COMPLEXITY CLASSES AS MATHEMATICAL AXIOMS II

SHAWN X. CUI\textsuperscript{1}, MICHAEL H. FREEDMAN\textsuperscript{2}, AND ZHENGHAN WANG\textsuperscript{1,2}

Abstract. The second author previously discussed how classical complexity separation conjectures, we call them “axioms”, have implications in three manifold topology: polynomial length stings of operations which preserve certain Jones polynomial evaluations cannot produce exponential simplifications of link diagrams. In this paper, we continue this theme, exploring now more subtle separation axioms for quantum complexity classes. Surprisingly, we now find that similar strings are unable to effect even linear simplifications of the diagrams.

1. Introduction

Evaluations of the Jones polynomial at $\omega_r = e^{\frac{2\pi i}{r}}$ is known to be $\#P$ hard for $r \geq 5$ but $\neq 6$ \cite{16, 17}. Following \cite{3}, we consider strings of Dehn surgeries designed to be easily (polynomially) describable and not to alter the $\omega_r$-Jones evaluation. In the earlier paper \cite{3}, it was shown that polynomial length strings of such Dehn surgeries cannot effect an exponential simplification of the general link diagram without contradicting standard conjectures—they were called “axioms”—regarding the separation of classical complexity classes. In particular, it was shown that “$\text{PP} \not\subset \text{NP}$” would be contradicted by exponential simplification of diagrams. In this paper, we continue this theme, exploring now more subtle separation axioms for quantum complexity classes. Moreover, we generalize the Dehn surgeries in \cite{3} so that we have more flexibility to change the link while preserving its Jones evaluations. Surprisingly, we now find that even the generalized strings are unable to effect even linear simplifications of the diagrams without contradicting the separation “axiom” that BQP is not in $\text{NP} \ast DQC1$.

Throughout this paper, we use the following notation: $r$ is an integer $\geq 5$ but $\neq 6$, and $d = 2\cos(\frac{\pi}{r})$. For a braid $\sigma \in B_{2n}$, $\hat{\sigma}^{\text{plat}}$ is the plat closure. For $\sigma \in B_{n}$, $\hat{\sigma}^{\text{tr}}$ is the trace closure. $J(\hat{\sigma}^{\text{plat}}; r)$ and $J(\hat{\sigma}^{\text{tr}}; r)$ are the Jones polynomial at the $r$-th root of unity $\omega_r$ of the plat closure.

Key words and phrases. Complexity class, link diagram, Jones polynomial.

S.-X. C and Z.W. are partially supported by NSF DMS 1108736.
and trace closure of $\sigma$, respectively. Finally, $p$ and $q$ are always integral polynomials of two variables.

The rest of the paper is organized as follows. In Section 2.1 we define an equivalence relation on links and a distance between two equivalent link diagrams. Section 2.2 consists of background materials on approximating the Jones polynomial at the root of unity $\omega_r$. In Section 2.3 we introduce three “axioms” regarding the separation of complexity classes. Finally in Section 3 we obtain three theorems, each of which follows from one of the axioms in Section 2.3.

2. Surgeries and Axioms

2.1. An equivalence relation and a distance. First we introduce an equivalence relation on links which generalizes the relation $\sim_r$ in [3]. Links and link diagrams in this paper are oriented and framed.

For a link diagram $D$ in the $x$-$z$ plane with the blackboard framing, we define its girth $g(D)$ to be the maximum over all $z_0$ of the cardinality of the set $D \cap \{z = z_0\}$, and define its complexity $c(D)$ to be the number of crossings of $D$. Intuitively, $g(D)$ measures how wide $D$ spreads along the $x$-axis direction, while $c(D)$ measures the “area” of the diagram. Note that the definition of $c(D)$ here is different from that in [3] since we will not deal with the maxima and minima of a diagram. For a link $L$, we define its girth $g(L) = \min\{g(D) \mid D \text{ is a diagram of } L\}$. The complexity $c(L)$ is defined similarly, i.e., $c(L) = \min\{c(D) \mid D \text{ is a diagram of } L\}$.

Given a link $L$ in $S^3$, recall in [3] that the $\pm \frac{1}{4r}$-Dehn surgery on $L$ is defined as follows. Consider $L \cup U$, where $U$ is an unknot disjoint from $L$, and performing a $\pm \frac{1}{4r}$-Dehn surgery on $U$ changes $L$ into a new link $L'$, which has the same $\omega_r$-Jones evaluation as $L$. For example, if $U$ bounds a standard disk and this disk meets $L$ transversally in $n$ points, then the surgery will introduce $4rn(n-1)$ crossings to $L$.

