Tao, The Honeycomb model of $GL_n(\mathbb{C})$ tensor products I: proof of the saturation conjecture, J. Amer. Math. Soc, 12, 1999, pp. 1055-1090.

[Le] A. Levin: Universal sequential search problems. Problems of information transmission (translated from Problemy Peredachi Informatsii (Russian)) 9 (1973).

[Lu1] G. Lusztig, Canonical bases arising from quantized enveloping algebras, J. Amer. Math. Soc. 3, (1990), 447-498.

[Lu2] G. Lusztig, Introduction to quantum groups, Birkhäuser, 1993.

[NW] N. Nisan, A. Wigderson, Hardness vs. randomness, J. Comput. Sys. Sci., 49 (2): 149-167, 1994.

[O] J. Orlin, A faster strongly polynomial minimum cost flow algorithm, proceedings of the twentieth Annual Symposium on Theory of Computing, 1988.

[Re] O. Reingold, Undirected s-t-connectivity in logspace, in proceedings of Annual ACM symposium on the Theory of Computing, 376-385, 2005.

[RVW] O. Reingold, S. Vadhan, A. Wigderson, Entropy waves, the zig-zag graph product and new constant-degree, Ann. of Math (2). vol 155 (2002), no. 1, 157-187.

[RTF] N. Reshetikhin, L. Takhtajan, L. Faddeev, Quantization of Lie groups and Lie algebras, Leningrad Math. J., 1 (1990), 193-225.

[RR] A. Razborov, S. Rudich, Natural proofs, J. Comput. System Sci., 55 (1997), pp. 24-35.

[Ta] E. Tardos, A strongly polynomial algorithm to solve combinatorial linear programs, Operations Research 34 (1986), 250-256.

$$\boxed{\text{(?): Nonstandard Riemann Hypotheses (+)}}$$

$$\Big\downarrow ?$$

$$\boxed{\text{The } P \neq NP \text{ conjecture (-)}}$$

Figure 4: The ultimate goal of the GCT flip

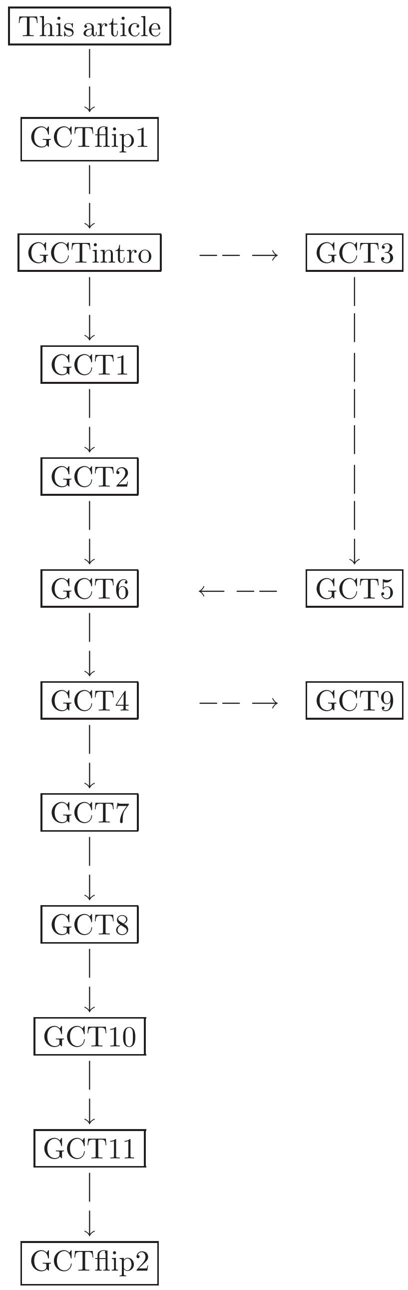

Figure 5: Logical dependence among the GCT papers