PHYSICAL REVIEW A **82**, 040302(R) (2010)

Estimating Turaev-Viro three-manifold invariants is universal for quantum computation

Gorjan Alagic,[1] Stephen P. Jordan,[2] Robert König,[2] and Ben W. Reichardt[1]
[1] *Institute for Quantum Computing, University of Waterloo, Waterloo N2L 3G1, Ontario, Canada*
[2] *Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA*

(Received 5 March 2010; revised manuscript received 10 August 2010; published 8 October 2010)

The Turaev-Viro invariants are scalar topological invariants of compact, orientable 3-manifolds. We give a quantum algorithm for additively approximating Turaev-Viro invariants of a manifold presented by a Heegaard splitting. The algorithm is motivated by the relationship between topological quantum computers and (2 + 1)-dimensional topological quantum field theories. Its accuracy is shown to be nontrivial, as the same algorithm, after efficient classical preprocessing, can solve any problem efficiently decidable by a quantum computer. Thus approximating certain Turaev-Viro invariants of manifolds presented by Heegaard splittings is a universal problem for quantum computation. This establishes a relation between the task of distinguishing nonhomeomorphic 3-manifolds and the power of a general quantum computer.

DOI: 10.1103/PhysRevA.82.040302 PACS number(s): 03.67.Ac, 02.40.Sf, 03.65.Vf, 05.30.Pr

The topological quantum computer is among the most striking examples of known relationships between topology and physics. Such a computer encodes quantum information in a quantum medium on a two-dimensional (2D) surface, whose topology determines the ground space degeneracy. Surface deformations implement encoded operations, and can apply arbitrary quantum circuits. It is natural to try to identify the topological origin of this computational power.

One answer is that the power stems from the underlying $(2+1)$D topological quantum field theory (TQFT) [1]. The TQFT assigns a Hilbert space $\mathcal{H}_\Sigma$ to a 2D surface Σ, and a unitary map $U(f):\mathcal{H}_\Sigma \to \mathcal{H}_{\Sigma'}$ to every diffeomorphism $f:\Sigma\to\Sigma'$, subject to a number of axioms [2]. However, this answer is not fully satisfactory; the definition of a TQFT is involved, and uses mathematics that appears in similar form in the theory of quantum computation. A second answer, arising in [3–6], is that quantum computers' power comes from their ability to approximate the evaluation, at certain points, of the Jones polynomial of the plat closure of a braid.

Here we give an alternative topological description of the power of quantum computers, in terms of the Turaev-Viro 3-manifold invariants. Restricting TQFTs to closed manifolds results in scalar invariants. We show that approximating certain such invariants is equivalent to performing general quantum computations. That is, we give an efficient quantum algorithm for additively approximating Turaev-Viro invariants, and conversely we show that for any problem decidable in bounded-error, quantum polynomial time (BQP), there is an efficient classical reduction to the Turaev-Viro invariant approximation problem. The classical procedure outputs the description of a 3-manifold whose certain Turaev-Viro invariant is either large or small depending on whether the original BQP algorithm outputs 1 or 0.

Turaev and Viro [7] defined a family of invariants for compact, orientable 3-manifolds. Each invariant, for $k\in\mathbb{N}$, is specified by algebraic data derived from the quantum group $SO(3)_k$. These data include $\lfloor k/2\rfloor+1$ inequivalent irreducible representations, commonly referred to as particles or topological charges. Particle i has quantum dimension $d_i>0$. Furthermore, a certain six-index tensor F^{ijm}_{kln}, known as the quantum $6j$ symbol, encodes the associativity for triples of representations.

