arXiv:quant-ph/0603069v3 3 Aug 2007

THE JONES POLYNOMIAL: QUANTUM ALGORITHMS AND APPLICATIONS IN QUANTUM COMPLEXITY THEORY

PAWEL WOCJAN[a]

Institute for Quantum Information, Caltech
Pasadena, CA 91125, USA

JON YARD[b]

Institute for Quantum Information, Caltech
Pasadena, CA 91125, USA

We analyze relationships between quantum computation and a family of generalizations of the Jones polynomial. Extending recent work by Aharonov et al., we give efficient quantum circuits for implementing the unitary Jones-Wenzl representations of the braid group. We use these to provide new quantum algorithms for approximately evaluating a family of specializations of the HOMFLYPT two-variable polynomial of trace closures of braids. We also give algorithms for approximating the Jones polynomial of a general class of closures of braids at roots of unity. Next we provide a self-contained proof of a result of Freedman et al. that any quantum computation can be replaced by an additive approximation of the Jones polynomial, evaluated at almost any primitive root of unity. Our proof encodes two-qubit unitaries into the rectangular representation of the eight-strand braid group. We then give QCMA-complete and PSPACE-complete problems which are based on braids. We conclude with direct proofs that evaluating the Jones polynomial of the plat closure at most primitive roots of unity is a #P-hard problem, while learning its most significant bit is PP-hard, circumventing the usual route through the Tutte polynomial and graph coloring.

Keywords: quantum algorithms, quantum complexity theory, topological quantum computation

Communicated by: to be filled by the Editorial

1 Introduction

There is evidence that a computer which could manipulate quantum mechanical degrees of freedom would be more powerful than a classical computer. Since the discovery by Shor that a quantum computer could efficiently factor composite integers, a task which is believed to be hard on conventional computers, much effort has been expended toward understanding the capabilities and limitations of quantum computers. In this paper, we investigate ways in which the Jones polynomial invariant of knots and links, together with its generalizations, contribute to this understanding. Witten discovered [40] that the Jones polynomial could

---

[a]School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816, USA. Electronic address: `wocjan@cs.ucf.edu`
[b]Electronic address: `jtyard@caltech.edu`

be understood via tools from topological quantum field theories. Freedman, Kitaev, Larsen and Wang [11] established its connection to computer science in the context of topological quantum computation. In a topological quantum computer, the trajectories of particles which are restricted to a plane are braided in order to manipulate the internal state of the computer. They showed that such computers can be simulated on conventional quantum computers, and also that when the underlying physics of a computer is described by a suitable topological quantum field theory, that it is possible to achieve universal quantum computation.

In [10], it was shown that topological quantum computers could be efficiently simulated by computers based on the standard quantum circuit model, implying the existence of an efficient algorithm for approximating the Jones polynomial of certain links obtained from braids. More recently, Aharonov, Jones and Landau [2] gave explicit quantum algorithms for approximating the Jones polynomial of either the trace or plat closure of a braid on a quantum computer. Our first contribution in this paper is a family of quantum circuits implementing the so-called Jones-Wenzl unitary representations of the braid group, generalizing the circuits for the Jones representation from [2]. We then show how to use our circuits to approximate a family of evaluations of the HOMFLYPT two-variable polynomial. We also sketch two different quantum algorithms for approximating the Jones polynomial of links obtained via a class of closures generalizing the trace and plat closures. In the sense of [7], our quantum algorithms obtain additive approximations of Jones and HOMFLYPT polynomial evaluations in polynomial-time.

In [12, 13], a converse to the above simulation results was proved. More specifically, it was shown there that quantum circuits can be simulated by braids, in such a way that the output probabilities of the quantum circuit are functions of the Jones polynomial of the plat closure of some braid of comparable length to that of the original circuit. Our third contribution is a simpler proof of their main result. In fact, this work grew from our attempts to understand the connections between these works and [2].

Finally, we give applications of the Jones polynomial to quantum complexity theory. We begin by restating a result that was proved in [7], showing that a machine which obtains an additive approximation of the Jones polynomial of the plat closure of a braid is equally as powerful as a quantum computer. We then introduce two new problems, **Increase Jones Plat** and **Approximate Concatenated Jones Plat**. The first asks if a given braid can be conjugated by another braid from a given class such that the Jones polynomial of its plat closure is nearly maximal. We prove that this problem is complete for the complexity class QCMA, a certain quantum analog of NP. The latter problem asks if a given braid, after being concatenated with itself exponentially many times, has a large plat closure. We show that this problem is PSPACE-complete. Finally, we give self-contained proofs that learning n of the most significant bits of the Jones polynomial of the plat closure of an n-strand braid is a #P-hard problem, while learning its most significant bit is PP-hard. This constitutes a simpler, quantum-based proof of the known result that computing the Jones polynomial is #P-hard. The original proof of this (see e.g. [39]) relates the Jones polynomial to the Tutte polynomial of a signed graph to the chromatic number of that graph to the #P-complete problem #SAT. Our proof, however, shows that learning a linear number of the highest order bits of the Jones polynomial of the plat closure of a braid is #P-hard.

The paper is organized as follows. In the next section, we review elements of the theory

of links, braids and the Jones polynomial. There, we review some different ways of turning a braid into a link, while introducing a new type of closure which we call a generalized closure. We also give precise statements of the approximations achieved by the algorithms. In Section 3, we describe the unitary representations of the braid group used in this paper, highlighting their origins from Hecke algebras. In Section 4, we show how to efficiently implement these representations on the state space of a quantum computer. Section 5 contains derivations of representation-theoretic formulae for the HOMFLYPT and Jones polynomials. Section 6 shows how to use the quantum circuits of the previous section to construct quantum algorithms for approximating certain evaluations of the HOMFLYPT and Jones polynomials of closed braids. In Section 7, we provide a self-contained proof of the converse of the results in the previous section – that local quantum circuits can be simulated by braids. Finally, in Section 8, we review notions of classical and quantum complexity theory, after which we present our complexity-theoretic results. We conclude with a discussion in Section 9.

2   Background on link invariants and additive approximations

Here we give background material on the links invariants used in this paper. We also formalize the notion of approximation for our quantum approximation algorithms. We refer the reader to, for example, [39] for further details on link invariants. A *knot* is a closed, nonintersecting curve in $\mathbb{R}^3$. More generally, a *link* is an embedding of some finite number of nonintersecting closed curves in $\mathbb{R}^3$. Links are identified up to *isotopy*, which means that two links which are related by some bijection $f \colon \mathbb{R}^3 \to \mathbb{R}^3$ of the ambient space with itself for which f and f^{-1} are continuous are considered to be *equivalent*. An *oriented link* is a link in which every component is assigned an orientation. If $\overrightarrow{L}$ is an oriented link, we will denote the unoriented link resulting from forgetting the orientation as L.

A central problem in knot theory is to determine, given descriptions of two links, whether or not they are equivalent. In order to solve such a problem, one must decide on how the links are to be described. One such way is in terms of a *link projection*. Informally, this is a two-dimensional diagram which uniquely specifies the link up to isotopy. The reader is referred to textbooks such as [25, 28, 29, 39] for examples and further exposition. The key property of any link projection is that at each crossing, it keeps track of which string goes above or below the other. Usually, this information is conveyed by leaving a gap in the string of the undercrossing. A classic result in knot theory states that two unoriented links are equivalent if and only if the link projection of one can be transformed into that of the other by a finite sequence of *Reidemeister moves* (see e.g. any of the texts listed above).

The HOMFLYPT and Jones polynomials

Another way of (partially) distinguishing links involves assigning an *invariant* to each link so that links which are equivalent up to isotopy have the same invariant. The *HOMFLYPT polynomial* [16, 32] $H_{\overrightarrow{L}}(t, x) \in \mathbb{Z}[t^{\pm 1}, x^{\pm 1}]$ is one such invariant. It is inductively defined by the *skein relation*

$$tH_{L_+}(t,x) - t^{-1}H_{L_-}(t,x) = xH_{L_0}(t,x) \tag{2.1}$$

(see Figure 2.1) together with the fact that the HOMFLYPT of the trivial knot (that is, a single unknotted circle) is unity. In this paper, we are concerned with various one-variable specializations of this invariant. For each integer $k \geq 2$ there is a corresponding *one-variable*
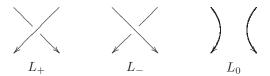
Fig. 2.1. L_+, L_-, L_0 denote three oriented links that differ in a small region, as symbolized by the above diagrams, but are otherwise the same. We say that the crossing corresponding to L_+ is a positive crossing, and the one corresponding to L_- is a negative crossing.

HOMFLYPT polynomial in $\mathbb{Z}[q^{\pm 1/2}]$:

$$H_{\overrightarrow{L}}^{(k)}(q) = H_{\overrightarrow{L}}(q^{k/2}, q^{1/2} - q^{-1/2}) \tag{2.2}$$

This is also known as the $\mathfrak{sl}_k$ invariant. Restricting to $k = 2$ yields the famous *Jones polynomial*:

$$J_{\overrightarrow{L}}(q) \equiv H_{\overrightarrow{L}}^{(2)}(q) = H_{\overrightarrow{L}}(q, q^{1/2} - q^{-1/2}).$$

If $\overrightarrow{L}$ consists of m unlinked copies of the trivial knot, setting $t = q^{k/2}$ and $x = q^{1/2} - q^{-1/2}$ in (2.1) implies that

$$H_{\overrightarrow{L}}^{(k)}(q) = \left(\frac{q^{k/2} - q^{-k/2}}{q^{1/2} - q^{-1/2}} \right)^{m-1}.$$

The exponentiated quantity on the right is known as a *quantum integer* and is easily shown to satisfy

$$\frac{q^{k/2} - q^{-k/2}}{q^{1/2} - q^{-1/2}} = q^{\frac{k-1}{2}} + q^{\frac{k-1}{2}-1} + \cdots + q^{-\frac{k-1}{2}} \tag{2.3}$$

if $q \neq 1$. By continuity, we consider this expression to hold as $q \to 1$, recovering the ordinary integer k. In this paper, we will only be interested in evaluations of these invariants at primitive roots of unity $q = e^{2\pi i/\ell}$, where ℓ is a nonnegative integer. To this end, we define for each integer k and each nonnegative integer ℓ, the constant[c]

$$[k]_\ell = \left. \frac{q^{k/2} - q^{-k/2}}{q^{1/2} - q^{-1/2}} \right|_{q=e^{2\pi i/\ell}} = \frac{\sin(\pi k/\ell)}{\sin(\pi/\ell)}.$$

A value which will occur frequently, especially when analyzing the Jones polynomial, is

$$[2]_\ell = \left. q^{1/2} + q^{-1/2} \right|_{q=e^{2\pi i/\ell}} = 2\cos(\pi/\ell). \tag{2.4}$$

The Jones polynomial will be the central object of our study, although we will also provide algorithms for approximating the one-variable HOMFLYPT polynomials. Where convenient, we sometimes write $J(\overrightarrow{L}, q) \equiv J_{\overrightarrow{L}}(q)$.

---

[c]Our definition here departs from the usual convention [38, 12] which defines $[k]_q = \frac{q^{k/2}-q^{-k/2}}{q^{1/2}-q^{-1/2}}$ for arbitrary q. This expression evaluates to ours when q is a primitive ℓ'th root of unity, which is the case of interest to us. We warn that other authors (e.g. [19]) use a different convention for the quantum integer and q.

The braid group

The braid group B_n on n strands is generated by counterclockwise twists $\{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ which satisfy the relations

$$
\begin{aligned}
\sigma_i \sigma_j \sigma_i &= \sigma_j \sigma_i \sigma_j, & |i-j| &= 1 & (2.5) \\
\sigma_i \sigma_j &= \sigma_j \sigma_i & |i-j| &> 1. & (2.6)
\end{aligned}
$$

The reader should picture n hanging pieces of string, and interpret each generator σ_i as a counterclockwise exchange of the strands in positions i and $i+1$, with inverses of the generators corresponding to clockwise twists. For instance, the braids $\sigma_1, \sigma_2^{-1} \in B_3$ are given by

$$
\sigma_1 = \; \text{\raisebox{-.5em}{⧓}} \; | \qquad \text{and} \qquad \sigma_2^{-1} = \; | \; \text{\raisebox{-.5em}{⧓}} \; .
$$

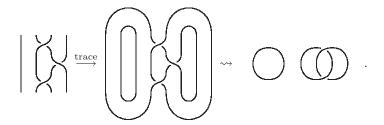The group product then corresponds to vertical concatenation of braids (up to isotopy equivalence). For instance,

$$
\sigma_2^{-1} \sigma_1 = \; \text{[braid diagram]} \; .
$$

The relation (2.5) is known as the Yang-Baxter equation, which is diagrammatically expressed as

$$
\text{[braid diagram]} = \text{[braid diagram]} \; .
$$

For each n, B_n is isomorphic to the subgroup of B_{n+1} generated by $\{\sigma_1, \ldots, \sigma_{n-1}\}$, consisting of braids in which the $n+1$'st strand does not participate. We denote the associated inclusion map as $\iota \colon B_n \to B_{n+1}$, which acts by adding an extra strand to the right of any given braid. Given a braid $b \in B_n$, there are many possible ways of *closing* the braid b to obtain a link. In the following we will recall three possible ways, the trace, the plat and a combination of these we call a generalized closure.