Let $\Gamma(4r)$ be the principal congruence subgroup of level $4r$ of $SL(2, \mathbb{Z})$, i.e., the kernel of the group homomorphism $SL(2, \mathbb{Z}) \rightarrow SL(2, \mathbb{Z}/4r\mathbb{Z})$ sending a matrix $A$ to $A \pmod{4r}$ entry-wise.

Now we generalize the $\pm \frac{1}{4r}$-Dehn surgery process. Consider a pair $(M, L)$, where $M$ is an oriented closed 3-manifold and $L$ is an oriented framed link in $M$. For any knot $K$ disjoint from $L$ in $M$, performing a Dehn surgery of $M$ along $K$ via a map $\phi \in \Gamma(4r)$ results in a new closed 3-manifold denoted by $M_{K, \phi}$. Passing from $(M, L)$ to $(M_{K, \phi}, L)$ is what we call a $\Gamma_r$-Dehn surgery on $(M, L)$; it generates an equivalence relation on pairs $(M, L)$ similar to the “congruence” studied by Lackenby [9] and Gilmer [5].
Given a link $L$ in $S^3$. A sequence of $\Gamma_r$-Dehn surgeries leads to a pair $(M, L)$ of a 3-manifold $M$ with a link $L$ inside, where $M$ may not be $S^3$. Since we are only interested here in links in $S^3$, we want the manifold $M$ to be diffeomorphic to $S^3$. If this is the case, we need to construct a diffeomorphism from $M$ to $S^3$ which transforms $L$ to a new link $L'$ in $S^3$. However, it is not presently known if there is an efficient (polynomial time) algorithm for recognizing the 3-sphere. But by [13], verifying whether a given closed 3-manifold is $S^3$ is a problem in $NP$. So there is a polynomial size certificate to verify if a manifold is diffeomorphic to $S^3$. Moreover, by [13], one may actually construct such a diffeomorphism if the certification gives “yes” output. Let us refer to this process as $S^3$ recognition.

**Definition 1.** Two oriented framed links $L$ and $L'$ are called $r$-equivalent, which is denoted by $L \sim_r L'$, if there is a sequence of operations consisting of $\Gamma_r$-Dehn surgeries and $S^3$ recognitions to pass from the pair $(S^3, L)$ to $(S^3, L')$. Two oriented framed link diagrams $D$ and $D'$ are $r$-equivalent if the links that they represent are $r$-equivalent.

Next we want to define a distance between two $r$-equivalent diagrams $D$ and $D'$. Roughly speaking, the distance is the minimal length of the sequence of operations consisting of Reidemeister moves, $\Gamma_r$-Dehn surgeries, and $S^3$ recognitions. However, the knots $K_1, \cdots, K_n$ and the regluing matrices $F_1, \cdots, F_n$ in $\Gamma(4r)$ along which we do the surgery should be efficiently describable, i.e. they should not be too complicated. Moreover, the complexity of $S^3$ recognition process would depend on the complexity of the Dehn surgery description. Considering these factors, we will assign a weighted distance to the transition from $D$, a diagram for $(S^3, L)$, to $D'$ for $(S^3, L')$. To do so, we use a larger, intermediate, diagram, $\tilde{D}'(S^3, L')$, a literal $\Gamma_r$-Dehn surgery diagram for $(S^3, L')$, consisting of $L$ and the components $K_1, \cdots, K_n$ labeled by $F_1, \cdots, F_n$, which designate the $\Gamma_r$-Dehn surgeries.

**Definition 2.** For two $r$-equivalent diagrams $D$ and $D'$, the $r$-distance $dist_r(D, D')$ is the minimum of $c + b + \gamma$, where $c$ is the total number of crossings (of all types) in $\tilde{D}'(S^3, L')$, $b$ is the number of bits needed to write the integral entries of matrices $\{F_1, \cdots, F_n\}$, and $\gamma$ is the number of Reidemeister moves required to take the image of $L$ in the surgered manifold, after sphere recognition has been applied, and transform it to $L'$. The minimum is taken over all possible $\Gamma_r$-Dehn surgery diagrams and all subsequent sequences of Reidemeister moves.

