ANNALS OF MATHEMATICS

Complexity classes as mathematical axioms

By Michael H. Freedman

SECOND SERIES, VOL. 170, NO. 2

September, 2009

ANMAAH

Annals of Mathematics, **170** (2009), 995–1002

Complexity classes as mathematical axioms

By MICHAEL H. FREEDMAN

Abstract

Complexity theory, being the metrical version of decision theory, has long been suspected of harboring undecidable statements among its most prominent conjectures. Taking this possibility seriously, we add one such conjecture, $P^{\#P} \neq NP$, as a new "axiom" and find that it has an implication in 3-dimensional topology. This is reminiscent of Harvey Friedman's work on finitistic interpretations of large cardinal axioms.

1. Introduction

This short paper introduces a new subject with a simple example. The theory of computation defines a plethora of complexity classes. While the techniques of diagonalization and oracle relativization have produced important separation results, for nearly forty years the most interesting (absolute) separation conjectures, such as $P \neq NP$, remain unproven, and with the invention of ever more complexity classes, analogous separation conjectures have multiplied in number.

With no prospect in sight for proving these conjectures (within ZFC) and the suspicion that some are actually independent, we propose considering them instead as potential axioms and looking for what implications they might have in mathematics as a whole. This program is analogous to the search for interesting "finitistic" consequences of large cardinal axioms, an area explored by Harvey Friedman and collaborators (e.g. [4]). (Although, in the latter case, the large cardinal axioms are actually known to be independent of ZFC.)

What would be the best possible theorem in this subject? It would be to postulate a very weak separation "axiom," say $P \neq PSPACE$, and prove the Riemann hypothesis, an important mathematical result apparently far removed from complexity theory. Of course, we should be more modest. We will assume a more technical but well accepted separation "axiom" $P^{\#P} \neq NP$, which we call

Work partly done at Aspen Physics Center.

Axiom A, and prove a theorem, Theorem A, in knot theory. The theorem is easily and briefly expressed in terms of classical notions such as "girth" and "Dehn surgery" and appears to be as close to current research topics in knot theory as the known finitistic implications of the large cardinal axioms are to research in Ramsey theory, to continue that analogy. Theorem A is extremely believable but seems to exist in a "technique vacuum." What makes the theorem interesting is that it sounds both "very plausible" and "impossible to prove."

2. **Theorem A**

We consider smooth links L of finitely many components in $\mathbb{R}^3$ and their planar diagrams D. The girth of a diagram D (in the xz-plane), $g(D)$, may be defined as the maximum over all lines $z =$ constant of the cardinality of the horizontal intersection $|D \cap (z = \text{constant})|$. For a link L, we define girth$(L) = \min\{g(D) \mid D$ is a diagram of $L\}$. Similarly, the complexity number $c(D)$ of a link diagram is defined as half its number of crossings plus half the number of local maxima and minima with respect to the z-coordinate. The complexity of a link, $c(L)$, equals $\min\{c(D) \mid D$ is a diagram of $L\}$. Theorem A addresses how girth can change under certain equivalence relations $\sim_r$ defined below.

Let $r \neq 6$ be an integer greater than or equal to 5. Consider passing from a link L to $L \amalg U$, the disjoint union of L and an additional unknotted component U, and then from $L \amalg U$ to L' by performing $\frac{\pm 1}{4r}$-Dehn surgery on U. Denote by $\sim_r$ the equivalence relation on links generated by $L \to L'$. In other words, this equivalence relation allows us to sequentially locate imbedded 2-disks Δ transverse to L and perform a $\pm 8\pi r$ twist across Δ to modify L; after several steps, we have arrived at a link, which we will denote L', "equivalent" to L. In slight abuse of notation, we also consider $\sim_r$ as an equivalence relation on diagrams: $D \sim_r D'$ if and only if D represents L, D' represents L', and $L \sim_r L'$.

