Proc. Natl. Acad. Sci. USA
Vol. 95, pp. 98–101, January 1998
Computer Sciences

P/NP, and the quantum field computer

MICHAEL H. FREEDMAN

Microsoft Research 9N, 1 Microsoft Way, Redmond, WA 98052

Contributed by Michael H. Freedman

ABSTRACT **The central problem in computer science is the conjecture that two complexity classes, *P* (polynomial time) and *NP* (nondeterministic polynomial time—roughly those decision problems for which a proposed solution can be checked in polynomial time), are distinct in the standard Turing model of computation: $P \neq NP$. As a generality, we propose that each physical theory supports computational models whose power is limited by the physical theory. It is well known that classical physics supports a multitude of implementation of the Turing machine. Non-Abelian topological quantum field theories exhibit the mathematical features necessary to support a model capable of solving all $\#P$ problems, a computationally intractable class, in polynomial time. Specifically, Witten [Witten, E. (1989) *Commun. Math. Phys.* 121, 351–391] has identified expectation values in a certain $SU(2)$-field theory with values of the Jones polynomial [Jones, V. (1985) *Bull. Am. Math. Soc.* 12, 103–111] that are $\#P$-hard [Jaeger, F., Vertigen, D. & Welsh, D. (1990) *Math. Proc. Comb. Philos. Soc.* 108, 35–53]. This suggests that some physical system whose effective Lagrangian contains a non-Abelian topological term might be manipulated to serve as an analog computer capable of solving *NP* or even $\#P$-hard problems in polynomial time. Defining such a system and addressing the accuracy issues inherent in preparation and measurement is a major unsolved problem.**

It is known that the partition function, correlation functions, and other observables in field theory and statistical mechanics are generally hard to compute. In idealized models the level of hardness can often be established within the computational hierarchy. We find that for topological quantum field theories (TQFTs), where the combinatorial nature of the propagation allows a complete analysis, hardness and noncommutativity are tightly linked. More broadly, we propose that a physical system S with a non-Abelian topological term in its Lagrangian may have observables that are *NP*-hard (or even $\#P$-hard) functions of their preparation parameters. The topological character of S is consistent with the exact preparation of a discrete initial state, e.g., a knot type. A central difficulty will be extracting the "hard" information with measurements of limited accuracy. The accuracy challenge may have been met, at least theoretically, by certain models of quantum computation (1, 2, $*$) in which (*i*) a multi-bit state projection is read out a spin at a time and (*ii*) the algorithm employed ensures the state projection will, with high probability, contain useful information. Solving the accuracy problem for S could, in principle, lead to an analog computer based on preparation and observation of S capable of solving all $\#P$-problems in polynomial time.

We begin with a brief sketch of computational concepts. The Turing machine T represents an abstraction of the principles of mechanical computation. The machine consists of a head and a tape. The head is capable of being in one of a finite number of "internal states" $\{q_i\}$ and can read and overwrite a symbol $\in \{S_j\}$ from a finite set of symbols and then shift one block left or right along the tape. It contains a finite internal program that directs its operations.

Consider a problem Q, with a yes/no answer, for which infinitely many instances exist, for example, the satisfiability of Boolean formulae. One asks: what is the fastest possible running time as a function of the size of the instance which a fixed program might achieve in correctly answering all of the instances of Q? One says that Q is in class P, if there is a program whose running time is bounded by a polynomial function of the number n of bits required to describe the instance I of Q on the Turing machine's tape. One says Q is in *NP* if there is an "existential" program operating on I plus a number of "guess bits" that correctly answer all instances I of Q in polynomial time. The existential program is deemed to say "yes," iff some setting of the guess bits returns a "yes" answer in poly-time. Clearly $P \subseteq NP$. It is easy to map *NP* into an apparently larger class of questions $\#P$ which ask of a given *NP* algorithm (with a fixed polynomial time cut-off), how many settings of the guess bits lead to "yes"?

The word "complete," following a class, is used to denote a problem $\bar{Q}$ within a class, which is maximally hard in the sense that any other problem in the class can be solved—again in poly-time—with an oracle giving, in a single clock cycle, solutions of $\bar{Q}$. The word "hard," following a class, denotes a problem not necessarily in the class, but to which all problems in the class reduce (again in poly-time). For example, counting the number of Boolean satisfactions is the paradigm $\#P$-complete problem.