Any compact 3-manifold M is homeomorphic to a finite collection of tetrahedra glued along their faces [8]. Beginning with such a triangulation, assign F to each tetrahedron and a d, interpreted as a gluing tensor, to every edge. The invariant $\mathrm{TV}_k(M)$ is the contraction of this tensor network, which can be expanded as

$$\mathrm{TV}_k(M)=\mathcal{D}^{-2|V|}\sum_{\text{labelings}}\prod_{\text{edges}}d_h\prod_{\text{tetrahedra}}\frac{F^{ijm}_{kln}}{\sqrt{d_m d_n}}. \qquad (1)$$

Here, the sum is over edge labelings of the triangulation by particles of $SO(3)_k$. The index h is the particle associated to an edge, while i,j,k,l,m,n are the particles associated to the six edges involved in a tetrahedron, ordered appropriately [7]. The prefactor depends on the number $|V|$ of vertices in the triangulation and the total quantum dimension $\mathcal{D}=\sqrt{\sum_i d_i^2}$ of $SO(3)_k$. The topological invariance of $\mathrm{TV}_k(M)$ follows from the fact that any two triangulations of M can be related by a finite sequence of local moves [9] which leave (1) invariant.

Instead of by a triangulation, we will assume that the manifold M is presented by a "Heegaard splitting." Consider two genus-g handlebodies (e.g., the solid torus for $g=1$). They can be glued together, to give a 3-manifold, using a self-homeomorphism of the genus-g surface. The set of orientation-preserving self-homeomorphisms modulo those isotopic to the identity form the mapping class group $\mathrm{MCG}(g)$ of the surface. It is an infinite group generated by the $3g-1$ Dehn twists illustrated in Fig. 1. A Heegaard splitting thus consists of a natural number g and an element $x\in\mathrm{MCG}(g)$, defining a manifold $M(g,x)$. The element x is specified as a word in the generators, of length $|x|$. Every compact, orientable 3-manifold has a Heegaard splitting.[1] Our result is as follows:

[1]This representation is unique up to (i) a "stabilization" move $(g,x)\cong(g+1,\tilde{x})$ obtained by taking the connected sum with a 3-sphere and using a standard genus-1 Heegaard splitting of the latter, and (ii) multiplications $x\cong yxz$ by elements y,z of the subgroup $\mathrm{MCG}^+(g)\subset\mathrm{MCG}(g)$ of self-homeomorphisms of the genus-g surface which extend to self-homeomorphisms of the handlebody [11–13].

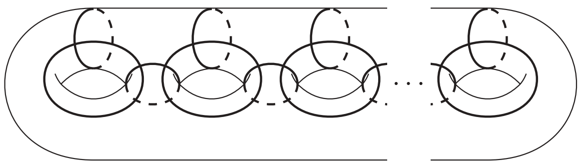


FIG. 1. A Dehn twist is a 2π rotation about a closed curve. The Dehn twists about the $3g-1$ curves shown above generate the full mapping class group of the genus-g surface [10].

Theorem 1. For any fixed $k \geqslant 3$, there is a quantum algorithm that, given a Heegaard splitting $M(g,x)$ and constants $\delta,\epsilon > 0$, runs in time poly$(g,|x|,\log 1/\delta, 1/\epsilon)$ and, except with probability at most δ, outputs an estimate of $_k\big(M(g,x)\big)$ to within $\pm\mathcal{D}^{2(g-1)}\epsilon$.

Conversely, for $k \geqslant 3$ such that $k+2$ is prime, it is BQP-hard to decide whether $\mathcal{D}^{2(1-g)}\,\mathrm{TV}_k\big(M(g,x)\big)$ is greater than $2/3$ or less than $1/3$. More precisely, given any quantum circuit Υ of T two-qubit gates acting on n qubits $|0^n\rangle$, with output either 0 or 1, one can classically find in polynomial time a word x in the standard Dehn-twist generators of MCG(g), with $g = n+1$ and $|x| = \mathrm{poly}(T)$, such that

$$\big|\Pr[\Upsilon \text{ outputs } 1] - \mathcal{D}^{2(1-g)}\,\mathrm{TV}_k\big(M(g,x)\big)\big| < 1/6. \tag{2}$$

In previous work, Garnerone *et al.* [14] have given a quantum algorithm for estimating the Turaev-Viro invariants for a manifold presented by Dehn surgery, but the hardness of their estimation remains open. In an unpublished article, Bravyi and Kitaev [15] have given an efficient classical algorithm to approximate the Turaev-Viro invariant for the $SU(2)_2$ group. They also prove that estimating the $SU(2)_2$ Turaev-Viro invariant of a 3-manifold *with boundary*, presented using Morse functions, is BQP-complete. Allowing a boundary is a crucial difference, as it allows feeding in certain "magic" states, as labelings of the boundary components, to obtain universality. Our approach using Heegaard splittings and $SO(3)_k$ is complementary and provides a concise formulation of a BQP-complete problem for closed manifolds, without requiring magic states.[2]