Specifying links with braids

One way to turn a braid into a link takes, for each $1 \leq i \leq n$, the i'th strand at the top of the braid and glues it to the i'th strand at the bottom. The resulting link $\widehat{b}$ is called the *trace closure* of b. For instance, the trace closure of the braid $b = \sigma_2 \sigma_3^{-1} \sigma_2$ is isotopic to the union of the trivial knot and the Hopf link:

Every link can be represented as the trace closure of some braid. Conventionally, one considers the trace closure of a braid to yield an oriented link, since an orientation can be unambiguously defined to travel downward along the braid. With this convention every generator σ_i gives rise to a positive crossing, while its inverse σ_i^{-1} to a negative crossing in the sense of Figure 2.1. A theorem of Markov demonstrates that, given braids b and b', their trace closures $\widehat{b}$ and $\widehat{b'}$ are isotopic if and only if b and b' are related by a finite sequence of *Markov moves*. We review these moves in Section 5 as they are relevant for obtaining a representation-theoretic formulae for the one-variable HOMFLYPT and Jones polynomials of trace closures of braids.

Another way of turning a braid on an even number $2p$ of strands into a link is known as the *plat closure*. Such a procedure starts with a braid $b \in B_{2p}$ and connects adjacent pairs of strands at the top and at the bottom. For example, the plat closure of $b = \sigma_2\sigma_3^{-1}\sigma_2 \in B_4$ is isotopic to the trefoil knot, as

Given a braid $b \in B_n$, we define a *generalized closure* of b to be specified by the following data: two braids $x, y \in B_n$ and nonnegative integers p and r which satisfy $2p + r = n$. The generalized closure $\chi_{x,y}^{p,r}(b)$ of b is obtained by first forming the braid xby, performing the plat closure on the $2p$ leftmost strands at the top and bottom, then connecting the remaining r strands at the top with the corresponding r strands at the bottom as in the trace closure.

Unlike with the trace closure, there is no unambiguous way to assign an orientation to the plat or generalized closure of a braid (unless $n = t$). While this poses a potential problem for defining the Jones and HOMFLYPT polynomials of such closures of braids, it is known [26] (and easily proved using the Kauffmann bracket [21] formula) that if $\overrightarrow{L}$ and $\overrightarrow{L'}$ are two oriented links that are isotopic as unoriented links, their Jones polynomials satisfy $J_{\overrightarrow{L}}(q) = q^m J_{\overrightarrow{L'}}(q)$ for some easily computable $m \in \mathbb{Z}$. This implies the absolute value of the Jones polynomial at roots of unity is independent of the orientation of a link, and is thus an invariant of unoriented links. In Section 5, we provide a representation-theoretic formula for the absolute value of the Jones polynomial of any generalized closure of a braid at primitive roots of unity, while in Section 6, we present a quantum algorithm which approximates these invariants of unoriented links.

Additive approximations

The notion of approximation which we will require was recently formalized in [7]; we review that material here. Let $\mathcal{X}$ be a set of problem instances, and suppose we are given a non-negative function $f \colon \mathcal{X} \to \mathbb{R}$ which is potentially difficult to evaluate exactly. The main idea of [7] is to approximate the function f with respect to some positive normalization function $g \colon \mathcal{X} \to \mathbb{R}$. Departing slightly from the definition given in [7], an *additive approximation* for the normalized function f/g associates a random variable $Z(x)$ to any problem instance

$x \in \mathcal{X}$ and $\delta > 0$ satisfying

$$\Pr\left\{\left|\frac{f(x)}{g(x)} - Z(x)\right| \leq \delta\right\} \geq 3/4.$$

In addition, it is required that such an approximation be achieved in time which is polynomial in the size of the problem instance and in $1/\delta$.

In Section 5 we provide tight upper bounds on the evaluations of the invariants we wish to approximate. We will see in (5.24) that if $b \in B_n$, the one-variable HOMFLYPT of the trace closure obeys $\left|H_{\hat{b}}^{(k)}(e^{2\pi i/\ell})\right| \leq [k]_\ell^{n-1}$. Similarly, we show in (5.38) that if $n = 2p + t$ and $x, y \in B_n$, the Jones of the generalized closure satisfies $\left|J(\xi_{x,y}^{p,r}(b), e^{2\pi i/\ell})\right| \leq [2]_\ell^{p+t-1}$. These bounds are achieved by closing the identity braid for the one-variable HOMFLYPT of the trace closure, or otherwise the braid $x^{-1}y^{-1}$ for the Jones of the generalized closure. We use these normalizations for our additive approximations, so that the absolute values of the resulting normalized polynomials always lie between 0 and 1, regardless of the size of the braid, number of strands, or particular primitive root of unity. We therefore consider the following two problems:

Problem 2.1 (Approximate HOMFLYPT Trace Closure) *Given is a braid $b \in B_n$ of length m, $\delta > 0$ and positive integers k, ℓ satisfying $2 \leq k < \ell$, where k is a constant. The task is to sample from a random variable $Z \in \mathbb{C}$, $|Z| \leq 1$, which is an additive approximation of the one-variable HOMFLYPT polynomial of the trace closure, evaluated at $e^{2\pi i/\ell}$, in the sense that*

$$\Pr\left\{\left|\frac{1}{[k]_\ell^{n-1}}H_{\hat{b}}^{(k)}(e^{2\pi i/\ell}) - Z\right| \leq \delta\right\} \geq 3/4.$$

Problem 2.2 (Approximate Jones Closure) *Given is a braid $b \in B_n$ of length m, two braids $x, y \in B_n$ of length $O(\mathrm{poly}(m))$, positive integers ℓ, p and r which satisfy $2p + r = n$, and $\delta > 0$. The task is to sample from a random variable $0 \leq Z \leq 1$ which is an additive approximation of the absolute value of the Jones polynomial of the generalized closure, evaluated at $e^{2\pi i/\ell}$, in the sense that*

$$\Pr\left\{\left|\frac{1}{[2]_\ell^{p+r-1}}\left|J\left(\chi_{x,y}^{p,r}(b), e^{2\pi i/\ell}\right)\right| - Z\right| \leq \delta\right\} \geq 3/4.$$

In Section 6, we prove:

Theorem 2.1 *Each of the above two problems can be solved in $O(\mathrm{poly}(m, 1/\delta))$ time on a quantum computer.*

3   Unitary Jones-Wenzl representations of the braid group

Here we summarize the representation theory of the braid group that we will need, following [38]. The relevant representations are inherited from representations of a certain family of Hecke algebras $H_n(q)$ which generalize the group algebra $\mathbb{C}S_n$ of the symmetric group S_n. In Section 5, we will show how these representations give rise to useful formulae for evaluations of the Jones and one-variable HOMFLYPT polynomials at roots of unity.

Fig. 3.1. Young diagram for the partition $\lambda = [5, 3, 2]$.

The Hecke algebra

It is well-known that the group algebra $\mathbb{C}S_n$ of the symmetric group S_n on $\{1, 2, \ldots, n\}$ objects has a presentation in terms of generators $\{1, s_1, s_2, \ldots, s_{n-1}\}$, where s_i is the involution which swaps i and $i + 1$. These satisfy the relations

$$s_i^2 = 1 \tag{3.1}$$

$$s_i s_j s_i = s_j s_i s_j, \quad |i - j| = 1 \tag{3.2}$$

$$s_i s_j = s_j s_i, \quad |i - j| > 1. \tag{3.3}$$

For every $q \in \mathbb{C}^\times$, the *Hecke algebra $H_n(q)$ of type A_{n-1}* is defined to be the algebra over $\mathbb{C}$ generated by 1 and $\{g_1, \ldots, g_{n-1}\}$ satisfying the relations

$$g_i^2 = g_i(q - 1) + q \tag{3.4}$$

$$g_i g_j g_i = g_j g_i g_j \qquad |i - j| = 1 \tag{3.5}$$

$$g_i g_j = g_j g_i \qquad |i - j| > 1. \tag{3.6}$$

Note that this is a deformation of the group algebra $\mathbb{C}S_n$ of the symmetric group S_n, which is obtained when $q = 1$. While it is known that $H_n(q) \simeq \mathbb{C}S_n$ whenever q is not a root of unity, we will rather be interested in the cases when q is a primitive root of unity, where the representation theory is slightly more subtle than that of $\mathbb{C}S_n$. One may represent the braid group B_n inside the Hecke algebra $H_n(q)$ by simply mapping each generator σ_i of B_n to the generator g_i of $H_n(q)$. Indeed, the representations of B_n we will use in this paper are induced by representations of $H_n(q)$ on suitable finite-dimensional Hilbert spaces. As with the braid groups, for each n, $H_n(q)$ is isomorphic to the subalgebra of $H_{n+1}(q)$ generated by 1 and $\{g_1, \ldots, g_{n-1}\}$. We use the same notation for the inclusion maps as with the braid groups, writing $\iota \colon H_n(q) \to H_{n+1}(q)$. One important distinction is that, writing 1_n for the identity in $H_n(q)$, we have $\iota(1_n) = 1_{n+1}$. We will therefore often omit the subscript for the identity element of each $H_n(q)$ whenever there is no cause for confusion.

Young diagrams and tableaux

As with S_n, the unitary irreps of B_n are labeled by *partitions* $\lambda = [\lambda_1, \lambda_2, \ldots, \lambda_n]$ satisfying $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$ and $\sum_i \lambda_i = n$. Throughout, we consider all partitions obtained by adding or deleting trailing zeros to be equivalent. We will identify any such partition with its *Young diagram* as pictured in Figure 3.1 for the partition $\lambda = [5, 3, 2]$. Note that the diagram has one row for each *part* of the partition, and that the i'th row contains λ_i boxes. We allow for the empty partition and diagram, which we denote $\emptyset$. Let Λ_n be the collection of n-box Young diagrams. Given two diagrams $\lambda \in \Lambda_n$ and $\mu \in \Lambda_m$, their *sum* $\lambda + \mu \in \Lambda_{n+m}$ is always well-defined, having parts equal to $(\lambda + \mu)_i = \lambda_i + \mu_i$. When it is well-defined as a partition, we will similarly define the *difference* $\lambda - \mu \in \Lambda_{n-m}$ to have parts $(\lambda - \mu)_i = \lambda_i - \mu_i$.
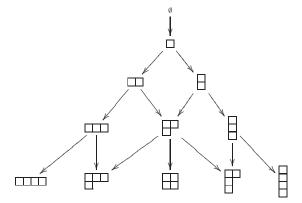
Fig. 3.2. The Young graph $\Lambda_{0,4}$.

Define the sets of diagrams $\Lambda_{m,n} \equiv \biguplus_{i=m}^{n} \Lambda_i$ and abbreviate $\Lambda \equiv \Lambda_{0,\infty}$. We may consider elements of Λ to be the nodes of an infinite directed graph, which we will call the *Young graph*, which contains an edge from a diagram λ' to a diagram λ whenever a single box can be added to λ' to obtain λ. We remark that we depart slightly from common terminology, where this graph, with each arrow reversed, is called a *Bratteli diagram*. With a slight abuse of notation, we write Λ for both the set of diagrams and for the corresponding Young graph, making a similar identification between subsets of Λ such as $\Lambda_{0,n}$ and the associated subgraph. In Figure 3.2, we give a picture of $\Lambda_{0,4}$.