It is a theorem (3) that evaluating the Jones polynomial at any primitive rth root of unity ζ, for $r \geq 5$, is $\#P$-hard. This ultimately employs a chain of reasoning relating the Jones polynomial to the Tutte polynomial to the chromatic polynomial to Boolean satisfiability to the operation of a Turing machine. The Jones polynomial (4) is a one-variable (t) polynomial invariant of smooth or P.L. knots in Euclidean 3-space which obeys the skein relation:

$$-tJ(\times) + t^{-1}J(\times) = (t^{1/2} - t^{-1/2})J(\rightleftharpoons) \qquad [1]$$

where ( ) means insert a knot or link diagram which is identical in the three occurrences except near one point where three indicated variations are drawn. Given a normalization $J(\text{unknot}) = 1$, Eq. **1** uniquely defines J as a "polynomial" with non-zero coefficients at finitely-many positive and negative whole powers of $t^{1/2}$ on all knots and links. The procedure for evaluation involves calculating a tree of resolutions and seems to be exponentially large in the number n of crossings in the knot diagram. This number n, or rather some small polynomial function of it, can be taken as the number of bits necessary to specify the knot, so the input size of each instance is easily quantified. Because the coefficients of J are ordinary integers,

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "*advertisement*" in accordance with 18 U.S.C. §1734 solely to indicate this fact.

Abbreviation: TQFT, topological quantum field theory.

*Bernstein, E. & Vazirani, U., "Quantum complexity theory" in Proceedings of the 25th ACM Symposium on Theory of Computing, May 16–18, 1993, San Diego, CA, pp. 11–20.

the output $J(\xi)$ is a cyclotomic integer which may be regarded as an r-vector of integers which, with little expansion of size, can be encoded as a single integer m. Interpreted in this way, the assertion that calculating $J(\xi)$ is $\#P$-hard makes sense and is a theorem.

Topological Quantum Field Theories

From a different direction (5), the Jones polynomial is connected to TQFT. This notion of a field theory capable of assigning scalar invariants to closed manifold or knots, i.e., one not depending on the background geometry, has emerged through work of Witten's (see ref. 6). Formal properties of Feynman integrals in this theory imply the skein relation and from this it is calculated that the expectation value $W_k(K)$ of an "observable" A_K associated to a Wilson loop K in $SU(2)$-Chern-Simons field theory satisfies

$$W_k(K) = J_K(\xi) \quad \text{for } k = r - 2, \qquad \textbf{[2]}$$

where W_k is formally given in terms of Feynman integrals as

$$W_k(K) = \int_{\mathcal{A}/\mathcal{G}} d\mathcal{A} e^{-2\pi i k CS\mathcal{A}} \operatorname{Tr}(\operatorname{hol}_K) \Big/ \int_{\mathcal{A}/\mathcal{G}} d\mathcal{A} e^{-2\pi i k CS\mathcal{A}}. \qquad \textbf{[3]}$$

We have written the Lagrangian as $kCS\mathcal{A}$. In full we have

$$\begin{aligned} \mathcal{L} = kCS\mathcal{A} &= \frac{k}{4\pi} \int_{M^3} \operatorname{Tr}(\mathcal{A} \wedge d\mathcal{A} + \frac{2}{3} \mathcal{A} \wedge \mathcal{A} \wedge \mathcal{A}) \\ &= \frac{k}{8\pi} \int_{M^3} \varepsilon^{ijk} \operatorname{Tr}\Big(A_i(\partial_j A_k - \partial_k A_j) \\ &\quad + \frac{2}{3} A_i [A_j, A_k] \Big). \end{aligned} \qquad \textbf{[4]}$$

Much thought has been devoted to repackaging the information in $\{W_k\}$ in terms of the perturbative Chern-Simons invariants C_ℓ:

$$\sum_{\ell=1}^{\infty} C_\ell \left(\frac{1}{k}\right)^\ell \qquad \textbf{[5]}$$

being an asymptotic expansion for W_k. In ref. 7 this expansion is written as a weighted sum over representations ρ of the exponentiation sums having the form

$$\sum_{n=1}^{\infty} a_{\ell,\rho} \left(\frac{1}{k}\right)^\ell. \qquad \textbf{[6]}$$

We have simply collected terms into a conceptually simple form at the risk of combining terms with distinct topological significance. The $a_{\ell,\rho}$ have been identified for ρ trivial $a_{\ell,\rho} = a_\ell$ (7) with Vassiliev's (8) finite-type invariants. The a_ℓ are individually computable in polynomial time in the complexity of K (9) but known computations are exponential time in ℓ. From the discussion of accuracy in the next section, even if $\{a_\ell\}$ is bounded, a_ℓ, ℓ up to poly(#), must be computed to determine $W_k(K)$ exactly, where # is the crossing-order number of the knot K. This appears to be an exponentially difficult task as a function of the crossing number. Thus it is the nonperturbative Witten invariant $W_k(K)$ which represents the computational power inherent in the physical theory.