If D and D' are diagrams for the same link L, we may take their distance to be the minimum number of Reidemeister/Morse moves connecting D to D'. Representative examples of these moves are displayed in Figure 1. We consider only diagrams in Morse position with respect to the z-coordinate and include in our count births, deaths, and level crossings, as well as the three familiar Reidemeister moves. Suppose next that D and D' are diagrams for $\sim_r$ equivalent links L and L'. We need a measure of the distance between D and D'. It does not make sense to count each Dehn surgery as one step since the disk Δ may have an unboundedly complicated relation to L. There is no loss of generality, since D can be modified by Reidemeister/Morse moves, in considering only disks Δ that meet D in the standard form, seen in Figure 2. More precisely, after Reidemeister/Morse moves,

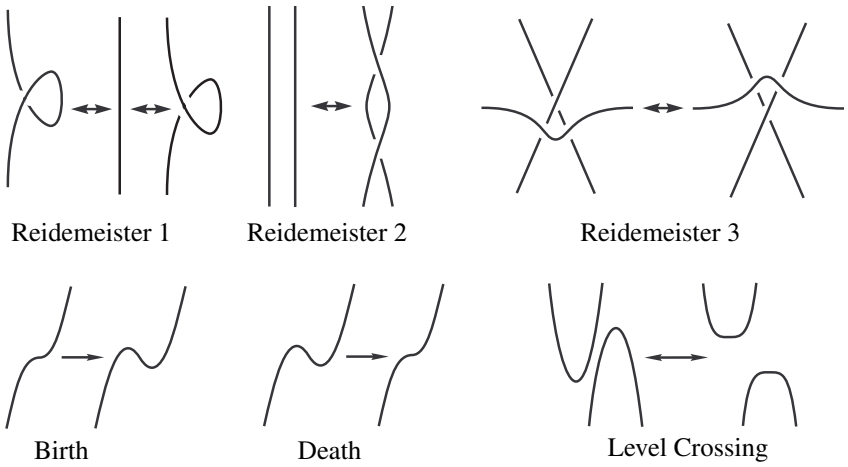

Figure 1

we may assume that in $D(L \amalg U)$, U bounds a disk Δ and a neighborhood of Δ in $D(L \amalg U)$ appears as in Figure 2.

Since $\pm 4r$-twisting along Δ introduces $4rn(n-1)$ crossings, we will call half this, $2rn(n-1)$, the distance between the twisted and untwisted diagrams. Now, $\text{dist}_r(D, D')$ can be defined to be the minimum number of (weighted) steps from D to D' where each isotopy induced, Reidemeister/Morse move is given weight 1, except Reidemeister 1 which is weighted $\frac{3}{2}$ since three features can appear, a crossing, a local max and a local min, and each standard form $4r$-twist along Δ is given weight $2rn(n-1)$. (The exact form of dist_r is irrelevant. What is important is that if D and D' have a polynomial "distance" (in $\max(c(D), c(D'))$) then there is a polynomial sized certificate demonstrating that $L \sim_r L'$. This clearly holds for dist_r as defined.)

THEOREM A. *If $r \geq 5$ is an integer not equal to 6, p a polynomial of one variable, and $b, b' > 0$ any constants, then there exists a diagram D such that if $D \sim_r D'$ then*

$$g(D') > b \log(c(D)) + b' \quad \textit{unless} \quad \text{dist}_r(D, D') > p(c(D)).$$

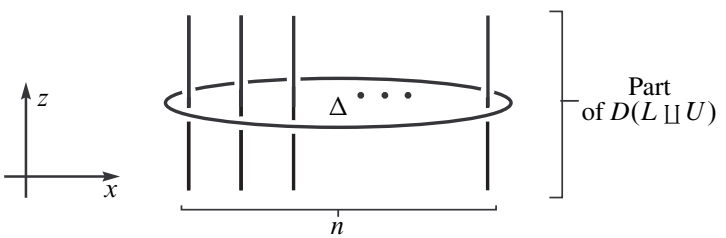

Figure 2

Roughly, the theorem says that some links L cannot be made, via $\sim_r$, extremely thin except possibly by an extraordinarily elaborate sequence of moves. It would be a surprise if the second alternative actually occurred. In high dimensions [7], unsolvability of the triviality problem for groups implies that geometric landscapes, for example that of the 5-sphere in S^6, are extremely (nonrecursively) rough. However, this phenomenon has not been seen in three manifold topology so it would be a surprise if girth could be reduced only by a very long sequence of moves. We conjecture that Theorem A remains true with the second alternative omitted. However, for this statement no complexity axiom appears to unlock the proof.

In the 1990's, A. Thompson [11] pointed out to me that girth, by itself, can sometimes be computed exactly (see Claim below). However, the equivalence relation $\sim_r$ is so disruptive of geometry that it appears to create the "technique vacuum" which we puncture with axiom A.