**Remark 1.** The explicit form of $dist_r$ is not relevant. What is important is that the number of computational steps to pass from $D$ to $D'$
is not larger than a polynomial in \( \text{dist}_r(D, D') \). The number of computational steps of each \( \Gamma_r \)-Dehn surgery and each Reidemeister move is clearly bounded by a polynomial in the weights they contribute to \( \text{dist}_r(D, D') \). After the \( \Gamma_r \)-Dehn surgeries, one can construct a triangulation of the resulting manifold. And the number of simplices in the triangulation is less than \( \text{poly}(b+c) \). So the number of computational steps of \( S^3 \) recognition is also a polynomial in \( b+c \), hence a polynomial in \( \text{dist}_r(D, D') \).

It is straightforward to pass in polynomial time between any of the common methods for describing a 3-manifold. For the case here, one imbeds the link diagram in an adequately fine triangulation of \( S^3 \) and then extends this restricted to the link complement to a triangulation of the solid tori to glue in. Notice that “how fine” is fine enough depends not only on the links involved by the regluing matrices.

The following lemma says that the Dehn surgery preserves the absolute value of the Jones polynomial at the \( r \)-th root of unity \( \omega_r \).

**Lemma 1.** [3] If \( D \sim_r D' \), then \( |J(D; r)| = |J(D'; r)| \).

**Proof** This lemma was from [3]. Here we prove it in the more general case. The connection between \( \omega_r \)-Jones evaluation and the Dehn surgery is the \( SU(2) \)-Reshetikhin-Turaev topological quantum field theory (TQFT) at level \( k = r - 2 \), which we call \( SU(2)_k \)-TQFT and denote by \((V_k, Z_k)\). Let \( L \) be the link represented by \( D \). By [15], \( J(L, r) = Z_k(S^3, L) \), the partition function of \((S^3, L)\) in the \( SU(2)_k \)-TQFT.

Now we prove that the Dehn surgery we defined preserves the partition function of \((M, L)\) up to a phase, where \( M \) is an oriented closed 3-manifold. Let \( K \) be the knot along which we do the surgery and let \( T \) be the torus which bounds a solid torus neighborhood \( N \) of \( K \). Then \( V_k(T) \cong \mathbb{C}^{k+1} \), where \( V_k \) is the \( SU(2)_k \)-modular functor. Let \( \phi \in \Gamma(4r) \) be the gluing map. Then we have the formula \( Z_k(M_{K, \phi}, L) = \langle Z_k(M \setminus N, L) | V_k(\phi)(Z_k(N)) \rangle \). By [11], \( \Gamma(4r) \) is contained in the kernel of the (projective) modular representation corresponding to \( SU(2)_k \)-TQFT. Thus \( V_k(\phi) \) acts as identity up to a phase. So \( |Z_k(M_{K, \phi}, L)| = |\langle Z_k(M \setminus N, L) | Z_k(N) \rangle| = |Z_k(M, L)| \).

The diffeomorphism from a manifold \( M \) to \( S^3 \) preserves the partition function up to a phase. So we have \( |Z_k(S^3, L)| = |Z_k(S^3, L')| \), which implies \( |J(L, r)| = |J(L', r)| \). \qed

2.2. **Approximating the Jones polynomial.** The following theorem can be found in [4, 10, 19, 11, 20, 8], which says approximating the
Jones polynomial of the plat closure of a braid at the $r$-th root of unity $\omega_r$ is BQP-complete for $r \geq 5$ but $\neq 6$.

**Theorem 1.** [4, 10, 19, 1, 20, 8] There is an efficient classical algorithm which, given a braid $\sigma \in B_{2n}$ of length $m$ and an error threshold $\varepsilon > 0$ as input, outputs a description of a quantum circuit $U_{\sigma, \varepsilon}$ of size $\text{poly}(n, m, \frac{1}{\varepsilon})$. This quantum circuit computes a random variable $0 \leq Z(\sigma) \leq 1$, such that

$$\Pr\left\{ \left| \frac{|J(\hat{\sigma}_{\text{plat}}; r)|}{d^n} - Z(\sigma) \right| < \varepsilon \right\} > \frac{3}{4}.$$ 

Moreover, the problem of approximating $\frac{|J(\hat{\sigma}_{\text{plat}}; r)|}{d^n}$ for a braid $\sigma \in B_{2n}$ is BQP-complete.