By a *numbering* of an n-box diagram, we mean any assignment of the numbers $\{1, 2, \ldots, n\}$ to the boxes of the diagram, where each number appears only once. For a given diagram $\lambda \in \Lambda_n$, we write T_λ for the set of *standard tableaux* with shape λ, corresponding to numberings which are strictly increasing along each row and column. We often call a standard tableau just a *tableau*. We denote the set of all n-box tableaux as $T_n = \biguplus_{\lambda \in \Lambda_n} T_\lambda$ and the set of all tableaux as $T = \biguplus_{n=1}^{\infty} T_n$. We identify members of T_n with length-n paths starting at $\emptyset$ in $\Lambda_{0,n}$, pictured in Figure 3.2, with elements of T_λ correspond to paths which end at the diagram λ.

In this paper, we shall rather require certain restricted classes of Young diagrams and tableaux. To each pair (k, ℓ) of integers satisfying $\ell > k > 0$ corresponds a class of irreducible unitary representations of B_n. These representations are labelled by the n-box (k, ℓ)-*Young diagrams*, defined as

$$\Lambda_n^{(k,\ell)} = \{\lambda \in \Lambda_n : \lambda_{k+1} = 0, \lambda_1 - \lambda_k \leq \ell - k\}.$$

Note that these are the diagrams with at most k rows for which the difference between the numbers of boxes in the first and k'th rows is at most $\ell - k$. We will often just say that such a λ is an (k, ℓ)-diagram. For a given diagram λ, we refer to $\lambda_1 - \lambda_k$ as the *level* of λ, so that $\ell - k$ is the maximum level of all diagrams in $\Lambda_n^{(k,\ell)}$. As before, we make the similar abbreviations $\Lambda_{m,n}^{(k,\ell)}$ and $\Lambda^{(k,\ell)}$. We also identify any of these sets of diagrams with the appropriate subgraph of Λ. We refer to such a graph as a (k, ℓ)-*Young graph*. In Figure 3.3, we show the graph $\Lambda_{0,4}^{(2,5)}$. For a given $\lambda \in \Lambda_n^{(k,\ell)}$, define the (k, ℓ)-*tableaux* $T_\lambda^{(k,\ell)} \subset T_\lambda$ to be those standard tableaux of shape λ for which successively deleting the largest numbered boxes yields, at each
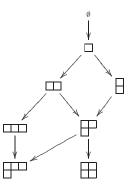
Fig. 3.3. The Young graph $\Lambda_{0,4}^{(2,5)}$. Comparison with Figure 3.2 reveals that this is the subgraph of $\Lambda_{0,4}$ obtained by removing vertices whose diagrams either have more than two rows, or level greater than $3 = 5 - 2$.

step, another (k, ℓ)-diagram. These tableaux can be identified with paths in $\Lambda_{0,n}^{(k,\ell)}$ going from $\emptyset$ to λ. We also define $T_n^{(k,\ell)}$ and $T^{(k,\ell)}$ in a similar manner as above. In the Section 5, we will see that the $(2, \ell)$-diagrams and tableaux are what is needed to give representation-theoretic expressions for the Jones polynomials $J(e^{2\pi i/\ell})$ of closures of braids, while the (k, ℓ)-diagrams are relevant for the one-variable HOMFLYPT polynomials $H^{(k)}(e^{2\pi i/\ell})$.

Unitary Jones-Wenzl representations of B_n

The representations of B_n we will introduce are parameterized by integers $\ell > k > 0$, where ℓ specifies a primitive ℓ'th root of unity which we will denote $q = e^{2\pi i/\ell}$. The irreducible components of the representations we will describe reduce to the usual irreps of S_n when $k = n$ and $\ell \to \infty$, so that $q \to 1$. For the rest of this section, we fix $\ell > k > 0$ and set $q = e^{2\pi i/\ell}$, describing a corresponding representation of $H_n(q)$ which induces a unitary representation of B_n. This representation is more easily described by a change of variables which leads to an equivalent presentation of $H_n(q)$. Rewriting the quadratic relation (3.4) as $(g_i + 1)(g_i - q) = 0$, we may define idempotents $e_i = (q - g_i)/(1 + q)$ (meaning that $e_i^2 = e_i$) for which

$$g_i = q(1 - e_i) - e_i = q - (1 + q)e_i. \tag{3.7}$$

Using these idempotents, the relations (3.4–3.6) may be expressed as

$$e_i^2 = e_i \tag{3.8}$$
$$e_i e_j e_i - \tau e_i = e_j e_i e_j - \tau e_j, \qquad |i - j| = 1 \tag{3.9}$$
$$e_i e_j = e_j e_i, \qquad |i - j| > 1, \tag{3.10}$$

where we follow the usual convention in setting $\tau \equiv [2]_\ell^{-2}$. For each integer d, define

$$a_\ell(d) = \frac{[d+1]_\ell}{[2]_\ell [d]_\ell}, \tag{3.11}$$

noting that $a_\ell(d) + a_\ell(-d) = 1 = a_\ell(1)$. Given any n-box tableau t and an integer $1 \leq i < n$, we respectively write $c_i(t)$ and $r_i(t)$ for the *column* and *row* which contain the number i,

defining

$$d_i(t) \equiv c_i(t) - c_{i+1}(t) - (r_i(t) - r_{i+1}(t)). \tag{3.12}$$

Note that $d_i(t)$ gives the total number of leftward and downward steps it takes to "walk" from i to $i+1$ on t, where moving right or up counts negatively. Given a generator s_i of S_n and a (k,ℓ)-tableaux $T_n^{(k,\ell)}$, let t' be the numbering obtained by swapping the numbers i and $i+1$ in $t \in T_n^{(k,\ell)}$. If t' is also a (k,ℓ)-tableau, define $s_i(t) = t'$ and $s_i(t') = t$; otherwise set $s_i(t) = t$. In order that $s_i(t) \neq t$, it is necessary and sufficient that i and $i+1$ *not* be in the same row or column of t. In such a case, we may think of it as a deformation of the path in $\Lambda_{0,n}^{(k,\ell)}$ corresponding to t which changes only the i-box diagram passed in the original path. Note that each generator s_i induces a partition of $T_n^{(k,\ell)}$ into sets of numberings (or paths) of size at most two.

We may now define a representation $\pi_n^{(k,\ell)}$ of $H_n(q)$ on a vector space $V_n^{(k,\ell)}$ which has an orthonormal basis labeled by n-box (k,ℓ) tableaux, i.e.

$$V_n^{(k,\ell)} = \mathrm{span}\big\{|t\rangle : t \in T_n^{(k,\ell)}\big\}.$$

For each i, $\pi_n^{(k,\ell)}(e_i)$ is a projection which is block diagonal in the $T_n^{(k,\ell)}$ basis with blocks of size either one or two. The size two blocks correspond to distinct pairs of tableaux t and $s_i(t)$ which are contained in $T_n^{(k,\ell)}$. Letting $V_{i,t} = \mathrm{span}\big\{|t\rangle, |s_i(t)\rangle\big\}$, the restriction of $\pi_n^{(k,\ell)}(e_i)$ to $V_{i,t}$ is the rank one projection onto $\sqrt{a_\ell\big(d_i(t)\big)}|t\rangle + \sqrt{a_\ell\big(-d_i(t)\big)}|s_i(t)\rangle$, written

$$\pi_n^{(k,\ell)}(e_i)\big|_{V_{i,t}} = \begin{pmatrix} a_\ell\big(d_i(t)\big) & \sqrt{a_\ell\big(d_i(t)\big)a_\ell\big(-d_i(t)\big)} \\ \sqrt{a_\ell\big(d_i(t)\big)a_\ell\big(-d_i(t)\big)} & a_\ell\big(-d_i(t)\big) \end{pmatrix}. \tag{3.13}$$

For the remaining $t \in T_n^{(k,\ell)}$, set $\pi_n^{(k,\ell)}(e_i)|t\rangle = |t\rangle$ if i and $i+1$ are in the same column of t; otherwise set $\pi_n^{(k,\ell)}(e_i)|t\rangle = 0$. This defines the action of $\pi_n^{(k,\ell)}(e_i)$ on all of $V_n^{(k,\ell)}$. Using (3.7), this representation maps each g_i to the unitary matrix

$$\pi_n^{(k,\ell)}(g_i) = q1_{V_n^{(k,\ell)}} - (1+q)\pi_n^{(k,\ell)}(e_i). \tag{3.14}$$

Abbreviating $d = d_i(t)$, we may use (2.3) to express the restriction to each $V_{i,t}$ as

$$\pi_n^{(k,\ell)}(g_i)\big|_{V_{i,t}} = -q^{1/2}\begin{pmatrix} \frac{q^{d/2}}{[d]_\ell} & \sqrt{1 - \frac{1}{[d]_\ell^2}} \\ \sqrt{1 - \frac{1}{[d]_\ell^2}} & -\frac{q^{d/2}}{[d]_\ell} \end{pmatrix}. \tag{3.15}$$

If i and $i+1$ are in the same column of t, this gives $\pi_n^{(k,\ell)}(g_i)|t\rangle = -|t\rangle$, while if they are in the same row we have $\pi_n^{(k,\ell)}(g_i)|t\rangle = q|t\rangle$. Because permutations cannot change the shapes of tableaux, it follows that this representation is reducible. The irreducible components are labeled by the (k,ℓ)-diagrams, so that

$$\pi_n^{(k,\ell)} = \bigoplus_{\lambda \in \Lambda_n^{(k,\ell)}} \pi_\lambda^{(k,\ell)},$$

where each $\pi_\lambda^{(k,\ell)}$ acts nondegenerately only on the subspace $V_\lambda^{(k,\ell)} = \big\{|t\rangle : t \in T_\lambda^{(k,\ell)}\big\}$, and

$$V_n^{(k,\ell)} = \bigoplus_{\lambda \in \Lambda_n^{(k,\ell)}} V_\lambda^{(k,\ell)}.$$

4   Efficient quantum circuits for unitary Jones-Wenzl representations

We will now show, for any integers $1 < k < \ell$, how to implement the corresponding Jones-Wenzl representations $\pi_n^{(k,\ell)}$ defined in (3.14) on a quantum computer. The basic idea is to embed these representations into a tensor product space (c.f. Section 5.2 of [33]). Our circuits resemble those of [2], where the $k = 2$ case is treated, although we require the combinatorial tools of Young diagrams and tableaux introduced in the previous section for higher values of k. These circuits allow us to give a new quantum algorithm in Section 6 for approximating the family of one-variable HOMFLYPT polynomials $H^{(k)}$ of the trace closures of braids. We begin with some background on quantum circuits.

The state space of a quantum computer has the structure of a Hilbert space $\mathcal{H}$. Denoting by $U(\mathcal{H})$ the group of unitary matrices acting on $\mathcal{H}$, a *quantum gate* is any $U \in U(\mathcal{H})$. By the *standard quantum circuit model*, we shall mean quantum computers whose state space decomposes into a finite number of localized two-dimensional subsystems, or qubits, so that $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$. We fix a preferred orthonormal basis for the Hilbert space of each qubit, which we call the *computational basis*:

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The state space of $\mathcal{H}$ is thus spanned by tensor products of these basis vectors, which we write as $\{|x^n\rangle : x^n \in \{0,1\}^n\}$, where

$$|x^n\rangle \equiv |x_1\rangle|x_2\rangle \cdots |x_n\rangle \equiv |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle.$$

We will abbreviate the set of all gates on n qubits as $U(2^n) \equiv U\big((\mathbb{C}^2)^{\otimes n}\big)$. We assume that the qubits are arranged on a line so that each qubit has at most two neighbors. In this case, it is well-known that an arbitrary unitary $U \in U(2^n)$ can be performed on the qubits by a sequence of (possibly exponentially many in n) *local unitaries* from $U(4)$ which act only on adjacent pairs of qubits. By a *length-m quantum circuit*, we will mean a sequence of m local two-qubit gates. When appropriate, we identify a quantum circuit with its overall unitary transformation $U = U_m U_{m-1} \cdots U_1$, where each U_i is a two-qubit unitary. Below, we will work with quantum circuits whose local systems (registers) may have dimension $k > 2$. Such systems can be implemented using $O(\log k)$ qubits, on which any unitary can be performed using only $O(k)$ two-qubit gates.