CLAIM. *Let k be the (p,q)-torus knot. Then $g(k) = 2\min(p,q)$.*

Proof. So, $k \subset T \subset \mathbb{R}^3$, where T is an unknotted torus which we assume without loss of generality to be in generic (Morse) position with respect to the z-coordinate of $\mathbb{R}^3$. A straightforward homological argument shows that some z-level must intersect T in one, in fact two, essential circles $C \coprod C' \subset T$. One easily builds imbedded disks (from bits of the level plane and subsurfaces of T) D and D' with $\partial D = D \cap T = C$ and $\partial D' = D' \cap T = C'$. Thus, C and C' are both meridians or both longitudes of T and therefore must contain at least $2\min(p,q)$ points of k. □

3. **A complexity reminder**

The inclusions exhibited in Figure 3 are all theorems or tautologies. The exhibited differences are all "separation conjectures" to which we might grant the status of axioms. The existence of a problem $y \in \mathrm{P}^{\#\mathrm{P}} \setminus \mathrm{NP}$ is the axiom, "Axiom A," we add to ZF, Zermelo-Fraenkel set theory, for the "proof" of Theorem A.

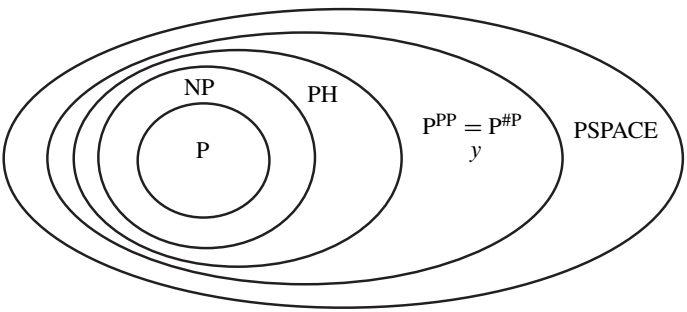

Figure 3

Briefly, P consists of decision (yes/no) problems or languages for which membership is determined in polynomial time (in input size) on a classical computer (Turing machine). NP (nondeterministic polynomial) is the class of languages which have a polynomial time protocol such that "yes" instances have a certificate which is accepted whereas there is no such requirement for "no" instances. #P is the counting analogy to NP and asks how many of a fixed family of potential certificates will be accepted; the paradigmatic example problem being to find the number of assignments satisfying a boolean formula. Since #P is a class of functions, not languages, one sometimes weakens #P to class PP of languages where membership is determined by asking if more than half of the nondeterministic computations are accepting. PP "sees" the first bit of #P. We use the oracle notation P^A in the sense of Cook (also called "Turing reduction"), to mean polynomial time computation assisted by (possibly repeated) calls to the A oracle (post processing permitted). It is known that $\mathrm{P}^{\mathrm{PP}} = \mathrm{P}^{\#\mathrm{P}}$, so weakening #P to a language does not affect its oracular power. A function f is called #P-hard if $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{P}^A$, A an oracle for f. PH denotes the polynomial time hierarchy, a game theoretic extension of NP allowing finite quantification. Toda proved that $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ [12]. Finally, PSPACE is the class of decision problems solvable in an arbitrary amount of time, but using only a polynomial memory resource. See [8] for more background.

We use Axiom A, $\mathrm{P}^{\#\mathrm{P}} \neq \mathrm{NP}$, to prove Theorem A. Failure of Axiom A would imply a large collapse of the polynomial hierarchy PH down to NP, so Axiom A must be considered extremely safe.

4. **Axiom A implies Theorem A**

Our connection between links L and complexity is the Jones polynomial [13] which we write as $J_L(q)$. Evaluations of J_L at roots of unity $\omega = e^{2\pi i/r}$ are known [14] to be computed as the partition function $Z_{\mathrm{SU}(2),k}(S^3, L)$ of the topological quantum field theory (TQFT) associated with the Lie group SU(2) at level $k = r-2$. What will be of critical importance for us is that these Jones evaluations $J_L(\omega)$ will be constant as L is transformed to $L' \sim_r L$.