In [14], the authors showed that for $r = 5$, approximating the Jones polynomial of the trace closure of a braid at the $r$-th root of unity is $DQC1$-complete. In [6], it was further shown that actually approximating the Jones polynomial of the trace closure at any $r$-root of unity is a $DQC1$ problem. Here $DQC1$ is the set of problems which can be solved efficiently by a 1-clean qubit quantum computer [7]. 1-clean qubit means the initial state consists of a single qubit in the pure state $|0\rangle$, and $n$ qubits in a maximally mixed state. This is described by the density matrix

$$\rho = |0\rangle\langle 0| \otimes \frac{I}{2^n}$$

Then we can apply a unitary evolution on these $(n + 1)$ qubits and measure the clean qubit in the computational basis. The probability of measuring $|0\rangle$ is

$$p_0 = 2^{-n} \text{Tr}\{(|0\rangle\langle 0| \otimes I)U(|0\rangle\langle 0| \otimes I)U^\dagger\}$$

For more detailed discussion of the $DQC1$ model, see [7, 14].

**Theorem 2.** [14, 6] There is an efficient classical algorithm which, given a braid $\sigma \in B_n$ of length $m$ and an error threshold $\varepsilon' > 0$ as input, outputs a description of a quantum circuit $U_{\sigma, \varepsilon'}$ of size $\text{poly}(n, m, \frac{1}{\varepsilon'})$. This quantum circuit computes a random variable $0 \leq Z(\sigma) \leq 1$, in the one clean qubit model such that

$$\Pr\left\{ \left| \frac{|J(\hat{\sigma}_{\text{tr}}; r)|}{d^n} - Z(\sigma) \right| < \varepsilon' \right\} > \frac{3}{4}.$$ 

**Theorem 3.** [14] The problem of approximating $\frac{|J(\hat{\sigma}_{\text{tr}}; r)|}{d^n}$ for a braid $\sigma \in B_n$ is $DQC1$-complete.
**Sketch of Proof.** The key point is that approximating the normalized trace of a circuit is $DQC_1$-complete \[2\]. We know that the Jones polynomial of a braid closure is equal to the generalized trace of the braid under the Jones representation. Thus if we ignore some technical details about how to encode the Jones representation into a circuit, the statement in the theorem is plausible. We now sketch the proof that approximating the normalized trace, $\frac{tr(U)}{2^n}$, of a circuit $U$ on $n$ qubits is a $DQC_1$-complete problem.

We first show approximating the normalized trace is in $DQC_1$. For a circuit $U$ of $n$ qubits and a pure state $|\psi\rangle$, there is a standard way to approximate $\langle \psi | U | \psi \rangle$, called the Hadamard test, which is shown below.

\[
\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad H \quad M
\]

In the circuit above, a horizontal line with a slash through it represents multiple qubits. $U$ is the $n$-qubit gate, $H$ is the Hadamard gate, and $M$ is the measurement of the first qubit in the computational basis. The following short computation shows that the probability of obtaining $|0\rangle$ is

\[
\tilde{p}_0 = \left| \langle 0 | 0 \rangle \otimes Id \right| (H \otimes Id) \bigwedge (U) \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi\rangle \right) \right| ^2 = \frac{1 + U}{2} |\psi\rangle \right| ^2 = \frac{1 + Re(\langle \psi | U | \psi \rangle)}{2}.
\]

Similarly, if the control bit is initialized with $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$, then the probability to obtain $|0\rangle$ is $\frac{1 + Im(\langle \psi | U | \psi \rangle)}{2}$.

Now suppose $|\psi\rangle$ is in a maximally mixed state, then running the Hadamard test to it gives the probability

\[
\tilde{p}_0 = \sum_{x \in \{0,1\}^n} \frac{1}{2^n} \frac{1 + Re(\langle x | U | x \rangle)}{2} = \frac{1}{2} + \frac{Re(Tr U)}{2^{n+1}}.
\]