As in this previous work, our proof of Theorem 1 begins not with Eq. (1), but with an alternative formulation of the Turaev-Viro invariant in terms of the Witten-Reshetikhin-Turaev (WRT) invariant [17,18]:

$$\mathrm{TV}_k(M) = |\mathrm{WRT}_k(M)|^2. \tag{3}$$

This was shown by Turaev [19] and Walker [2] (see too [20,21]). The WRT invariant itself has multiple equivalent definitions. Unlike the previous work that used a definition based on a Dehn-surgery presentation of M, we will use the Crane-Kohno-Kontsevich formulation [22–24] of the WRT invariant. This is given by

$$\mathrm{WRT}_k\big(M(g,x)\big) = \mathcal{D}^{g-1}\langle v_{k,g}|\rho_{k,g}(x)|v_{k,g}\rangle. \tag{4}$$

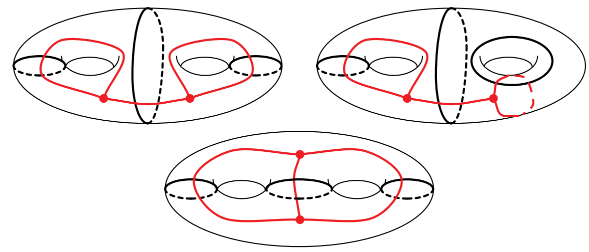


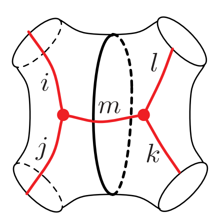
FIG. 2. (Color online) Three examples of decompositions of the genus-2 surface Σ_2 into three-punctured spheres. Trivalent adjacency graphs of the punctured spheres are shown in red.

Here $|v_{k,g}\rangle$ is a certain unit-normalized vector in a Hilbert space $\mathcal{H}_{k,g}$, and $\rho_{k,g} : \mathrm{MCG}(g) \to \mathrm{GL}(\mathcal{H}_{k,g})$ is a certain projective representation.[3] Equivalence of the definitions is shown in [25]; see also [26], Sec. 2.4.

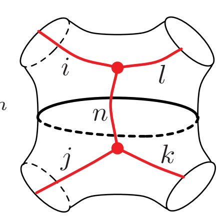
We now briefly describe the objects $\mathcal{H}_{k,g}$, $\rho_{k,g}$ and $|v_{k,g}\rangle$. Further details are in [22–24,27]. First, fixing a particular k, the quantum group $SO(3)_k$ has a distinguished trivial particle 0 and specifies fusion rules, quantum dimensions d_i, the quantum $6j$ symbol F^{ijm}_{kln}, and the R matrix R^{jk}_i. These tensors satisfy algebraic identities discussed in, e.g., [27,28].

Let $g \in \mathbb{N}$, $g \geqslant 2$. The space $\mathcal{H}_{k,g}$ can be defined by specifying an orthonormal basis. Decompose the genus-g surface Σ_g into three-punctured spheres (or "pants") by cutting along $3g-3$ noncontractible curves, as illustrated in Fig. 2. Dual to such a decomposition is a trivalent graph Γ. A basis vector $|\ell\rangle_\Gamma$ is a fusion-consistent labeling of the edges of Γ by particles of $SO(3)_k$. Fusion consistency is defined by the fusion rules, i.e., a set of triples of labels that are allowed to meet at every vertex. Define the states $\mathcal{B}_\Gamma := \{|\ell\rangle_\Gamma\}_\ell$ to be orthonormal, and their span to be $\mathcal{H}_{k,g}$. Note that this definition gives a natural encoding of $\mathcal{H}_{k,g}$ into qudits, with one qudit to store the label of each edge of Γ.