Although TQFTs with non-Abelian geometry groups have been proposed in connection with the quantum Hall effect and anyons (10) they necessarily display physically peculiar features: (*i*) the theory is (2 + 1)-dimensional so must describe surface effects; (*ii*) the spatial Hilbert space is finite-dimensional; (*iii*) since it is topological, the theory is "static" in that the Hamiltonian $\mathcal{H}$ when derived by the standard rules, vanishes; and finally, (*iv*) the Lagrangian is topologically invariant, as the metric does not explicitly enter in Eq. **3** [although interpretation of the integral requires, after Polyakov (11), a regularization which brings in a metric quantity, writhe (K), which must be subtracted to achieve the identification with the Jones polynomial in Eq. **2**].

It is this peculiar rigidity of a TQFT which simplifies the calculation of observables to the point where it is governed by a skein relation as in **2**. This simplification and discretization has allowed computer science to evaluate the computational power of such theories. It was necessary to have, in addition to the Feynman integral "definition" of $W_k(K)$, the precise (but exponentially slow) skein theoretic method for evaluating $W_k(K)$ to discover the computational class, $\#P$-hard, of the output. A physical theory lacking a discrete closed form evaluation of observables is not as easily placed in the computational hierarchy. This is why we focus on topological theories.

Consider the "evidence" tabulated below on the "computational power" of TQFTs. The striking pattern observed in Table 1 is that the TQFTs with an Abelian gauge group yield polynomial-time invariants, whereas all the non-Abelian TQFTs yield $\#P$-hard information. Within this class of examples, the Abelian theories are free (the Lagrangian is Gaussian), whereas the non-Abelian theories contain a higher-degree (cubic) self-interaction term $\frac{2}{3} \mathcal{A} \wedge \mathcal{A} \wedge \mathcal{A}$, see Eq. **4**, in the Lagrangian. Thus our evidence leaves open the possibility that an Abelian field theory with particles, and hence cubic or higher terms, also performs a $\#P$-hard calculation. In this direction, the duality between Donaldson theory (12) and Seiberg-Witten theory (13) shows that the information present in a matterless $SU(2)$-theory can also be found in a $U(1)$-theory containing an additional (spinor) field. Thus the broadest possible interpretation of Table 1 is that any interaction term in the Lagrangian confers computational power. This could be tested by finding a combinatorial evaluation of an Abelian TQFT incorporating particles.

Complexity of Physical Systems and Accuracy of Measurement

We take the view that a physical system S (and even an idealized one such as those considered in the table) can be prepared up to some level of accuracy in a state Ψ described by input bits $B = b_1, \ldots, b_n$. A measurement (or several measurements), each assumed to take only one tick of our computational clock, produces a number(s), again to some accuracy, represented by bits $B' = b'_1, \ldots, b'_m$ of output. It is assumed that B' is a (perhaps statistically) reproducible function of B. We regard the complexity class of the function $B'(B)$ as giving a *lower bound* on the complexity of the system. If $B'(B)$ is, for example, $\#P$-hard, then adding S as an oracle to the usual (Turing) theory of computation collapses the "polynomial hierarchy" (16). If S is a physically practicable system, it would be very attractive as the core of an analog computer.

A simple analogy will clarify the concept. A transformer has a primary solenoid, which we treat as a simple closed loop $\alpha \subset \mathbb{R}^3$ and a secondary loop $\beta \subset \mathbb{R}^3$. If an alternating current is sent through α, Maxwell's equations tell us that a current will be generated in β, which is proportional to the linking-number link(α, β). This fact could serve as the core for the design of an analog computer, but not a good one. The quantity being computed by the physics, link(α, β), is directly computable from the link projection (count crossing of α over β according to sign) in linear time—certainly no longer than it would have taken to configure the link(α, β) as input. One is tempted to