LEMMA 4.1. *If $L \sim_r L'$ then $J_L(e^{2\pi i/r}) = J_{L'}(e^{2\pi i/r})$.*

Proof. In the $\mathrm{SU}(2)_{r-2}$ theories, all "labels" a (that is, positive normed irreps of the quantum group, or "particle types" in physics language) have twist factor $\theta(a)$ which is a $4r$-th root of unity. Specifically, enumerating $a = 0, \ldots, r-2$, one has $\theta(a) = \beta^{a^2+2a}$ where $\beta = e^{2\pi i/4r}$ [14].

Now consider $L \sqcup U$ where U is a single unknotted loop bounding an imbedded disk Δ transverse to L. Recoupling transforms L to a superposition of trivalent ribbon graphs $\sum \alpha_i G_i$ with identical partition function, where each G_i meets Δ in one edge with label a_i. Now the partition function $Z(S^3, L) = J_L(e^{2\pi i/r})$ can

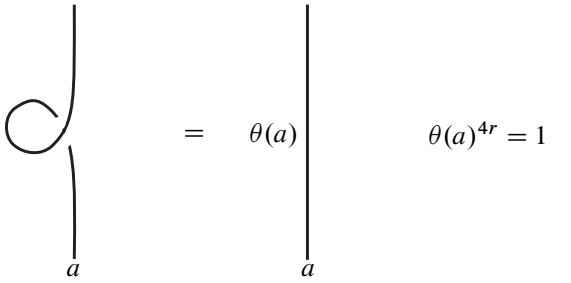

Figure 4

be computed as $\sum \alpha_i Z(G_i)$. But passing from L to L' amounts only to adding $4r$ full twists of the type drawn in Figure 4 to the a_i labeled particle line crossing Δ. Since $\theta(a_i)^{4r} = 1$, $Z(G_i)$ does not change under a $8\pi r$ twist. Consequently, $J_L(e^{2\pi i/r}) = J_{L'}(e^{2\pi i/r})$. I thank Ian Agol for pointing out that Fox [2] considered a relation similar to $\sim_r$ in the 1950's and that Lackenby's theorem 2.1 [6] contains Lemma 4.1. □

It is a theorem of Vertigan ([15] or [16] assisted by the result of [10]) that all nonzero algebraic evaluations of the Jones polynomial $J_L(q)$ are $\#P$-hard functions[1] of the input L with the exceptions of those q satisfying $q^4 = 1$ or $q^6 = 1$. Thus, in oracle notation, $\mathrm{P}^{\mathbb{J}_r} = \mathrm{P}^{\#\mathrm{P}}$ where $\mathbb{J}_r$ accepts L as input and returns (an encoding of the algebraic integer) $J_L(e^{2\pi i/r})$, provided $r \geq 5$ is an integer and $r \neq 6$.

From the lemma we see that the oracle $\mathbb{J}_r$ can work equally well with any link $L' \sim_r L$ as input or any diagram D' for L'. But if $g(D') \leq b \log(c(L)) + b'$, then throughout the computation of the partition function, the "physical" Hilbert space (i.e. the Hilbert space associated by $\mathrm{SU}(2)_k$ TQFT to the $z =$ constant slices of L (with charge $a = 1 =$ fundamental)) will have dimension

$$d < \sum_{i=0}^{r-2} S_{0,i}^{-(b \log c(D(L)) + b')} < \mathrm{poly}(c(D)),$$

using the Verlinde formula (VF), where $S_{0,i} = \sqrt{2/r}\, \sin((i+1)\pi/r)$, the first row of the S-matrix. We have used minus our bound on girth as a lower bound to the Euler characteristic (the exponent in VF) for any $z =$ constant slice of the link complement in $\mathbb{R}^3$.

Thus, there is a prospect of replacing the oracle $\mathbb{J}_r$ entirely with a classical polynomial time computation in this small Hilbert space, by representing crossings by R-matrices and maxima (minima) by (co)units (as in Turaev's book [13]). To do this, two things must happen. First, $c(D')$ cannot be larger than $\mathrm{poly}(c(D))$;

[1] Actually, applying Lagrange interpolation, these functions are shown in [5] to be $\mathrm{FP}^{\#\mathrm{P}}$ complete.

that is, the diagram D', although fairly thin, also must not be too long in the z-direction. Second, there must be a polynomial number of advice bits which encode the steps from D to D' which certify that $D' \sim_r D$. If Theorem A were false, these poly-many advice bits could be used to certify transformations $D \sim_r D'$ where D' would be thin enough, $g(D') < b \log(c(L)) + b'$ and short enough $c(D') < c(D) + p(c(D))$ for a poly-time calculation of $J_{D'}(e^{2\pi i/r})$ to replace appeal to the oracle $\mathbb{J}_r$ implying $\mathrm{P}^{\mathbb{J}_r} \subset \mathrm{NP}$, contradicting Axiom A. We have used that $\mathrm{dist}_r(D, D') < p(c(D))$ implies $c(D') < c(D) + p(c(D))$ since no more than two crossings or two critical points can be added to a diagram per unit weight step. This completes the proof of Theorem A in ZF $\cup$ Axiom A.