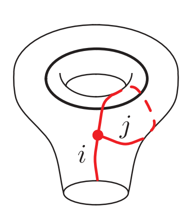
The above definition depends on Γ, but alternative pants decompositions simply represent different bases $\mathcal{B}_\Gamma$ for the same Hilbert space. To convert between all possible pants decompositions of Σ_g, two identities are needed:



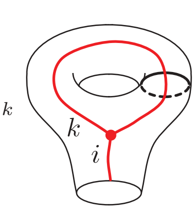
$$= \sum_n F^{ijm}_{kln}$$



, (5)



$$= \sum_k S^i_{jk}$$



. (6)

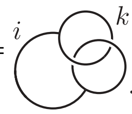
[2]Furthermore, a quantum algorithm of Arad and Landau [16] can efficiently approximate the Turaev-Viro invariants for a manifold presented by a triangulation, but the naive algorithm's approximation factor will be trivial.

[3]Invariance follows essentially from the fact that $|v_{k,g}\rangle$ is invariant under the action of $\mathrm{MCG}^+(g)$. As the representation is projective, WRT_k is a 3-manifold invariant only up to a multiple of $e^{2\pi i c/24}$ where c is the so-called central charge.

The F move, in Eq. (5), relates bases that differ by a "flip" of a cut between two three-punctured spheres. In the qudit encoding, it is a five-qudit unitary, with four control qudits. The S move, in Eq. (6), applies when two boundaries of a single three-punctured sphere are connected. It is a two-qudit unitary, with one control qudit.

As discussed in [2], S^i_{jk} can be computed from the quantum dimensions, the $6j$ symbols, and the R matrix by the identity

$$\mathcal{D}S^i_{jk} = \mathcal{D}S^i_{jk} \sum_l F^{ikk}_{ljj} \frac{d_l}{\sqrt{d_i}} R^{kj}_l R^{jk}_l =$$



,

where the sum is over all l such that (j,k,l) is fusion consistent. (The last expression uses ribbon graph notation. It reduces to the Hopf link when i is the trivial particle, giving the usual S matrix which diagonalizes the fusion rules according to the Verlinde formula.)

The action $\rho_{k,g}$ of MCG(g) on $\mathcal{H}_{k,g}$ can now be specified by the action of the Dehn-twist generators on basis vectors. For a Dehn twist about a curve σ, apply a sequence of F and S moves to change into a basis $\mathcal{B}_\Gamma$, i.e., a pants decomposition of Σ_g, in which σ divides two three-punctured spheres. In such a basis, the Dehn twist acts diagonally: if the edge of Γ crossing σ has label i, the twist applies a phase of R^{ii}_0 (or its conjugate, depending on the direction of the twist).

To complete the definition of WRT$_k(M(g,x))$ from Eq. (4), it remains to define the state $|v_{k,g}\rangle$. Pants-decompose Σ_g such that every cut through a handle is meridional, as illustrated on the right-hand side of Eq. (6). The dual graph Γ to one such collection of cuts is illustrated in Fig. 3(a). Then $|v_{k,g}\rangle$ is the state in which every edge of Γ is labeled by the trivial particle 0.

Theorem 1 will follow from locality and density properties of the representations $\rho_{k,g}$. The importance of such properties of mapping class group representations has been recognized earlier in the context of topological quantum computation, where the focus is most commonly on punctured spheres and quantum circuits are translated into closed links (arising from braids) [1]. In contrast, we deal with genus-g surfaces, translating circuits into closed 3-manifolds and relating them to invariants.

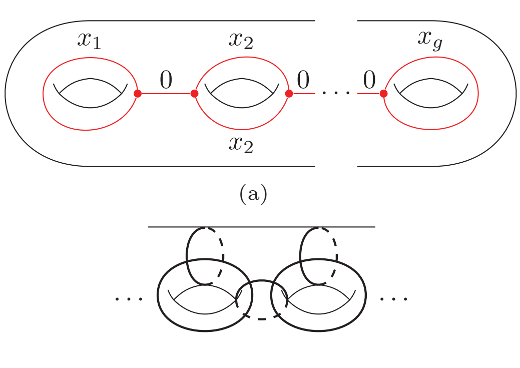


FIG. 3. (Color online) (a) A g-qubit state $|z\rangle$, $z \in \{0,1\}^g$, can be encoded into $\mathcal{H}_{k,g}$ for the genus-g handlebody. (b) Any two-qubit gate can be approximated within the codespace using the Dehn twists involving the two corresponding handles.