Notice that the maximally mixed state is exactly the input of the one qubit clean model. We can use the one clean qubit as the control qubit in the Hadamard test to convert the circuit $U$ into controlled-$U$. Therefore, the one qubit clean model can approximate the normalized trace.
Next we show that approximating the normalized trace is $DQC_1$-complete. This should be more or less clear from Equation 2.1, namely after applying an $(n+1)$-qubit gate $U$ to the density matrix $|0⟩⟨0| \otimes \frac{I}{\sqrt{2^n}}$ followed by the measurement of the clean qubit, the probability to obtain $|0⟩$ is $p_0 = 2^{-n}Tr\{(|0⟩⟨0| \otimes I)U(|0⟩⟨0| \otimes I)U^†\}$. Note that $(|0⟩⟨0| \otimes I)U(|0⟩⟨0| \otimes I)U^†$ is not a unitary transformation so we cannot approximate the trace directly. However, the following circuit $U'$ can be easily constructed, and one can check that $p_0 = \frac{tr(U')}{2^{n+2}}$. Also note that $U'$ is an $(n+3)$-qubit gate, thus we can approximate the normalized trace $\frac{tr(U')}{2^{n+3}}$. This shows that approximating the normalized trace is $DQC_1$-complete.

\[ \begin{array}{c}
\text{the clean qubit} \\
\text{n qubits} \\
\hline \\
U^† \quad U \quad = U'
\end{array} \]

2.3. Complexity Classes as Axioms. It is easy to show that $DQC_1 \subset BQP$. But it’s not known whether this inclusion is strict or not. Another generally accepted conjecture is that $BQP \not\subset NP$. We are going to give a stronger assumption.

We define a complexity class $NP * DQC_1$, which informally is the composition of $NP$ and $DQC_1$.

More formally, a problem $X$ is in $NP * DQC_1$, if there exists a problem $Y$ in $NP$ and a problem $Z$ in $DQC_1$, such that for any input $x$ of size $n$, there is a certificate $y(x)$ of size $poly(n)$, such that $Y(x, y(x))$ outputs 1 and $Z$ takes $(Y(x, y(x)))$ as input and outputs $X(x)$. Intuitively, a problem $X$ in $NP * DQC_1$ can be solved by solving two related problems, one is in $NP$ and the other in $DQC_1$.

Obviously, $NP * DQC_1$ contains both $NP$ and $DQC_1$. But again it’s not known whether it contains $BQP$.

Axiom 1. $BQP \not\subset NP * DQC_1$

Axiom 2. $BQP \not\subset NP$

Axiom 3. $BQP \not\subset DQC_1$

Remark 2. Note that Axiom 1 is potentially stronger than Axioms 2 and 3. Thus if we accept Axiom 1, then Axioms 2 and 3 follow automatically. The reason that we still list them separately as axioms is
that Theorems 5 and 6 depend only on Axiom 2 and Axiom 3, respectively. In next section, we use these three axioms to prove Theorems 4, 5, and 6.

3. **Main Theorems**

**Lemma 2.** [12] Let $D$ be an oriented link diagram, denote the number of crossings of $D$ by $c(D)$, the number of Seifert circles of $D$ by $s(D)$, the number of components by $n(D)$, and the genus of the corresponding Seifert surface from the Seifert algorithm by $g(D)$. Then the following equality holds:

$$c(D) - s(D) - n(D) + 2 - 2g(D) = 0.$$  

In particular, $s(D) \leq c(D) + 2$.

**Proof** For a link diagram $D$, let $S$ be the corresponding Seifert surface obtained from the Seifert algorithm. By shrinking the disks bounded by Seifert circles into vertices and the half twisted bands into edges, we can easily compute the Euler characteristics of $S$, namely $\chi(S) = s(D) - c(D)$. Then we attach a disk to $S$ along each component of the boundary of $S$ to obtain a closed surface, which we assume has genus $g(D)$. Clearly the number of disks that we need to attach is $n(D)$. So we have the relation $2 - 2g(D) = \chi(S) + n(D)$, which implies the equation in the lemma. 

From Axiom 1.

**Theorem 4.** If $r$ is an integer, $r \geq 5$ but $\neq 6$, then given any two-variable integral polynomials $p$ and $q$, there exists a link diagram $D$ such that, if $D' \sim_r D$, and $D'$ is the trace closure of some braid, then

$$g(D') > g(D) + \log q(g(D), c(D))$$

unless

$$\text{dist}_r(D, D') > p(g(D), c(D)).$$

**Remark 3.** This is reminiscent of Theorem A in [3], which basically says a diagram cannot be made logarithmically thin via polynomially many operations. Theorem 4 refines Theorem A in [3] in the sense that if the resulting diagram has the nice form of a trace closure, we get a much better linear lower bound.