We now proceed by describing an encoding of the basis states of the reducible representation $V^{(k,\ell)}$ into $O\big(n \log(k)\big)$ qubits. Then we show how, using $O\big(n \log(n)\big)$ ancillary qubits, one can implement the image $\pi_n^{(k,\ell)}(\sigma_i)$ of each braid group generator σ_i with a quantum circuit of length $O\big(\text{poly}(n,k)\big)$. Given a tableau $t \in T_n^{(k,\ell)}$ and an integer $1 \le i \le n$, recall that we write $r_i(t)$ and $c_i(t)$ for the row and column which respectively contain the number i. Notice that these numbers satisfy $1 \le r_i(t) \le k$ and $1 \le c_i(t) \le n$ for each i. We abbreviate $r(t) = r_1(t)r_2(t) \cdots r_n(t) \in \{1, \ldots, k\}^n$ and define $c(t) \in \{1, \ldots, n\}^n$ similarly. Our first observation is that $r(t)$ uniquely specifies t. We may thus assign to each t a computational basis state of n systems with Hilbert spaces $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n$, where each Hilbert space $\mathcal{R}_i \simeq \mathbb{C}^k$ is spanned by computational basis states $\{|1\rangle^{\mathcal{R}_i}, \ldots, |k\rangle^{\mathcal{R}_i}\}$. Together, the systems have a combined Hilbert space which we write $\mathcal{R}^n = (\mathbb{C}^k)^{\otimes n}$. This yields an embedding $|t\rangle \mapsto |r(t)\rangle^{\mathcal{R}^n}$ of $V_n^{(k,\ell)}$ into $\mathcal{R}^n$ whose image we call the *computational subspace*.

We now introduce, for each $1 \leq i \leq n-1$, a register with Hilbert space $\mathcal{D}_i$ which will store the value $d_i(t)$ defined in (3.12) for each tableau. Because $|d_i(t)| \leq n$, we let $\mathcal{D}_i$ be spanned by basis states $\{|-n\rangle^{\mathcal{D}_i}, |-n+1\rangle^{\mathcal{D}_i}, \ldots, |n\rangle^{\mathcal{D}_i}\}$. We may now define an isometry $W \colon \mathcal{R}^n \to \mathcal{R}^n \mathcal{D}^{n-1}$ which coherently computes these values for a given encoding of a tableau as

$$W|r(t)\rangle^{\mathcal{R}^n} = |r(t)\rangle^{\mathcal{R}^n}|d(t)\rangle^{\mathcal{D}^{n-1}}. \tag{4.16}$$

Below, we will show that this isometry can be implemented efficiently. Now we follow (3.15) to define the unitaries which perform the braiding, while taking care to appropriately update the $\mathcal{D}^{n-1}$ registers. For each $2 \leq i \leq n-2$, define the unitary U_i' which acts on $\mathcal{R}_i \mathcal{R}_{i+1} \mathcal{D}_{i-1} \mathcal{D}_i \mathcal{D}_{i+1}$ as

$$U_i'|r_i, r_{i+1}, d_{i-1}, d_i, d_{i+1}\rangle = \alpha_{d_i}|r_i, r_{i+1}, d_{i-1}, d_i, d_{i+1}\rangle + \beta_{d_i}|r_{i+1}, r_i, d_{i-1}+d_i, -d_i, d_{i+1}+d_i\rangle.$$

where $\alpha_d = -\frac{q^{-\frac{d-1}{2}}}{[d]_\ell}$ and $\beta_d = -q^{1/2}\sqrt{1 - \frac{1}{[d]_\ell^2}}$. Since d_1 can only equal ± 1, we also set

$$U_1'|d_1\rangle^{\mathcal{D}_1} = \begin{cases} -|d_1\rangle^{\mathcal{D}_1} & \text{if } d_1 = 1 \\ q|d_1\rangle^{\mathcal{D}_1} & \text{if } d_1 = -1. \end{cases}$$

Additionally, we define U_{n-1}' to act on $\mathcal{R}_{n-1}\mathcal{R}_n \mathcal{D}_{n-2}\mathcal{D}_{n-1}$ via

$$U_{n-1}'|r_{n-1}, r_n, d_{n-2}, d_{n-1}\rangle = \alpha_{d_{n-1}}|r_{n-1}, r_n, d_{n-2}, d_{n-1}\rangle + \beta_{d_{n-1}}|r_{n-1}, r_n, d_{n-2}+d_{n-1}, -d_{n-1}\rangle.$$

Each of these unitaries can be implemented using $O(\text{poly}(n,k))$ two-qubit gates. Define the unitaries $U_i = W^{-1}U_i'W$ for $1 \leq i < n$. By construction, the map $\sigma_i \mapsto U_i$ defines a (degenerate) unitary representation $\rho_n^{(k,\ell)}$ of B_n which is isomorphic to $\pi_n^{(k,\ell)}$. Suppose now that we are given a braid $b = \sigma_{i_m}^{x_m} \cdots \sigma_{i_2}^{x_2} \sigma_{i_1}^{x_1} \in B_n$. The corresponding unitary

$$\begin{aligned} \sigma_{i_m}^{x_m} \cdots \sigma_{i_2}^{x_2} \sigma_{i_1}^{x_1} &\mapsto & U_{i_m}^{x_m} \cdots U_{i_2}^{x_2} U_{i_1}^{x_1} \\ &=& W^{-1}U_{i_m}'^{x_m} \cdots U_{i_2}'^{x_2} U_{i_1}'^{x_1} W \end{aligned}$$

therefore evolves the computational subspace of $\mathcal{R}^n$ according to the following commutative diagram

$$\begin{array}{ccc} V_n^{(k,\ell)} & \xrightarrow{\pi_n^{(k,n)}(b)} & V_n^{(k,\ell)} \\ \downarrow & & \uparrow \\ \mathcal{R}^n & \xrightarrow{\rho_n^{(k,\ell)}(b)} & \mathcal{R}^n. \end{array}$$

Now we show that the isometry W in (4.16) can be efficiently implemented. For this, we introduce n systems with joint Hilbert space $\mathcal{C}^n$, where each $\mathcal{C}_i$ is spanned by computational basis states $\{|0\rangle^{\mathcal{C}_i}, \ldots, |n\rangle^{\mathcal{C}_i}\}$. The purpose of these systems is to store the column numbers of each i. In addition, we introduce k registers $\mathcal{L}_1, \ldots, \mathcal{L}_k$ with bases $\{|0\rangle, \ldots, |n\rangle\}$ which will store the *shape* of the tableau. Given a qubit encoding $|r(t)\rangle^{\mathcal{R}^n}$ of a tableau t, we define the isometry $W' \colon \mathcal{R}^n \to \mathcal{R}^n \mathcal{C}^n \mathcal{L}^k$ as

$$W'|r(t)\rangle^{\mathcal{R}^n} = |r(t)\rangle^{\mathcal{R}^n}|c(t)\rangle^{\mathcal{C}^n}|\lambda(t)\rangle^{\mathcal{L}^k},$$

where $\lambda(t)$ is the vector of row lengths of t. This isometry can be efficiently implemented by first preparing the additional systems in the state $|0\cdots0\rangle^{\mathcal{C}^n}|0\cdots0\rangle^{\mathcal{L}^k}$, after which the composition of local gates $W' = W'_n\cdots W'_2 W'_1$ is applied, where each W'_i acts on $\mathcal{R}_i\mathcal{C}_i\mathcal{L}^k$ as

$$W'_i|r\rangle^{\mathcal{R}_i}|0\rangle^{\mathcal{C}_i}|\lambda\rangle^{\mathcal{L}^k} = |r\rangle^{\mathcal{R}_i}|\lambda_r{+}1\rangle^{\mathcal{C}_i}|\lambda'\rangle^{\mathcal{L}^k}$$

where λ' is λ with an additional box in row r. For each $1 \leq i < n$, we then define local unitaries W_i which act as $\mathcal{R}_i\mathcal{R}_{i+1}\mathcal{C}_i\mathcal{C}_{i+1}\mathcal{D}_i$ as

$$W_i|r\rangle^{\mathcal{R}_i}|r'\rangle^{\mathcal{R}_{i+1}}|c\rangle^{\mathcal{C}_i}|c'\rangle^{\mathcal{C}_{i+1}}|0\rangle^{\mathcal{D}_i} = |r\rangle^{\mathcal{R}_i}|r'\rangle^{\mathcal{R}_{i+1}}|c\rangle^{\mathcal{C}_i}|c'\rangle^{\mathcal{C}_{i+1}}|c - c' - (r - r')\rangle^{\mathcal{D}_i}.$$

We may thus write $W = W'^{-1}W_{n-1}\cdots W_2 W_1 W'$, where we uncompute the $\mathcal{C}^n$ and $\mathcal{L}^k$ registers. Because each W_i and W'_i can be implemented with $O\big(\text{poly}(n,k)\big)$, we find that W can be implemented with $O\big(\text{poly}(n,k)\big)$ local gates.

5   Representation-theoretic formulae for the Jones and HOMFLYPT

We will now illustrate how to use the unitary representations of Section 3 to write expressions for the evaluations, at primitive roots of unity, of the Jones and one-variable HOMFLYPT polynomials of the trace closure of a braid. We then review the Temperley-Lieb algebra, which we use to derive a formula for the Jones polynomial of our generalized closure of a braid.

Jones and HOMFLYPT polynomials of trace closures from the Markov trace

Here, we review the theory of Markov traces on Hecke algebras and show how they yield formulae for the one-variable HOMFLYPT polynomials of the trace closure of a braid. Our presentation is primarily based on Section 6 of [19] and Section 3 of [38]. We urge the reader who seeks a deeper understanding to consult these references. We also recommend [4]. Throughout this section, we fix a primitive root of unity $q = e^{2\pi i/\ell}$ for some integer $\ell \geq 3$.

The theory of Markov traces is best understood in light of the so-called Markov moves on braids. As mentioned earlier, the trace closures of two braids are isotopic iff the braids are connected by a finite sequence of Markov moves. Given any $b \in B_n$, a *type I Markov move* consists of conjugating b by any braid $x \in B_n$, taking $b \mapsto xbx^{-1}$. A *type II Markov move* adds another strand to b which is twisted either clockwise or counterclockwise with the n'th strand at the bottom of b, acting as $b \mapsto \sigma_n^{\pm}\iota(b)$. It is clear that the trace closures of braids related by the first Markov move are isotopic, since the top braid x is untied by the bottom braid x^{-1}. A picture more clearly illustrates the invariance of the trace closure under the second Markov move, as shown in Figure 5.4.

These topological considerations are reflected algebraically as follows. It is a theorem of Ocneanu [16] (see [19] for a simple proof) that for every $1 \leq k < \ell$ and for each n, there is a linear function $\text{tr}_{k\ell}\colon H_n(q) \to \mathbb{C}$ uniquely determined by

1. $\text{tr}_{k\ell}(1_n) = 1$ for $1_n \in H_n(q)$

2. $\text{tr}_{k\ell}(wv) = \text{tr}_{k\ell}(vw)$ for $w, v \in H_n(q)$

3. $\text{tr}_{k\ell}(e_n\iota(w)) = \frac{[k-1]_\ell}{[k]_\ell[2]_\ell}\,\text{tr}_{k\ell}(w)$ for all $w \in H_n(q)$ for all n.
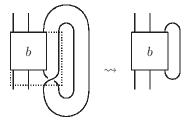
Fig. 5.4. Trace closure after the second Markov move on some $b \in B_3$. The dotted box on the left represents the braid $\sigma_3 \iota(b) \in B_4$. We have omitted the strands which close the two leftmost strands for visibility.