Table 1. The computational complexity of Chern-Simons field theories

Source						
Year	Ref.	Base	$\mathcal{L}$	Str. group	Top. invariant	Invariant's complexity
1978	1	2 + 1	Abelian *CS*	$U(1)$	Reidemeister-Ray-Singer torsion	Determinant of a chain complex : P
1988	11	2 + 1 with Wilson loops	Abelian *CS*	$U(1)$	Linking number	P
1989	5	2 + 1 and 2 + 1 with Wilson loops	$SU(2)CS$ and $SU(N)CS$	$SU(2)$ and $SU(N)$	Witten invariant Jones poly and 2-variable Jones poly	Both Jones polynomials are $\#P$-hard to evaluate away from a thin set of exceptions. See ref. 3.
1993	14	d + 1 and $d \geq 1$	Characteristic class in $H^{d+1}(BG, R/Z)$	Any finite group G	Counts representations of π_1 base into G	P, when G is Abelian, in general appears exponential in number of generations of π_1 base.
1997	15	2 + 1	Abelian *CS* integrated over all bundles	$U(1)$	Involves Abelian *CS* times volume of representations variety T^n in an invariant metric determined by Reidemeister torsion	Although these invariants are real, to a fixed accuracy they appear to be poly-time in the base manifold's complexity.

assign the weakness of this computation to the fact that electromagnetism is an Abelian theory. In contrast, if some "$SU(2)$-current" could be driven through α to produce information about the Jones polynomial of the link(α, β), this would be much more promising.

The example (2), $W_k(K) = J_K(\xi)$, illustrates the role of finite accuracy in the interpretation of a continuous measurement. The breadth $b(J_K)$ of J_K is defined to be the difference between the highest and lowest powers of t. Both $b(J_K)$ and the number of bits in each coefficient of J_K satisfy an upper bound which is linear in $\#K$ = the crossings-number of K : $b(J_K) \leq 4\#K$ and $\log_2$(coefficient) $\leq \#K$ + const. Setting $r = b + 1$, there is a linear system which solves for the coefficients $\{c_a, 1 \leq a \leq r\}$ of J_K in terms of $\{J(\xi^a) | 1 \leq a \leq r\}$, where $\xi = e^{2\pi i/r}$. Solving for $\{c_a\}$ depends on inverting the Vandermonde matrix $(\xi^{ij}, 1 \leq i, j \leq r)$. Since the matrix is Unitary up to a scale, determinant $\det(\xi^{ij}) = i^{r(r-1)/2} \times r^{r/2}$, this process is numerically stable. An *approximate* set of "observations" $\{\tilde{J(\xi^a)}, 1 \leq a \leq r\}$ yields approximate coefficients $\{\tilde{c}_a\}$ which can be rounded to the nearest integers, which if the observations were sufficiently accurate, will be $\{c_a\}$. Substitution of ξ^a now yields the exact $\{J(\xi^a)\}$. Thus the number of reliable bits in each observation required to error correct to the *exact* values of $J(\xi^a)$ is only linear in the size of the problem $\#K$. In other contexts, such as quantum computing (5), this scaling of accuracy requirements has been considered reasonable although a better goal for accuracy of individual measurements is poly(log K) bits or even a small constant number of bits. Because $r \approx 4\#K$ observations are required to solve the linear system, a total of quadratically-many bits must be collected before all observational errors can be corrected. A superior error-correcting scheme might be based on measuring nonlinear functions of $\{c_a\}$ determined by "knot cabling" or other topological constructions. The goal is to find a polynomially-large set of constant accuracy measurements from which $\{c_a\}$ can be inferred. We remind the reader that if no limit (or cost) on accuracy is imposed in a system with single step integer multiplication and "bit output," then it is a result of ref. 17 that *NP*-complete problems can be solved in polynomial time. Realistic computational schemes must account for the accuracy of observation.

To be computationally interesting, it appears that the Lagrangian should contain terms beyond quadratic. In QED this occurs with the inclusion of particles. For example, the creation of a photon (A) through the annihilation of a positron ($\bar{\Psi}$) − electron (Ψ) pair comes from the $\bar{\Psi}A\Psi$ term inside a Lagrangian density $\bar{\Psi}(\partial_A - A)\Psi$, which is cubic in the three fields taken together. The perturbative evaluation of an expectation value in such a theory is made by summing over (a technically-divergent series indexed by) Feynman diagrams. However, the metric dependence of ∂_A makes the theory nontopolocial and more difficult to relate with decision problems. The most interesting physical candidates seem to be solid state systems describable by Lagrangians containing topological terms [refs. 10 and 18 (http://xxx.lanl.gov/abs/quant-ph/970721)].