**Proof** We will show that the failure of this theorem contradicts Axiom 1. Assuming the theorem does not hold, then we have the following statement:
∃ integral polynomials \( p \) and \( q \) of two variables, ∀ link diagram \( D \),
∃ \( D' = \sigma^{tr} \) for some braid \( \sigma' \), \( D' \sim_r D \), such that
\[
dist_r(D, D') \leq p(g(D), c(D)) \quad \text{and} \quad g(D') \leq g(D) + \log q(g(D), c(D))
\]

In complexity theory language, this is essentially to say there exists a problem in \( NP \) which, with a diagram \( D \) as input, outputs a diagram \( D' = \hat{\sigma}'^{tr} \) such that \( D' \sim_r D \) and \( g(D') \leq g(D) + \log q(g(D), c(D)) \).

Given a braid \( \sigma \in B_{2n} \), \(|\sigma| = m\), then we know that \( g(\hat{\sigma}^{plat}) = 2n \), and \( c(\hat{\sigma}^{plat}) = m \). By the statement above, there exists a diagram \( D' = \hat{\sigma}'^{tr} \), \( D' \sim_r \hat{\sigma}^{plat} \), such that \( \dist_r(\hat{\sigma}^{plat}, D') \leq p(2n, m) \), and \( g(D') \leq 2n + \log q(2n, m) \).

Assume \( \sigma' \in B_{n'} \), then \( g(D') = 2n' \). So we have the inequality:
\[ n' \leq n + \frac{1}{2} \log q(2n, m). \]

Notice that \(|\sigma'|\) is \( poly(n, m) \) since \( \dist_r(\hat{\sigma}^{plat}, D') \leq p(2n, m) \).

Now we apply Theorem 2 to \( \sigma' \). Setting the error threshold \( \varepsilon' = \frac{\varepsilon}{\sqrt{q(2n, m)}} \), then we get a circuit \( U \) of size \( poly(n', |\sigma'|, q(2n, m)) = poly(n, m, \frac{1}{\varepsilon}) \), and
\[
Pr\left\{ \left| \frac{J(\hat{\sigma}'^{tr}; r)}{d^{n'}} - Z(\sigma') \right| < \frac{\varepsilon}{\sqrt{q(2n, m)}} \right\} > \frac{3}{4}.
\]
The above inequality is equivalent to
\[
Pr\left\{ \left| \frac{J(\hat{\sigma}^{plat}; r)}{d^n} - \sqrt{q(2n, m)}Z(\sigma') \right| < \varepsilon \right\} > \frac{3}{4}.
\]
The polynomial \( \sqrt{q(2n, m)} \) is efficiently computable on a 1-clean qubit machine. Therefore, approximating \( \frac{J(\hat{\sigma}^{plat}; r)}{d^n} \) is a problem in \( NP \ast DQC1 \). By Theorem 1 this problem is complete in \( BQP \). So it follows that \( BQP \subset NP \ast DQC1 \), which contradicts to Axiom 1.

\[ \square \]

**Corollary 1.** If \( r \) is an integer, \( r \geq 5 \) but \( \neq 6 \), then given any two-variable integral polynomials \( p \) and \( q \), there exists a link diagram \( D \) such that, for any diagram \( D' \), \( D' \sim_r D \), we have
\[
c(D') > \frac{g(D)}{2} + \log q(g(D), c(D)) \quad \text{unless} \quad \dist_r(D, D') > p(g(D), c(D)).
\]
Assuming that the corollary is false, we have the following statement:

\[ \exists \text{ polynomials } p \text{ and } q \text{ of two variables}, \forall \text{ link diagram } D, \exists D', D' \sim_r D, \text{ such that} \]

\[ \text{dist}_r(D, D') \leq p(g(D), c(D)) \quad \text{and} \quad c(D') \leq \frac{g(D)}{2} + \log q(g(D), c(D)) \]

By Lemma 2, \#(Seifert circles of \(D') \leq c(D') + 2.

It's a well known result that transforming a link diagram into the trace closure of some braid diagram while preserving the link type is a problem in \(P\) (e.g. see [21]). Moreover, as the algorithm described in Theorem 1-1 of [18], if a link diagram has \(n\) Seifert circles, then at most \(n^2\) Reidemeister II moves need to be performed to implement this transformation. No other types of Reidemeister moves are required, and this algorithm preserves the number of Seifert circles.