Using (3.7), a direct calculation shows that 3. implies that for $w \in H_n(q)$,

$$\mathrm{tr}_{k\ell}(g_n \iota(w)) = \left(q - (1+q)\frac{[k-1]_\ell}{[k]_\ell[2]_\ell} \right) \mathrm{tr}_{k\ell}(w) = \frac{q^{\frac{k+1}{2}}}{[k]_\ell} \mathrm{tr}_{k\ell}(w). \tag{5.17}$$

Such a function is known as a *positive Markov trace* on the inductive limit $H_\infty(q)$ of the Hecke algebras $H_n(q)$. This trace has a representation-theoretic formula which we recall below in (5.21). But first, we show how it can be used to express the Jones and one-variable HOMFLYPT polynomials. One first extends this trace to B_n via the identification $\sigma_i^\pm \mapsto g_i^\pm$. Cyclicity of the trace implies that $\mathrm{tr}_{k\ell}$ is invariant under type I Markov moves. However, it is not invariant under the second move because (5.17) implies that multiplication of $w \in H_n(q)$ by either g_n or g_n^{-1} affects the trace nontrivially. We will therefore construct, for each n, a normalized version $\overline{\mathrm{tr}}_{k\ell} \colon H_n(q) \to \mathbb{C}$ of the Markov trace which is also invariant under type II Markov moves, i.e.

$$\overline{\mathrm{tr}}_{k\ell}(\sigma_n^{\pm 1} \iota(b)) = \overline{\mathrm{tr}}_{k\ell}(b) \tag{5.18}$$

for each $b \in B_n$. For this, we define

$$\overline{\mathrm{tr}}_{k\ell}(b) \quad = \quad [k]_\ell^{n-1} q^{-\frac{k+1}{2}e(b)} \mathrm{tr}_{k\ell}(b). \tag{5.19}$$

Here, $e(b)$ is the sum of the exponents of the generators in the expression of b. Now if $b \in B_n$ and $b' = \sigma_n^{\pm 1} \iota(b) \in B_{n+1}$,

$$\begin{aligned}
\overline{\mathrm{tr}}_{k\ell}(b') &= [k]_\ell^n q^{-\frac{k+1}{2}e(b')} \mathrm{tr}_{k\ell}(b') \\
&= [k]_\ell^n q^{-\frac{k+1}{2}(e(b)\pm 1)} \frac{q^{\pm\frac{k+1}{2}}}{[k]_\ell} \mathrm{tr}_{k\ell}(b) \\
&= [k]_\ell^{n-1} q^{-\frac{k+1}{2}e(b)} \mathrm{tr}_{k\ell}(b) \\
&= \overline{\mathrm{tr}}_{k\ell}(b)
\end{aligned}$$

as required. To see that this normalized trace is equal to the one-variable HOMFLYPT of the trace closure of b, we follow [19] by considering an arbitrary oriented link diagram L_0 described as the trace closure of some braid. Choose a crossing in the braid arbitrarily – we assume it to be positive without loss of generality. By a type I Markov move, one can then express L_0 as the trace closure of a braid where the given positive crossing is at the bottom, i.e. $L_0 = \widehat{\sigma_i b}$. Inserting a positive or negative crossing adjacent to the one specified

above results in the oriented links $L_+ = \widehat{\sigma_i^2 b}$ and $L_- = \widehat{b}$. Using the formula (5.19) to express the normalized trace in terms of the linear trace $\mathrm{tr}_{k\ell}$, and replacing σ_i^2 using the quadratic relation (3.4), it is straightforward to check that

$$q^{k/2}\overline{\mathrm{tr}}_{k\ell}(\sigma_i^2 b) = q^{-k/2}\overline{\mathrm{tr}}_{k\ell}(b) + (q^{1/2} - q^{-1/2})\overline{\mathrm{tr}}_{k\ell}(\sigma_i b).$$

Therefore, the normalized trace satisfies the definition (2.2) of the one-variable HOMFLYPT polynomial from the skein relation (2.1) with $H_{\widehat{\sigma_i b}}^{(k)}(q) = \overline{\mathrm{tr}}_{k\ell}(\sigma_i b)$, so that

$$H_{\widehat{b}}^{(k)}(q) = [k]_\ell^{n-1} q^{-\frac{k+1}{2}e(b)} \, \mathrm{tr}_{k\ell}(b). \tag{5.20}$$

For $w \in H_n(q)$, the Markov trace has the following representation-theoretic formula

$$\mathrm{tr}_{k\ell}(w) = \sum_{\lambda \in \Lambda_n^{(k,\ell)}} s_\lambda^{(k,\ell)} \, \mathrm{Tr}\, \pi_\lambda^{(k,\ell)}(w). \tag{5.21}$$

Here, the *Markov weights* $s_\lambda^{(k,\ell)}$ are Schur functions given explicitly by

$$s_\lambda^{(k,\ell)} = \frac{1}{[k]_\ell^n} \prod_{(i,j)\in\lambda} \frac{[j-i+k]_\ell}{[h(i,j)]_\ell} \tag{5.22}$$

for each $\lambda \in \Lambda_n^{(k,\ell)}$ and $h(i,j)$ denotes the *hook length* of the box with row-column coordinates (i,j) in λ. For each $\lambda \in \Lambda_n^{(k,\ell)}$, if we write $d_\lambda^{(k,\ell)}$ for the dimension of $V_\lambda^{(k,\ell)}$, we may evaluate (5.21) at the identity $1_n \in H_n(q)$ to obtain the following formula relating the Markov weights and the dimensions of the irreps:

$$\sum_{\lambda \in \Lambda_n^{(k,\ell)}} s_\lambda^{(k,\ell)} d_\lambda^{(k,\ell)} = \mathrm{tr}_{k\ell}(1_n) = 1. \tag{5.23}$$

We are now equipped to verify the bound on the HOMFLYPT given at the end of Section 2. Indeed, by unitarity we may combine (5.20), (5.21) and (5.23) to obtain, for each $b \in B_n$,

$$\begin{aligned}
\left| H_b^{(k)}(e^{2\pi i/\ell}) \right| &= [k]_\ell^{n-1} \left| \sum_{\lambda \in \Lambda_n^{(k,\ell)}} s_\lambda^{(k,\ell)} \, \mathrm{Tr}\, \pi_\lambda^{(k,\ell)}(b) \right| \\
&\leq [k]_\ell^{n-1} \sum_{\lambda \in \Lambda_n^{(k,\ell)}} s_\lambda^{(k,\ell)} d_\lambda^{(k,\ell)} \\
&= [k]_\ell^{n-1}. \tag{5.24}
\end{aligned}$$

Specializing to $k = 2$, we can obtain a more explicit formula for the Jones polynomial. The appropriate Markov weights $s_{[\lambda_1,\lambda_2]}^{(2,\ell)}$ when $\lambda_1 + \lambda_2 = n$ can be computed as follows. By Lemma 3.5(b) of [38], if λ' is the $(2,\ell)$-diagram obtained by adding r columns of two boxes to the left of another $(2,\ell)$-diagram λ, it follows that $s_{\lambda'}^{(2,\ell)} = [2]_\ell^{-2r} s_\lambda^{(2,\ell)}$. A direct computation from the hook length formula (5.22) gives the Markov weight for a single row diagram $[m]$ as

$$s_{[m]}^{(2,\ell)} = \frac{1}{[2]_\ell^m} \frac{[2]_\ell [3]_\ell \cdots [m+1]_\ell}{[1]_\ell [2]_\ell \cdots [m]_\ell} = \frac{[m+1]_\ell}{[2]_\ell^m}.$$

Since $\lambda = [\lambda_1, \lambda_2]$ can be obtained by adding λ_2 columns of two boxes to the left of the row diagram $[\lambda_1 - \lambda_2]$, it follows that

$$s_\lambda^{(2,\ell)} = \frac{s_{[\lambda_1 - \lambda_2]}^{(2,\ell)}}{[2]_\ell^{2\lambda_2}} = \frac{[\lambda_1 - \lambda_2 + 1]_\ell}{[2]_\ell^{\lambda_1 + \lambda_2}} = \frac{[\lambda_1 - \lambda_2 + 1]_\ell}{[2]_\ell^n}.$$

Plugging into (5.19) thus leads to the following expression for the evaluation at $q = e^{2\pi i/\ell}$ of the Jones polynomial of the trace closure of a braid $b \in B_n$:

$$\begin{aligned} J_{\hat{b}}(e^{2\pi i/\ell}) &= \overline{\mathrm{tr}}_{2\ell}(b) \\ &= \frac{1}{[2]_\ell} q^{-\frac{3}{2}e(b)} \sum_{\lambda \in \Lambda_n^{(2,\ell)}} [\lambda_1 - \lambda_2 + 1]_\ell \, \mathrm{Tr}\, \pi_\lambda^{(2,\ell)}(b) \end{aligned}$$

$$(5.25)$$

Because the numerator of the coefficient in front is just a complex phase, the absolute value of the Jones polynomial is

$$\left| J_{\hat{b}}(e^{2\pi i/\ell}) \right| = \left| \overline{\mathrm{tr}}_{2\ell}(b) \right| = \frac{1}{[2]_\ell} \left| \sum_{\lambda \in \Lambda_n^{(2,\ell)}} [\lambda_1 - \lambda_2 + 1]_\ell \, \mathrm{Tr}\, \pi_\lambda^{(2,\ell)}(b) \right|. \qquad (5.26)$$

Jones polynomial of generalized closure from the Temperley-Lieb algebra

Here we obtain representation-theoretic formulae for the Jones polynomial of the generalized closure of a braid. For this, we need to briefly describe the connection between the Jones polynomial and the Temperley-Lieb algebra.

The Temperley-Lieb algebra

As we have described in the previous subsection, the representations corresponding to the case $k = 2$ are all that is relevant for the Jones polynomial. In these cases, it is known that the representation matrices satisfy $\pi^{(2,\ell)}(e_i e_{i+1} e_i - \tau e_i) = 0$, where $\tau = [2]_\ell^{-2}$. This can be shown using the fact that each of the q-deformed three-row anti-symmetrizers

$$1 - q^{-1}(g_i + g_{i+1}) + q^{-2}(g_i g_{i+1} + g_{i+1} g_i) - q^{-3} g_i g_{i+1} g_i$$

vanishes on representations with fewer than three rows (the proof is similar to the well-known undeformed case at $q = 1$, where there can exist no totally antisymmetric state of three qubits). The quotient of the Hecke algebra by the relations $e_i e_{i+1} e_i = \tau e_i$ yields the Temperley-Lieb algebra $TL_n(\tau)$ which is generated by 1 and idempotents $\{e_1, \ldots, e_{n-1}\}$ satisfying

$$\begin{aligned} e_i^2 &= e_i & &(5.27) \\ e_i e_j e_i &= \tau e_i & |i - j| = 1 & \quad (5.28) \\ e_i e_j &= e_j e_i & |i - j| > 1. & \quad (5.29) \end{aligned}$$

Temperley-Lieb algebra is advantageous because it provides representations of the *diagram monoid* K_n [21], defined as follows. For each $1 \le i \le n - 1$, define the "cup-cap" diagram

$$\omega_i = \left| \cdots \right| \underset{\frown}{\overset{\smile}{\times}} \left| \cdots \right|,$$

where the cup-caps act on strands i and $i + 1$. Multiplication of cup-caps is performed pictorially (up to isotopy), amounting to stacking the generators ω_i in the same way as with the generators of B_n. Then, K_n is generated by the cup-cap generators $\{\omega_1, \ldots, \omega_{n-1}\}$, together with an extra closed-loop diagram δ, which satisfy the relations

$$
\begin{aligned}
\omega_i^2 &= \delta\omega_i & & & (5.30) \\
\omega_i\omega_j\omega_i &= \omega_i & |i - j| = 1 & & (5.31) \\
\omega_i\omega_j &= \omega_j\omega_i & |i - j| > 1. & & (5.32)
\end{aligned}
$$

These relations are perhaps best understood in terms of pictures which we invite the reader to draw, or otherwise to consult Figure 8 of [21]. While these relations are similar to those used above to define the Temperley-Lieb algebra, a more transparent connection is obtained by reformulating (5.27)–(5.29) in terms of the scaled projections $E_i \equiv [2]_\ell e_i$, in which case the corresponding relations

$$
\begin{aligned}
E_i^2 &= [2]_\ell E_i & & & (5.33) \\
E_i E_j E_i &= E_i & |i - j| = 1 & & (5.34) \\
E_i E_j &= E_j E_i & |i - j| > 1 & & (5.35)
\end{aligned}
$$

are formally identical to (5.30)–(5.32). The diagram monoid K_n is then represented inside $TL_n(\tau)$ via the map taking $\omega_i \mapsto E_i$ and $\delta \mapsto [2]_\ell$. As with B_n, we use this map to obtain representations of K_n from those of $TL_n(\tau)$ by setting

$$
\pi_\lambda^{(2,\ell)}(\omega_i) = \pi_\lambda^{(2,\ell)}(E_i) = [2]_\ell \pi_\lambda^{(2,\ell)}(e_i).
$$

For every even number $2p$, define the rectangular tableau $t_{2p} \in T_{[p,p]}$ by

$$
t_{2n} = \begin{array}{|c|c|c|c|c|}
\hline
1 & 3 & 5 & \cdots & 2p-1 \\
\hline
2 & 4 & 6 & & 2p \\
\hline
\end{array}. \tag{5.36}
$$

We slightly abuse notation and write the projection onto the corresponding vector $|t_{2n}\rangle$ as $t_{2p} \equiv |t_{2p}\rangle\langle t_{2p}|$. We pause to mention a convention; given any $t \in T_{[p,p]}^{(2,\ell)}$ and $t' \in T_\lambda^{(2,\ell)}$, let tt' be the tableau of shape $[p + \lambda_1, p + \lambda_2]$ obtained by adding $2p$ to each box of t' and placing it to the right of t. It is easily checked that $tt' \in T_{[p+\lambda_1, p+\lambda_2]}^{(2,\ell)}$. This defines a natural embedding of vector spaces $V_{[p,p]} \otimes V_\lambda \hookrightarrow V_{[p+\lambda_1, p+\lambda_2]}$ which we denote $|t\rangle|t'\rangle \mapsto |tt\rangle$. Throughout, we freely make this identification on vectors and operators. Now consider the following lemma.