5. Conclusion

Mathematical structures such as tilings [1], groups [9], and, in several contexts, links [3] are known to encode quite general computations. If transformations are found which preserve the computational "content" of the structure, then it may be expected that axioms stating a lower bound to computational complexity will limit the scope of such transformations in simplifying the structure.

References

[1] R. BERGER, The undecidability of the domino problem, *Mem. Amer. Math. Soc. No.* **66** (1966), 72. MR 36 #49 Zbl 0199.30802

[2] R. H. FOX, Congruence classes of knots, *Osaka Math. J.* **10** (1958), 37–41. MR 24 #A1718 Zbl 0084.19204

[3] M. H. FREEDMAN, A. KITAEV, M. J. LARSEN, and Z. WANG, Topological quantum computation, *Bull. Amer. Math. Soc.* **40** (2003), 31–38. MR 2003m:57065 Zbl 1019.81008

[4] H. M. FRIEDMAN, Finite functions and the necessary use of large cardinals, *Ann. of Math.* **148** (1998), 803–893. MR 2002b:03108 Zbl 0941.03050

[5] F. JAEGER, D. L. VERTIGAN, and D. J. A. WELSH, On the computational complexity of the Jones and Tutte polynomials, *Math. Proc. Cambridge Philos. Soc.* **108** (1990), 35–53. MR 91h:05038 Zbl 0747.57006

[6] M. LACKENBY, Fox's congruence classes and the quantum-SU(2) invariants of links in 3-manifolds, *Comment. Math. Helv.* **71** (1996), 664–677. MR 97m:57007 Zbl 0871.57003

[7] A. NABUTOVSKY, Non-recursive functions, knots "with thick ropes", and self-clenching "thick" hyperspheres, *Comm. Pure Appl. Math.* **48** (1995), 381–428. MR 96d:58025 Zbl 0845.57023

[8] C. H. PAPADIMITRIOU, *Computational Complexity*, Addison-Wesley Publ. Co., Reading, MA, 1994. MR 95f:68082 Zbl 0833.68049

[9] J. STILLWELL, The word problem and the isomorphism problem for groups, *Bull. Amer. Math. Soc.* **6** (1982), 33–56. MR 82m:20039 Zbl 0483.20018

[10] M. B. THISTLETHWAITE, A spanning tree expansion of the Jones polynomial, *Topology* **26** (1987), 297–309. MR 88h:57007 Zbl 0622.57003

[11] A. THOMPSON, Private communication.

[12] S. TODA, On the computational power of PP and $\oplus$P, *Proc. 30th* IEEE *Symposium on the Foundations of Computer Science* (1989), 514–519.

[13] V. G. TURAEV, *Quantum Invariants of Knots and 3-Manifolds*, *de Gruyter Stud. Math.* **18**, Walter de Gruyter & Co., Berlin, 1994. MR 95k:57014 Zbl 0812.57003

[14] V. G. TURAEV and N. RESHETIKHIN, Invariants of 3-manifolds via link polynomials and quantum groups, *Invent. Math.* **103** (1991), 547–597. MR 92b:57024 Zbl 0725.57007

[15] D. VERTIGAN, The computational complexity of Tutte, Jones, Homfly and Kaufman invariants, Ph.D. thesis, Oxford University, Oxford, England, 1991.

[16] _____, The computational complexity of Tutte invariants for planar graphs, SIAM *J. Comput.* **35** (2005), 690–712. MR 2006k:68045 Zbl 1089.05017

(Received October 1, 2008)

E-mail address: michaelf@microsoft.com
MICROSOFT CORPORATION, CNSI BUILDING, RM. 2245, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CA 93106-6105

http://stationq.cnsi.ucsb.edu/~freedman/