Applying this algorithm to the diagram \(D'\) results the trace closure of some braid \(\dot{\sigma}^{tr} \in B_{n'}\). Since \#(Seifert circles of \(D') = \#(Seifert circles of \dot{\sigma}^{tr}) = n' = \frac{g(\dot{\sigma}^{tr})}{2}\), we have

\[ g(\dot{\sigma}^{tr}) \leq 2c(D') + 4 \leq g(D) + 2 \log q(g(D), c(D)) + 4 \]

and

\[ \text{dist}_r(D, \dot{\sigma}^{tr}) \leq p(g(D), c(D)) + \left(\frac{g(D)}{2} + \log q(g(D), c(D)) + 2\right)^2 \]

Clearly, \(\dot{\sigma}^{tr} \sim_r D\). This contradicts to Theorem 4.

\[ \square \]

The following theorem is in [3], where it followed from the assumption that \(\#P \not\subseteq NP\). Here we deduce it from Axiom 2.

From Axiom 2.

**Theorem 5.** If \(r\) is an integer, \(r \geq 5\) but \(\neq 6\), then given any two-variable integral polynomials \(p\) and \(q\), there exists a link diagram \(D\) such that, if \(D' \sim_r D\), then

\[ g(D') > \log q(g(D), c(D)) \quad \text{unless} \]

\[ \text{dist}_r(D, D') > p(g(D), c(D)). \]

**Proof** As in the original proof in [3], if the theorem is not true, then evaluating the Jones polynomial of a link diagram at the \(r\)-th root of unity is a problem in \(NP\). Then approximating \(\frac{|J(\dot{\sigma}^{plat}, r)|}{d^n}\) for a braid \(\sigma \in B_{2n}\) is a problem in \(NP\), which implies \(BQP \subset NP\), contradicting Axiom 2.

\[ \square \]
The following corollary is clearly weaker than Corollary 1. Since it follows directly from Axiom 2 (and Theorem 5), which is weaker than Axiom 1, we still include it here with a proof:

**Corollary 2.** If \( r \) is an integer, \( r \geq 5 \) but \( \neq 6 \), then given any two-variable integral polynomials \( p \) and \( q \), there exists a link diagram \( D \) such that, if \( D' \sim_r D \), then

\[
c(D') > \log q(g(D), c(D)) \quad \text{unless} \quad \text{dist}_r(D, D') > p(g(D), c(D)).
\]

**Proof** If the statement is not true, then \( \exists \) polynomials \( p \) and \( q \), given any braid \( \sigma \in B_{2n}, |\sigma| = m \), there exists a link diagram \( D \), such that \( \hat{\sigma}_{\text{plat}} \sim_r D \), \( \text{dist}_r(\hat{\sigma}_{\text{plat}}, D) < p(2n, m) \) and \( c(D) < \log q(2n, m) \).

Classically evaluating the Jones polynomial of the diagram \( D \) has the complexity \( O(2^{c(D)}) < O(q(2n, m)) \). Thus evaluating \( |J(\hat{\sigma}_{\text{plat}}; r)| \) for a braid \( \sigma \in B_{2n} \) is a problem is \( NP \), which contradicts to Axiom 2.

\[\Box\]

Theorem 6 below and its corollary 3 are weaker than Theorem 4 and Corollary 1. However, we still point them out separately since they follow from weaker axioms.

From Axiom 3:

**Theorem 6.** If \( r \) is an integer, \( r \geq 5 \) but \( \neq 6 \), \( q \) is any two-variable integral polynomial, let \( Q(r, q) \) be such a problem, which takes a link diagram \( D \) as input, and outputs a braid diagram \( \sigma \), such that \( D \) and \( \hat{\sigma}_{\text{tr}} \) have the same Jones polynomial at the \( r \)-th root of unity and

\[g(\hat{\sigma}_{\text{tr}}) \leq g(D) + \log q(g(D), c(D)).\]

Then \( Q(r, q) \) is not in \( P \).