Lemma 5.1 *Let p and n be positive integers satisfying $2p \leq n$. If $\lambda = [\lambda_1, \lambda_2] \in \Lambda_n^{(2,\ell)}$, then*

$$
\pi_\lambda^{(2,\ell)}(\omega_1\omega_3\cdots\omega_{2p-1}) = \begin{cases} [2]_\ell^p \, t_{2p} \otimes 1_{[\lambda_1-p, \lambda_2-p]} & \text{if } \lambda_2 \geq p \\ 0 & \text{otherwise.} \end{cases}
$$

Proof: Abbreviating $e_i = \pi_n^{(2,\ell)}(e_i)$, recall that $e_j|t\rangle = |t\rangle$ iff j and $j + 1$ are in the same column, while $e_j|t\rangle = 0$ iff j and $j + 1$ are in the same row. Because the e_{2i-1} are mutually commuting, if $2i - 1$ and $2i$ are in the same row of a given tableau for some $1 \leq i \leq p$, $|t\rangle$ is annihilated by $e_1 e_3 \cdots e_{2p-1}$, and thus also by $\omega_1\omega_3\cdots\omega_{2p-1}$. Therefore, only vectors $|t\rangle$ for

which $t = t_{2n}t'$ for some $t' \in T^{(2,\ell)}_{[\lambda_1-p,\lambda_2-p]}$ survive. Clearly this is impossible if $\lambda_2 < p$. On the other hand, for $1 \le i \le p$ the e_{2i-1}, and therefore the ω_{2i-1}, may only act nontrivially on the leftmost p columns of any given tableau. By the convention mentioned above, this means that when $\lambda_2 \ge p$, the quantity in the lemma is proportional to the tensor product of the rank 1 projector t_{2p} with an identity matrix as required. $\square$

It is possible to combine B_n and K_n into a unified structure which was called a *braid monoid* by Kauffman [21]. As this braid monoid contains diagrams consisting of both cup-caps and twists, its generators are the union of those of B_n and K_n. However, there are considerably more relations that these generators must satisfy (see e.g. [6]) in addition to those of the braid group and diagram monoid. For our purposes, however, we will not need the full braid monoid. Instead, we shall only need to consider such generalized braids of the form bw, where $b \in B_n$ and $w \in K_n$ is a word in the ω_i's, in which case $\pi^{(2,\ell)}_n(bw) = \pi^{(2,\ell)}_n(b)\pi^{(2,\ell)}_n(w)$.

Jones polynomial of the generalized closures

For any braid $b \in B_n$, we give a formula for the absolute value of the Jones polynomial of the generalized closure of b when $x = y = 1_n \in B_n$. Such a closure then depends only the parameters p and r which satisfy $2p + r = n$. We obtain this formula by computing the normalized Markov trace of the braid b with p cup-caps at the tops of the leftmost $2p$ strands. The formula is

$$
\begin{aligned}
\left|J\big(\chi^{p,r}_{1,1}(b), e^{2\pi i/\ell}\big)\right| &= \left|\overline{\mathrm{tr}}_{2\ell}(b\omega_1\omega_3\cdots\omega_{2p-1})\right| \\
&= \frac{1}{[2]_\ell}\left|\sum_{\lambda\in\Lambda^{(2,\ell)}_n}[\lambda_1-\lambda_2+1]_\ell\,\mathrm{Tr}\left(\pi^{(2,\ell)}_\lambda(b)\pi^{(2,\ell)}_\lambda(\omega_1\omega_3\cdots\omega_{2p-1})\right)\right| \\
&= [2]^{p-1}_\ell\left|\sum_{\lambda\in\Lambda^{(2,\ell)}_n:\lambda_2\ge p}[\lambda_1-\lambda_2+1]_\ell\,\mathrm{Tr}\left(\pi^{(2,\ell)}_\lambda(b)(t_{2p}\otimes 1_{\lambda-[p,p]})\right)\right| \\
&= [2]^{p-1}_\ell\left|\sum_{\mu\in\Lambda^{(2,\ell)}_r}[\mu_1-\mu_2+1]_\ell\,\mathrm{Tr}\left(\pi^{(2,\ell)}_{[p,p]+\mu}(b)(t_{2p}\otimes 1_\mu)\right)\right|, \qquad (5.37)
\end{aligned}
$$

In the second line, we have used the formula (5.26) for the absolute value of the normalized Markov trace. The third line is by Lemma 5.1, while the last line is straightforward.

We remark here that this expression yields an immediate upper bound on the absolute value of the Jones polynomial of a link obtained as a generalized closure of a braid. By unitarity, it is clear that the matrix traces above are maximized when the formula is evaluated at the identity braid $1_n \in B_n$. In this case, we obtain

$$
\begin{aligned}
\left|J\big(\chi^{p,r}_{1,1}(1_n), e^{2\pi i/\ell}\big)\right| &= [2]^{p-1}_\ell\sum_{\mu\in\Lambda^{(2,\ell)}_r}[\mu_1-\mu_2+1]_\ell\,d^{(2,\ell)}_\mu \\
&= [2]^{p-1}_\ell\sum_{\mu\in\Lambda^{(2,\ell)}_r}[2]^r_\ell\,s^{(2,\ell)}_\mu\,d^{(2,\ell)}_\mu \\
&= [2]^{p+r-1}_\ell, \qquad (5.38)
\end{aligned}
$$

where we have used (5.23) for the last step. By specializing (5.37) to the case where $r = 0$ and $p = n$, we obtain the following formula for the Jones polynomial of the plat closure of $b \in B_{2n}$:

$$
\begin{aligned}
\left| J(\widetilde{b}, e^{i2\pi/\ell}) \right| &= [2]_\ell^{n-1} \left| \mathrm{Tr}\left(\pi_{[n,n]}^{(2,\ell)}(b)\, t_{2n} \right) \right| \\
&= [2]_\ell^{n-1} \left| \langle t_{2n} | \pi_{[n,n]}^{(2,\ell)}(b) | t_{2n} \rangle \right|.
\end{aligned}
\tag{5.39}
$$

6   Algorithms for approximating the Jones and HOMFLYPT polynomials

In this section, we use the circuits of Section 4 to give quantum algorithms for approximately evaluating, in the sense described in Section 2, the Jones and one-variable HOMFLYPT polynomials at primitive roots of unity. In particular, the results of this section constitute a proof of Theorem 2.1. We begin by giving a quantum algorithm which obtains an additive approximation of the one-variable HOMFLYPT polynomials $H^{(k)}$ of the trace closure of a braid, generalizing the Jones polynomial algorithm of [2]. If k is a fixed constant, this algorithm runs in time polynomial in the length of the braid. Then, we sketch two complementary ways in which this algorithm can be generalized to approximate the absolute value of the Jones polynomial of any generalized closure of a braid.

Approximating the HOMFLYPT of the trace closure

Recall the setup of Problem 2.1. We are given a length-m braid $b \in B_n$, positive integers k, ℓ satisfying $2 \le k < \ell$, and a number $\delta > 0$. We assume that k is a fixed constant. Because a length m braid can act nontrivially on at most $2m$ strands, we lose no generality in assuming that $n \le 2m$. We showed in (5.24) that the maximal value of $\left| H_{\widehat{b}}^{(k)}(e^{2\pi i/\ell}) \right|$ over all $b \in B_n$ is $[k]_\ell^{n-1}$. We therefore focus on estimating the following normalized version of the one-variable HOMFLYPT which, by (5.20) and (5.21), has the following expression for $b \in B_n$:

$$
\begin{aligned}
\frac{1}{[k]_\ell^{n-1}} H_{\widehat{b}}^{(k)}(e^{2\pi i/\ell}) &= q^{\frac{k-1}{2}e(b)}\, \mathrm{tr}_{k,\ell}(b) \\
&= e^{\frac{2\pi i(k-1)e(b)}{2\ell}} \sum_{\lambda \in \Lambda_n^{(k,\ell)}} s_\lambda^{(k,\ell)}\, \mathrm{Tr}\, \pi_\lambda^{(k,\ell)}(b).
\end{aligned}
$$

The Markov weights $s_\lambda^{(k,\ell)}$ are defined in (5.22). We sample from a complex-valued random variable with the above expectation by a procedure similar to that of [2]. First observe that by (5.23), the numbers $\left\{ P_\lambda = s_\lambda^{(k,\ell)} d_\lambda^{(k,\ell)} : \lambda \in \Lambda_n^{(k,\ell)} \right\}$ are probabilities. Because k is constant, the number of weights grows polynomially with n, so choosing a $\lambda \in \Lambda_n^{(k,\ell)}$ with probability P_λ can be done efficiently because those probabilities can be precomputed and sampled from by a standard procedure. Second, note that given $\lambda \in \Lambda_n^{(k,\ell)}$, there is an efficient procedure for choosing a path $t \in T_\lambda^{(k,\ell)}$ uniformly at random. This is because the Young graph $\Lambda_{0,n}^{(k,\ell)}$ is a layered graph, with a polynomial number of diagrams $\le \left(\min\{n, \ell - k\} + 1 \right)^k$ in each layer. Therefore, the number of paths from $\emptyset$ to a given node in the diagram can be computed in advance. To choose a path ending in a particular diagram $\lambda \in \Lambda_n^{(k,\ell)}$, the trick is to move in reverse; starting at λ, choose the next diagram $\lambda' \in \Lambda_{n-1}^{(k,\ell)}$ with a probability proportional to the number of paths from $\emptyset$ to λ', divided by the total number of paths from $\emptyset$ ending in the $n-1$'st layer.

The algorithm proceeds as follows. One first chooses a tableau $t \in T_n^{(k,\ell)}$ randomly as above. Next, one samples from random variables $X, Y \in \{\pm 1\}$ with conditional expectations satisfying

$$\mathbb{E}[X + iY | \lambda, t] = \langle t | \pi_\lambda^{(k,\ell)}(b) | t \rangle.$$

This can be done efficiently using the quantum circuits for the Jones-Wenzl representation described in Section 4, together with the following standard lemma which we prove in the appendix for convenience:

Lemma 6.1 (Sampling Lemma) *Let U be a quantum circuit of length $O\big(\mathrm{poly}(n)\big)$ acting on n qubits, and let $|\psi\rangle$ be a pure state of the n qubits which can be prepared in time $O\big(\mathrm{poly}(n)\big)$. It is then possible to sample from random variables $X, Y \in \{\pm 1\}$ for which*

$$\mathbb{E}[X + iY] = \langle \psi | U | \psi \rangle$$

in $O\big(\mathrm{poly}(n)\big)$ time.

This process is repeated, averaging the values of X and Y, until the desired precision is met. The nonconditional expected value of $X + iY$ is

$$
\begin{aligned}
\mathbb{E}[X + iY] &= \sum_{\lambda \in \Lambda_n^{(k,\ell)}} \frac{P_\lambda}{d_\lambda^{(k,\ell)}} \sum_{t \in T_\lambda^{(k,\ell)}} \mathbb{E}[X + iY | \lambda, t] \\
&= \sum_{\lambda \in \Lambda_n^{(k,\ell)}} s_\lambda^{(k,\ell)} \sum_{t \in T_\lambda^{(k,\ell)}} \langle t | \pi_\lambda^{(k,\ell)}(b) | t \rangle \\
&= \sum_{\lambda \in \Lambda_n^{(2,\ell)}} s_\lambda^{(k,\ell)} \, \mathrm{Tr} \, \pi_\lambda^{(k,\ell)}(b).
\end{aligned}
$$

Therefore

$$e^{\frac{2\pi i (k-1)e(b)}{2\ell}} \mathbb{E}\big[X + iY\big] = \frac{1}{[k]_\ell^{n-1}} H_{\widehat{b}}^{(k)}(e^{2\pi i/\ell}),$$

so a sufficiently good estimate of $\mathbb{E}\big[X + iY\big]$ provides the needed estimate of the normalized one-variable HOMFLYPT polynomial. By the following lemma, we will see that the above procedure only needs to be repeated polynomially many times to obtain the desired estimate.