The Relation with Quantum Computation

Quantum computing has developed as an abstract variant of computer science with roots in early results on the universality of reversible computation (19) and ideas of Feynman (20). It received wide attention with results of Shor† on applications, e.g., probable factoring in poly-time, of potential importance to cryptography. Recently, it has been shown that any problem which classically requires a search of 2^n cases can be accomplished in roughly $2^{n/2}$ steps on a quantum computer, and that this speed-up is essentially optimal.‡

Quantum computing (QC) and our proposal for "quantum field computing" (QFC) share the idea that a quantum system, exploiting superposition (in the first case, of states, and in the second case of complex weights of fields in the Lagrangian formalism), can explore an exponentially large computational tree. In quantum computing, after the exploration is completed, the report-back is a single eigenvalue of an observable which depends statistically on cacophony of voices. Some deconvolution is required to extract useful information. In QFC the $\#P$-hard information is an average, or "expectation value," rather than a particular eigenvalue, so the interpretation is direct. In the presence of accuracy limitations, many approximate-expectation values with known algebraic rela-

†Shor, P., Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, Nov. 20–22, 1994, Santa Fé, NM, pp. 124–134.

‡Grover, L., "A fast quantum mechanical algorithm for database search" in Proceedings of the 28th Annual ACM Symposium on Theory of Computing, May 22–24, 1996, Philadelphia, PA, pp. 212–219.

tions might be measured and used together to solve for the hard information.

Formally, QC occurs on a new type Turing machine which can write and read superpositions of symbols, i.e., vectors in a finite-dimensional Hilbert space $\mathcal{H}$, and where the read $\rightarrow$ write transformations dictated by the machine's internal program is always unitary. The benefit of superposition and the departure from classical probablist computation in QC derives from the creation of "entanglement of states" (e.g., the Bell state $1/\sqrt{2} \mid \uparrow > \otimes \mid \downarrow > - 1/\sqrt{2} \mid \downarrow > \otimes \mid \uparrow >$) which must be built up through successive elementary Unitary transformations (called gates) and defended against decoherence. In QFC, superposition (over all backround fields A) is postulated in the Lagrangian formulation to occur spontaneously. It is this superposition that QFC seeks to exploit.

I would like to express thanks to Peter Doyle, Dan Freed, David Meyer, Curt McMullen, and Cliff Taubes for stimulating conversations on the material presented. This work was partially supported by the University of California, San Diego, by National Science Foundation Grant DMS 9501105, and by Microsoft Research.

1. Schwarz, A. (1978) *Lett. Math. Phys.* **2,** 247–252.
2. Bennet, C., DiVincenzo, D., Smolin, J. & Wootters, W. (1996) *Phys. Rev. A* **54,** 3824–3851.
3. Jaeger, F., Vertigen, D. & Welsh, D. (1990) *Math. Proc. Cambridge Philos. Soc.* **108,** 35–53.
4. Jones, V. (1985) *Bull. Am. Math. Soc.* **12,** 103–111.
5. Witten, E. (1989) *Commun. Math. Phys.* **121,** 351–391.
6. Atiyah, M. (1990) *The Geometry and Physics of Knots* (Cambridge Univ. Press, Cambridge, U.K.).
7. Bar-Natan, D. & Witten, E. (1991) *Commun. Math. Phys.* **141,** 423–440.
8. Vassiliev, V. (1992) *Complements of Discriminants of Smooth Maps: Topology and Applications*, translated from the Russian by B. Goldfarb, *Translations of Mathematical Monographs* (Am. Math. Soc., Providence, RI), Vol. 98.
9. Bar-Natan, D. (1995) *Math. Res. Lett.* **2,** 239–246.
10. Wilczek, F. (1990) *Fractional Statistics and Anyon Superconductivity* (World Scientific, Singapore).
11. Polyakov, A. M. (1988) *Mod. Phys. Lett. A* **3,** 325–328.
12. Donaldson, S. & Kronheimer, P. (1990) *The Geometry of Four-Manifolds*, Oxford Mathematical Monographs, Oxford Science Publications (The Clarendon Press, Oxford Univ. Press, New York).
13. Seiberg, N. & Witten, E. (1994) *Nucl. Phys. B* **426,** 19–52.
14. Freed, D. & Quinn, F. (1993) *Commun. Math. Phys.* **156,** 435–472.
15. Manoliu, M. (1998) *J. Math. Phys.*, in press.
16. Toda, S. (1989) *Proceedings of the 30th Annual Symposium on the Foundations of Computer Science* (IEEE Comput. Soc. Press, Los Alamitos, CA), pp. 514–519.
17. Schönhage, A. (1974) *Proceedings of the 6th ICALP, Lecture Notes in Computer Science* (Springer, New York), Vol. 71, pp. 520–529.
18. Kitaev, A. Y. (1997) *Fault-tolerant quantum computation by anyons*, quant-ph/9707021, 9 July 1997, preprint.
19. Bennett, C. (1973) *IBM J. Res. Dev.* **17,** 525–532.
20. Feynman, R. (1982) *Int. J. Theor. Phys.* **21,** 467–468.