**Proof** Assume \( Q(r, q) \in P \), then apply \( Q(r, q) \) to the plat closure of the braid \( \sigma \in B_{2n}, |\sigma| = m \). Let \( \sigma' \in B_{n'} \) be the output. Then

\[g(\hat{\sigma}_{\text{tr}}') \leq 2n + \log q(2n, m).\]

As in the last part of the proof in Theorem 4, we can approximate \( \frac{|J(\hat{\sigma}_{\text{plat}}; r)|}{d^n} \) by applying Theorem 2 to \( \sigma' \) to approximate \( \frac{|J(\hat{\sigma}_{\text{tr}}'; r)|}{d^n} \) which is \( DQC1 \) complete. By Theorem 1, approximating \( \frac{|J(\hat{\sigma}_{\text{plat}}; r)|}{d^n} \) is \( BQP \) complete. This implies \( BQP \subset DQC1 \), which contradicts to Axiom 3.

\[\Box\]
Corollary 3. If $r$ is an integer, $r \geq 5$ but $r \neq 6$, $q$ is any two-variable integral polynomial, let $R(r,q)$ be such a problem, which takes a link diagram $D$ as input, and outputs a link diagram $D'$, such that $D$ and $D'$ have the same Jones polynomial at the $r$-th root of unity and
\[ c(D') \leq \frac{g(D)}{2} + \log q(g(D), c(D)). \]

Then $R(r,q)$ is not in $P$.

References

[1] Dorit Aharonov, Vaughan Jones, and Zeph Landau. A polynomial quantum algorithm for approximating the Jones polynomial. Algorithmica, 55(3):395–421, 2009.
[2] Shepherd Dan. Computation with unitaries and one pure qubit. arXiv preprint quant-ph/0608132, 2006.
[3] M. H. Freedman. Complexity classes as mathematical axioms. Annals of Mathematics, 170(995), 2009.
[4] Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. Bulletin of the American Mathematical Society, 40(1):31–38, 2003.
[5] P.-M. Gilmer. Congruence and quantum invariants of 3-manifolds. Algebr. Geom. Topol, 7:1767–1790, 2007.
[6] S.-P. Jordan and P. Wocjan. Estimating Jones and homfly polynomials with one clean qubit. Quantum Information and Computation, 9(264), 2009.
[7] E. Knill and R. Laflamme. Power of one bit of quantum information. Physical Review Letters, 81(25), 1998.
[8] Greg Kuperberg. How hard is it to approximate the Jones polynomial? arXiv preprint arXiv:0908.0512, 2009.
[9] M. Lackenby. Fox’s congruence classes and the quantum-su (2) invariants of links in 3-manifolds. Commentarii Mathematici Helvetici, 71(1):664–677, 1996.
[10] L. Lovasz M. Bordewich, M. Freedman and D. Welsh. Approximate counting and quantum computation. Combinatorics Probability and Computing, 14(5/6):737–754, 2005.
[11] S.-H. Ng and P. Schauenburg. Congruence subgroups and generalized frobenius-schur indicators. Communications in Mathematical Physics, 300(1), 2010.
[12] D. Rolfsen. Knots and links. Mathematics lecture series. Publish or Perish, 1976.
[13] S. Schleimer. Sphere recognition lies in np. http://arxiv.org/pdf/math/0407047.pdf, 2004.
[14] P.-W. Shor and S.-P. Jordan. Estimating Jones polynomials is a complete problem for one clean qubit. Quantum Information and Computation, 8(681), 2008.
[15] V.-G. Turaev and N. Reshetikhin. Invariants of 3-manifolds via link polynomials and quantum groups. Invent. Math, 103(3), 1991.
[16] D. Vertigan. The computational complexity of tutte, Jones, homfly and kauffman invariants. DPhil Thesis, Oxford University, Oxford, England, 1991.
[17] D. Vertigan. The computational complexity of tutte invariants for planar graphs. *SIAM J. Comput.*, 35(3), 2005.

[18] P. Vogel. Representation of links by braids: A new algorithm. *Comment. Math. Helvetici*, 65(104), 1990.

[19] Zhenghan Wang. *Topological quantum computation*, volume 112. Amer Mathematical Society, 2010.

[20] P. Wocjan and J. Yard. The jones polynomial: Quantum algorithms and applications in quantum complexity theory. *Quantum Information and Computation*, 0(0), 2003.

[21] S. Yamada. The minimal number of seifert circles equals the braid index of a link. *Invent. Math*, 89(347), 1987.

1Department of Mathematics, University of California, Santa Barbara, CA 93106

E-mail address: xingshan@math.ucsb.edu, zhenghwa@math.ucsb.edu

2Microsoft Research, Station Q, University of California, Santa Barbara, CA 93106

E-mail address: michaelf@microsoft.com, zhenghwa@microsoft.com