Lemma 6.2 (Chernoff Bound) *Let $\{X_1, \ldots, X_M\}$ be real-valued random variables satisfying $|X_j| \le 1$ and $\mathbb{E}\, X_j = \mu$. Then*

$$\mathrm{Pr}\left\{ \left| \frac{1}{M} \sum_{j=1}^{M} X_j - \mu \right| > \delta \right\} \le 2\exp\left(-\frac{M\delta^2}{4} \right).$$

Suppose the above algorithm is run M times, obtaining random variables $\{X_j, Y_j\}_{j=1}^{M}$. Setting $Z_j = X_j + iY_j$, the union bound and the above lemma imply

$$
\mathrm{Pr}\left\{ \left| \frac{1}{M} \sum_{j=1}^{M} Z_j - \mathbb{E}Z_1 \right| > \delta \right\} \le \mathrm{Pr}\left\{ \left| \frac{1}{M} \sum_{j=1}^{M} X_j - \mathbb{E}X_1 \right| > \frac{\delta}{\sqrt{2}} \right\} + \mathrm{Pr}\left\{ \left| \frac{1}{M} \sum_{j=1}^{M} Y_j - \mathbb{E}Y_1 \right| > \frac{\delta}{\sqrt{2}} \right\}
$$

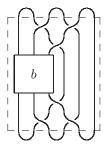$$\le 4\exp\left(-\frac{M\delta^2}{8} \right).$$

Fig. 6.1.   The trace closure of $b \in B_3$ is isotopic to the plat closure of the modified braid $(\sigma_3^5 \sigma_2^3)^{-1} b \sigma_3^5 \sigma_2^3 = \sigma_2^{-1} \sigma_4^{-1} \sigma_3^{-1} b \sigma_3 \sigma_4 \sigma_2$. Note that we identify b with its image $\iota \circ \iota \circ \iota(b) \in B_6$.

Thus, for any $\delta > 0$, the probability that $Z \equiv e^{\frac{2\pi i (k-1) e(b)}{2\ell}} \frac{1}{M} \sum Z_j$ deviates from the desired value of the normalized one-variable HOMFLYPT polynomial by more than δ is smaller than the desired error of $1/4$, provided that the number of samples satisfies $M > 32 \ln(2)/\delta^2$. Since each sample is obtained in $O\big(\mathrm{poly}(m)\big)$ time, the desired additive approximation is obtained in $O\big(\mathrm{poly}(m, 1/\delta)\big)$ time as required.

Approximating the Jones polynomial of generalized closures

In this section we show how to approximate the absolute value of the Jones polynomial of generalized closures of a braid. As mentioned in Section 2, we focus on the absolute value because there is no unambiguous way to assign an orientation to a generalized closure. Recall the setup for Problem 2.2. We are given a length-m braid $b \in B_n$, two nonnegative integers p, r for which $2p + r = n$ and a positive integer ℓ. We lose no generality in assuming that the top and bottom braids which define the generalized closure are $x, y = 1_n$. As we showed in (5.38), the largest absolute value of the Jones polynomial is obtained when the closure yields $p + r$ trivial knots. Therefore we focus on estimating the normalized quantity

$$\frac{1}{[2]_\ell^{p+r-1}} \left| J\big(\xi_{1,1}^{p,r}(b), e^{2\pi i/\ell}\big) \right|.$$

We show two different ways of achieving this goal, as each constitutes a different generalization of the previous algorithm which is interesting in its own right. The first makes use of the following proposition [19], which shows that the generalized closure $\xi^{p,r}(b)$ can be written as the plat closure of a related braid on $2p + 2r$ strands.

Proposition 6.3 *Let $b \in B_{2p+r}$. Then $\xi_{1,1}^{p,r}(b) = \widetilde{c^{-1}bc}$, where $c = \sigma_{2p+r}^{2p+2r-1} \cdots \sigma_{2p+3}^{2p+5} \sigma_{2p+2}^{2p+3}$ and for $i < j$, we write $\sigma_i^j = \sigma_i \sigma_{i+1} \cdots \sigma_{j-2} \sigma_{j-1}$ for the braid where strand j is moved above its neighboring strands on the left and is inserted in position i.*

While we invite the reader to verify this, the main idea is contained in Figure 6.1, where we illustrate how the trace closure can be obtained from the plat closure. Note that since the braid c in the proposition consists of $\sum_{i=1}^{t-1} i = O(t^2)$ generators, the modified braid $b' \equiv c^{-1}bc$ is at most polynomially longer than b itself. Setting $p' = p + r$, observe that since $b' \in B_{2p'}$,

(5.39) implies that

$$
\begin{aligned}
\frac{1}{[2]_\ell^{p+r-1}} \left| J\big(\xi_{1,1}^{p,r}(b), e^{2\pi i/\ell}\big) \right| &= \frac{1}{[2]_\ell^{p'-1}} \left| J\big(\widetilde{b'}, e^{2\pi i/\ell}\big) \right| \\
&= \left| \langle t_{2p'} | \pi_{[p',p']}^{(2,\ell)}(b') | t_{2p'} \rangle \right|.
\end{aligned}
$$

In the same manner as with the HOMFLYPT, one then samples from a complex random variable Z satisfying $\mathbb{E}Z = \langle t_{2p'} | \pi_{[p',p']}^{(2,\ell)}(b') | t_{2p'} \rangle$. After averaging the results a suitable number of times, the absolute value of the average is reported. We omit the details as they are identical to the former case.

Another procedure for this task makes direct use of the following representation-theoretic formula for the absolute value of the Jones polynomial:

$$
\begin{aligned}
\frac{1}{[2]_\ell^{p+r-1}} \left| J\big(\xi_{1,1}^{p,r}(b), e^{2\pi i/\ell}\big) \right| &= \frac{[2]_\ell^{p-1}}{[2]_\ell^{p+r-1}} \left| \sum_{\lambda \in \Lambda_r^{(2,\ell)}} [\lambda_1 - \lambda_2 + 1]_\ell \operatorname{Tr}\left(\pi_{[p,p]+\lambda}^{(2,\ell)}(b)(t_{2p} \otimes 1_\lambda) \right) \right| \\
&= \frac{1}{[2]_\ell^r} \left| \sum_{\lambda \in \Lambda_r^{(2,\ell)}} [\lambda_1 - \lambda_2 + 1]_\ell \operatorname{Tr}\left(\pi_{[p,p]+\lambda}^{(2,\ell)}(b)(t_{2p} \otimes 1_\lambda) \right) \right|. \quad (6.1)
\end{aligned}
$$

Recall that by (5.23), the numbers $\left\{ P_\lambda = s_\lambda^{(2,\ell)} d_\lambda^{(2,\ell)} : \lambda \in \Lambda_r^{(2,\ell)} \right\}$ sum to unity and thus define probabilities. The algorithm proceeds as in [2] by first selecting an irrep $\lambda \in \Lambda_r^{(2,\ell)}$ at random with probability $P_\lambda \equiv s_\lambda^{(2,\ell)} d_\lambda^{(2,\ell)}$. Then, a path t in the Young graph $\Lambda_\lambda^{(2,\ell)}$ is chosen uniformly at random. By the same arguments as in the HOMFLYPT case, one may then sample from random variables $X, Y \in \{\pm 1\}$ with conditional expectations satisfying

$$
\mathbb{E}[X + iY | \lambda, t] = \langle t_{2p} | \langle t | \pi_{[p,p]+\lambda}^{(2,\ell)}(b) | t_{2p} \rangle | t \rangle.
$$

This procedure is then repeated, averaging the results until the desired precision is attained, after which the absolute value is reported. Using (6.1), it is straightforward to show that

$$
\left| \mathbb{E}[X + iY] \right| = \frac{1}{[2]_\ell^{p+r-1}} \left| J\big(\xi_{1,1}^{p,r}(b), e^{2\pi i/\ell}\big) \right|.
$$

The remainder of the proof is identical to the HOMFLYPT situation.

7 Simulating quantum circuits with braids

In this section, we show how to "compile" any quantum circuit on n qubits consisting of m two-qubit gates into a description of a braid on $4n$ strands with $\operatorname{poly}(m)$ crossings in such a way that the output of the circuit is encoded into an evaluation of the Jones polynomial of the plat closure of the braid at any primitive ℓ'th root of unity with $\ell \geq 5, \ell \neq 6$. While this was first proved in [12], our proof is simpler as it only uses the representation of B_8 corresponding to the rectangular diagram ▦.

There are uncountably many quantum circuits on n qubits, but countably many braids. Therefore, we will have to settle for approximations of quantum circuits. Given unitaries U and U' and some $0 \leq \epsilon \leq 1$, we say that U *ϵ-approximates* U' if $\|U - U'\|_\infty \leq \epsilon$, where for a square matrix M, $\|M\|_\infty$ denotes the *operator norm*, or largest singular value of M. Our main goal in this section will be to prove the following:

Theorem 7.1 *Let $U = U_m U_{m-1} \cdots U_1$ be a quantum circuit of length m acting on n qubits and let $\epsilon = \Omega\big(2^{-\mathrm{poly}(n)}\big)$. Then there is a braid $b \in B_{4n}$ with $O\big(\mathrm{poly}(m)\big)$ crossings such that U is ϵ-approximated by $\pi^{(2,\ell)}_{[2n,2n]}(b)$. In this case, the following inequality holds:*

$$\left| |\langle 00 \cdots 0|U|00 \cdots 0\rangle|^2 - \frac{1}{[2]^{2n-1}_\ell} \left| J\big(\widetilde{b}, e^{2\pi i/l}\big) \right|^2 \right| \leq \epsilon. \tag{7.1}$$

Moreover, such a braid can be found from a description of the circuit in $O\big(\mathrm{poly}(m)\big)$ time on a classical computer.

To prove Theorem 7.1 we must first introduce some machinery. A finite set of gates in $U(\mathcal{H})$ is said to be *universal* if it generates a dense subset of $U(\mathcal{H})$. The following lemma implies that the measurement probabilities of an ϵ-approximation of a quantum circuit differ by at most ϵ from those of the desired circuit. The proof is in the appendix.

Lemma 7.2 *Let U and U' be $d \times d$ unitaries for which U' ϵ-approximates U, where $\epsilon \leq 1$. Then, for every pair of normalized pure states $|\phi\rangle, |\psi\rangle \in \mathbb{C}^d$, we have*

$$\left| |\langle \phi|U|\psi\rangle|^2 - |\langle \phi|U'|\psi\rangle|^2 \right| \leq \epsilon.$$

The next theorem assures that universal sets of unitaries suffice to efficiently ϵ-approximate an arbitrary quantum circuit.

Theorem 7.3 (Solovay-Kitaev) *Let $\mathcal{G} \subset U(d)$ be a finite universal set of unitaries on a Hilbert space of constant dimension d which are closed under inverses, i.e. $\mathcal{G}^{-1} = \mathcal{G}$. Then any unitary $U \in U(d)$ can be ϵ-approximated by a sequence of $O\big(\mathrm{poly}\log(1/\epsilon)\big)$ gates in $\mathcal{G}$. Moreover, such a sequence can be found by a classical computer in $O\big(\mathrm{poly}\log(1/\epsilon)\big)$ time.*

Fixing any finite, universal set of two-qubit unitaries $\mathcal{G}_2 \subset U(4)$, let $\mathcal{G}_n \subset U(2^n)$ be the set of gates obtained by letting $\mathcal{G}_2$ act on all pairs of neighboring qubits. Given a length m circuit $U_m U_{m-1} \cdots U_1$ consisting of gates from $\mathcal{G}_n$ and any *fixed* desired degree of accuracy ϵ, the Solovay-Kitaev Theorem further implies that for each i, there is an ϵ/m approximation U'_i to U_i which is obtained by a sequence of $O\big(\mathrm{poly}\log(m)\big)$ gates in $\mathcal{G}$, and also that such a sequence can be found in $O\big(\mathrm{poly}\log(m)\big)$ time (since ϵ does not grow with m, it does not figure into the complexity estimate). Observe that for any unitaries U and U', the operator norm is *stable*, meaning that $\|U - U'\|_\infty = \|U \otimes 1_d - U' \otimes 1_d\|_\infty$ for every finite dimension d. Therefore, the same approximations hold for the embeddings of the local gates into $U(2^n)$. By a telescoping sum and the triangle inequality, we have

$$\|U_m \cdots U_2 U_1 - U'_m \cdots U'_2 U'_1\|_\infty \leq \sum_{i=1}^m \|U_i - U'_i\|_\infty. \tag{7.2}$$

Therefore, there is an ϵ-approximation to the desired circuit which uses $O\big(m\,\mathrm{poly}\log(m)\big)$ gates from $\mathcal{G}_n$. So we see that working with finite universal sets of gates is just as good as working with all possible two-qubit unitaries, provided that one can live with bounded errors and polylogarithmically more gates. In Section 8, we define classes of quantum computational problems which are insensitive to these limitations.