Let us now prove Theorem 1. The Turaev-Viro and WRT invariants for $M(g,x)$ can be approximated essentially by implementing $\rho_{k,g}(x)$. The algorithm maintains a classical register storing the graph Γ, together with a quantum register containing the current state in $\mathcal{H}_{k,g}$ in the basis $\mathcal{B}_\Gamma$. The algorithm uses an N-dimensional qudit for each edge of Γ, where $N = \lfloor k/2 \rfloor + 1$ is the number of particle types in SO$(3)_k$. The action $\rho_{k,g}(x_j)$ of the jth Dehn twist can be applied by using a sequence of F and S moves, i.e., certain local unitaries, to change to a basis in which x_j acts diagonally. Since x_j is one of the generators from Fig. 1, starting with the graph Γ of Fig. 3(a) (for which every edge is labeled 0 in $|v_{k,g}\rangle$) at most one F and one S move are needed. An estimate to within ϵ of the desired matrix element $\langle v_{k,g}|\rho_{k,g}(x)|v_{k,g}\rangle$ can be given, except with probability δ, using $O\big(\log(1/\delta)/\epsilon^2\big)$ Hadamard tests, as in [3].

To prove BQP-hardness we reduce from the BQP-complete problem of deciding whether $|\langle 0^g|\Upsilon|0^g\rangle|^2$ is larger than 5/6 or less than 1/6, given the g-qubit quantum circuit Υ [3]. Fix $k \geqslant 3$ such that $k+2$ is prime. Given Υ consisting of T two-qubit gates, our aim is to construct efficiently the Heegaard splitting (g,x) of a manifold $M = M(g,x)$ such that $\mathcal{D}^{2(1-g)}\text{TV}_k(M)$ approximates $|\langle 0^g|\Upsilon|0^g\rangle|^2$. As illustrated in Fig. 3(a), we use one handle of a genus-g handlebody to encode each qubit. Such a labeling is fusion consistent, and the encoding of the initial state $|0^g\rangle$ is exactly $|v_{k,g}\rangle \in \mathcal{H}_{k,g}$. As shown in [29,30], by our choice of k the representation $\rho_{k,g}$ has a dense image, up to phases, in the group of unitary operators on $\mathcal{H}_{k,g}$ for $g \geqslant 2$.

By the density for $g = 2$ and the Solovay-Kitaev theorem [31], it follows that any two-qubit gate can be approximated in the codespace to precision $1/(6T)$ by applying a $(\log T)^c$-long sequence of the five Dehn twists shown in Fig. 3(b) for some constant c. Thus we obtain a polynomial-length word $x = x_1 \cdots x_{T(\log T)^c}$ in the Dehn-twist generators whose action approximates Υ on the codespace. Then $\langle v_{k,g}|\rho_{k,g}\big(M(g,x)\big)|v_{k,g}\rangle$ approximates $\langle 0^g|\Upsilon|0^g\rangle$.

This completes the proof. We remark that our results generalize as follows. The topological invariance of TV$_k$ follows from certain properties of the category of irreducible representations of SO$(3)_k$. Barrett and Westbury [32] showed that more generally, any spherical category gives rise to a 3-manifold invariant.[4] Similarly, our algorithm also applies to any multiplicity-free unitary modular tensor category. The hardness result requires density and thus applies also to, e.g., SU$(2)_k$ for $k \geqslant 3$ and $k+2$ prime [29,30].

The additive approximation error in Theorem 1 is exponential in g. Complexity-theoretic reasons make it unlikely that a multiplicative or otherwise presentation-independent error can be efficiently computed [33].

This work demonstrates how quantum physics, in the form of TQFTs, can inspire new quantum algorithms for problems based on topology and tensor networks. The approach taken here realizes in a sense the traditional vision of quantum computers as universal simulators for physical systems, but

[4]In [27], Eq. (3) is discussed in a more general category-theoretic setting.

with a different outcome: it provides a purely mathematical problem whose difficulty exactly captures the power of a quantum computer.

S.J. acknowledges support from the Sherman Fairchild Foundation and NSF Grant No. PHY-0803371. R.K. acknowledges support by the Swiss National Science Foundation (SNF) under Grant No. PA00P2-126220. B.R. and G.A. acknowledge support from NSERC and ARO. Some of this research was conducted at the Kavli Institute for Theoretical Physics, supported by NSF Grant No. PHY05-51164.

[1] M. H. Freedman, A. Y. Kitaev, and Z. Wang, Commun. Math. Phys. **227**, 587 (2002).
[2] K. Walker, [http://canyon23.net/math/].
[3] D. Aharonov, V. Jones, and Z. Landau, in *Proceedings of the 38th ACM Symposium on the Theory of Computing (STOC), 2006* (ACM, New York, 2006), pp. 427–436.
[4] D. Aharonov, I. Arad, The BQP-hardness of approximating the Jones Polynomial, e-print arXiv:quant-ph/0605181.
[5] S. Garnerone, A. Marzuoli, and M. Rasetti, Int. J. Quantum. Inform. **6**, 773 (2008).
[6] P. Wocjan and J. Yard, Quantum Inf. Comput. **8**, 147 (2008).
[7] V. G. Turaev and O. Y. Viro, Topology **31**, 865 (1992).
[8] E. E. Moise, Ann. Math. (2) **56**, 96 (1952).
[9] U. Pachner, Eur. J. Comb. **12**, 129 (1991).
[10] W. B. R. Lickorish, Proc. Cambridge Philos. Soc. **60**, 769 (1964); **62**, 679 (1966).
[11] K. Reidemeister, Zur dreidimensionalen Topologie, Abh. Math. Sem. (University of Hamburg, 1933).
[12] J. Singer, Trans. Am. Math. Soc. **35**, 88 (1933).
[13] L. Funar, Commun. Math. Phys. **171**, 405 (1995).
[14] S. Garnerone, A. Marzuoli, and M. Rasetti, Adv. Theor. Math. Phys. **13**, 1601 (2009).
[15] S. B. Bravyi and A. Y. Kitaev, Quantum invariants of 3-manifolds and quantum computation (unpublished).
[16] I. Arad and Z. Landau, SIAM J. Comput. **39**, 3089 (2010).
[17] E. Witten, Commun. Math. Phys. **121**, 351 (1989).
[18] N. Reshetikhin and V. G. Turaev, Invent. Math. **103**, 547 (1991).
[19] V. Turaev, J. Differential Geom. **36**, 35 (1992).
[20] V. G. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, de Gruyter Studies in Mathematics Vol. 18 (de Gruyter, New York, 1994).
[21] J. D. Roberts, Topology **34**, 771 (1995).
[22] L. Crane, Commun. Math. Phys. **135**, 615 (1991).
[23] T. Kohno, Topology **31**, 203 (1992).
[24] M. Kontsevich, Centre de Physique Marseille Report No. CPT-88/p2189, 1988.
[25] S. Piunikhin, J. Knot Theor. Ramif. **2**, 65 (1993).
[26] T. Kohno, *Conformal Field Theory and Topology*, Translations of Mathematical Monographs Vol. 210 (American Mathematical Society, Providence, RI, 2002), Chap. 2.4.
[27] R. Koenig, G. Kuperberg, and B. W. Reichardt, Ann. Phys. **325**, 2707 (2010).
[28] J. Preskill [http://theory.caltech.edu/people/preskill/ph229/].
[29] M. H. Freedman, M. J. Larsen, and Z. Wang, Commun. Math. Phys. **228**, 177 (2002).
[30] M. Larsen and Z. Wang, Commun. Math. Phys. **260**, 641 (2005).
[31] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[32] J. W. Barrett and B. W. Westbury, Trans. Am. Math. Soc. **348**, 3997 (1996).
[33] G. Kuperberg, e-print arXiv:0908.0512v1.