Throughout this section, we fix an $\ell \geq 5, \ell \neq 6$ and for each diagram λ, we abbreviate $\pi_\lambda \equiv \pi^{(2,\ell)}_\lambda$ and $V_\lambda = V^{(2,\ell)}_\lambda$. We begin by describing how to encode a single logical qubit into
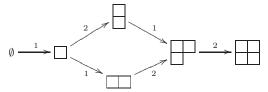
Fig. 7.1. Qubit path basis for W_1. The upper path corresponds to the basis state $|t_0\rangle$, the lower path to $|t_1\rangle$.

$V_{\boxplus}$. This is a two-dimensional representation of B_4 with orthonormal basis

$$|t_0\rangle \equiv \left| \begin{smallmatrix} 1 & 3 \\ 2 & 4 \end{smallmatrix} \right\rangle \qquad\qquad |t_1\rangle \equiv \left| \begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix} \right\rangle.$$

These basis states may also be viewed as paths in the Young graph (see Figure 7.1). Let t and t' be $(2,\ell)$-tableaux of respective shapes $[j,j]$ and $[k,k]$. Recall the convention mentioned before Lemma 5.1 where we write tt' for the tableau of shape $[j+k,j+k]$ obtained by adding $2j$ to each box in t' then placing it to the right of t. Central to our proof is that tt' will always be a $(2,\ell)$-tableaux. Recall that this allows us to define a natural embedding of vector spaces $V_{[j,j]} \otimes V_{[k,k]} \hookrightarrow V_{[j+k,j+k]}$ via the mapping $|t\rangle|t'\rangle \mapsto |tt'\rangle$. We encode n qubits into a subspace $W^{(n)}$ of the irreducible representation $V_{[2n,2n]}$ of B_{4n} which is spanned by the 2^n computational basis states $\{|t_{x_1} t_{x_2} \cdots t_{x_n}\rangle : (x_1, x_2, \ldots, x_n) \in \{0,1\}^n\}$. By our embedding the subspace $W^{(n)}$ can be identified with a tensor product $\bigotimes_{i=1}^n W_i$, where for each $1 \le i \le n$, we identify W_i with $V_{\boxplus}$, so that it is spanned by $|t_0\rangle$ and $|t_1\rangle$. In this subspace of $V_{[2n,2n]}$, each consecutive group of four strands is associated to a single qubit in the following way. For each $1 \le j < k \le n-1$, define the subset $\Sigma_j^k = \{\sigma_j, \sigma_{j+1}, \ldots, \sigma_k\}$ of generators of B_n and write $B_j^k \subseteq B_n$ for the subgroup generated by Σ_j^{k-1}. For each $1 \le i \le n-2$, the image of the 8 strand braid group $B_{4(i-1)+1}^{4(i+1)}$ under the representation $\pi_{[2n,2n]}$, when restricted to $W^{(n)}$, acts nontrivially only on the subsystem $W_i \otimes W_{i+1}$. In fact, it rapidly approximates any $U \in SU(W_i \otimes W_{i+1})$. To see this, it suffices to look at the case $i = 1$. Note that $W_1 \otimes W_2 \subset V_{\boxplus}$. The embedding $V_{\boxplus} \otimes V_{\boxplus} \hookrightarrow V_{\boxplus}$ looks like

$$
\begin{aligned}
|t_0\rangle|t_0\rangle &\mapsto \left| \begin{smallmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \end{smallmatrix} \right\rangle \\
|t_0\rangle|t_1\rangle &\mapsto \left| \begin{smallmatrix} 1 & 3 & 5 & 6 \\ 2 & 4 & 7 & 8 \end{smallmatrix} \right\rangle \\
|t_1\rangle|t_0\rangle &\mapsto \left| \begin{smallmatrix} 1 & 2 & 5 & 7 \\ 3 & 4 & 6 & 8 \end{smallmatrix} \right\rangle \\
|t_1\rangle|t_1\rangle &\mapsto \left| \begin{smallmatrix} 1 & 2 & 5 & 6 \\ 3 & 4 & 7 & 8 \end{smallmatrix} \right\rangle.
\end{aligned}
$$

While this proves that $\dim V_{\boxplus} \ge 4$, we mention that its dimension is 13 when $\ell = 5$ and is 14 when $\ell > 6$. So it is clear that $SU(W_1 \otimes W_2) \subset SU(V_{\boxplus})$. Consider now the following proposition.

Proposition 7.4 (Freedman, Larsen, Wang [13]) *Let $\ell \ge 5, \ell \ne 6$. The image of B_8 under $\pi_{\boxplus}^{(2,\ell)}$ is dense in $SU\left(V_{\boxplus}^{(2,\ell)}\right)$.*

With this density result in hand, we are now equipped to prove Theorem 7.1.

Proof of Theorem 7.1: Set $\epsilon' = \epsilon/m = \Omega\left(2^{-m}/m\right)$. Together with the Solovay-Kitaev

Theorem, Proposition 7.4 implies that for each $U' \in SU(W_1 \otimes W_2)$, there is a braid $b \in B_8$ of length $O\big(\mathrm{poly}\log(1/\epsilon')\big) = O\big(\mathrm{poly}(m)\big)$ for which $\pi_{\boxplus}(b)$ ϵ'-approximates U', where we consider U' to be embedded in $SU(V_{\boxplus})$. Note that while some unitaries $\pi_{\boxplus}(\sigma_i)$ will *not* be contained in $SU(W_1 \otimes W_2)$, the construction above ensures that $\pi_{\boxplus}(b)$ can be made arbitrarily close to any $U' \in SU(W_1 \otimes W_2)$.

Because of the four-periodicity of our encoding, the same arguments apply for approximating gates on any other adjacent pair of qubits. Now, let $U = U_m U_{m-1} \cdots U_1$ as in the statement of the theorem. Without loss of generality, we may assume that each U_i has unit determinant. By (7.2), we may conclude that there is a braid $b \in B_{4n}$ of length $O\big(\mathrm{poly}(m)\big)$ for which $\pi_{[2n,2n]}(b)$ ϵ-approximates the circuit U, and also that such a braid can be determined on a classical computer in $O\big(\mathrm{poly}(m)\big)$ time. The rest of the theorem now follows by Lemma 7.2 and the expression (5.39) for the absolute value of the Jones polynomial of the plat closure; the normalization constant $1/[2]_\ell^{2n-1}$ is so because the braid has $4n$ strands. $\square$

8   Complexity-theoretic applications of the Jones polynomial

Complexity theory characterizes the asymptotic consumption of resources, such as time and space, required to obtain the solutions of certain classes of problems on a computer. Writing $\{0,1\}^*$ for the set of all binary strings of finite length, a *decision problem* asks for the evaluation of some function $f \colon \{0,1\}^* \to \{0,1\}$ on an arbitrary input. Such a function determines a *language* $L \subseteq \{0,1\}^*$ defined as $L = f^{-1}(1)$, so equivalently, the task is to determine, for each bit string x^n, whether $x^n \in L$. Examples of languages include the set of all binary strings of even parity and the set of prime numbers, written in binary. A *complexity class* is a collection of computational problems, usually defined in terms of the resources required to determine membership of arbitrarily long bit strings in each language contained in that class. For instance, any class of languages is a complexity class. Two well-known complexity classes are P and NP. The former is defined to contain every language $L \subseteq \{0,1\}^*$ for which there is a uniform family $\big\{C_n \colon \{0,1\}^n \to \{0,1\}\big\}$ of polynomial-size classical circuits (see e.g. [30, 31] for a definition of a classical circuit) for which $C_n(x^n) = 1$ when $x^n \in L$, while $C_n(x^n) = 0$ otherwise. By a *uniform family*, it is meant that there should be a classical algorithm which, given the number n as input, produces a description of the circuit C_n in $O(\mathrm{poly}(n))$-time. We mention that this definition of a uniform family of circuits extends to quantum circuits in the obvious way. NP, on the other hand, contains those languages L for which there is a uniform family of classical circuits $\big\{C_n \colon \{0,1\}^n \times \{0,1\}^m \to \{0,1\}\big\}$, where the number m of *guess bits* grows polynomially with n, so that for each $x^n \in L$, there exists a *witness string*, or *certificate* y^m, so that $C_n(x^n, y^m) = 1$ if $x^n \in L$, while if $x^n \notin L$, $C_n(x^n, y^m) = 0$ for every possible certificate y^m. Below, we will recall the definitions of certain quantum generalizations of these classes, showing how they may be characterized using the Jones polynomial.

The complexity class BQP is defined to contain those decision problems whose solution can be determined with bounded error in polynomial time in the *standard quantum circuit model*. Formally, a language L is in BQP if there exists a uniform family of quantum circuits $\{U_n\}$ of polynomial length such that

$$|\langle x^n 00 \cdots 0 | U_n | x^n 00 \cdots 0\rangle|^2 \begin{cases} \geq 3/4 & \text{if } x^n \in L \\ \leq 1/4 & \text{if } x^n \notin L. \end{cases}$$

This relates the usual definition of BQP, in which a single output qubit is measured to obtain the result of a computation, as follows. Consider a circuit U'_n such that if $x^n \in L$, a measurement of the first qubit of $U'_n|x^n 0 \cdots 0\rangle$ in the computational basis yields 1 with probability $\geq 3/4$ while if $x^n \notin L$, that measurement outcome will be 0 with probability $\geq 3/4$. Appending an additional qubit $|0\rangle^A$ and labeling the output qubit of U'_n as B, we then take

$$U_n = (I^A \otimes U'_n)(\sigma^A_x \otimes |0\rangle\langle0|^B + I^A \otimes |1\rangle\langle1|^B)(I^A \otimes U'^\dagger_n).$$

Note that the Solovay-Kitaev theorem implies that the class BQP remains unchanged if the particular universal gate set chosen for the model merely contains a universal set of gates for each pair of qubits. The following theorem essentially appears in [7]; we prove it in this paper for the sake of completeness.

Theorem 8.0 *Let A be a random oracle which solves* **Approximate Jones Closure** *with $\delta = 1/8$ for the plat closure and some constant $\ell \geq 5, \ell \neq 6$. Then $\mathrm{P}^A = \mathrm{BQP}$. Loosely speaking, this means that* **Approximate Jones Closure** *is "BQP-complete."*

Proof: To begin, it is an immediate consequence of Theorem 2.1 that $\mathrm{P}^A \subseteq \mathrm{BQP}$. To see that $\mathrm{BQP} \subseteq \mathrm{P}^A$, let $L \in \mathrm{BQP}$ and let U be n'th quantum circuit in the uniform family of circuits for L. By definition, U is of length $m = O(\mathrm{poly}(n))$ and acts on $n' = O(\mathrm{poly}(n))$ qubits. For each x^n, define the circuit $W_{x^n} = \bigotimes_{i=1}^n X^{x_i}$, which acts as the identity on the ancillary qubits. Because

$$\langle 00 \cdots 0|W_{x^n} U W_{x^n}|00 \cdots 0\rangle = \langle x^n 00 \cdots 0|U|x^n 00 \cdots 0\rangle,$$

it follows by Theorem 7.1 that for any constant $\epsilon > 0$, there is a braid b of length $O(\mathrm{poly}(m)) = O(\mathrm{poly}(n))$ on $4n'$ strands which satisfies

$$\left| \frac{1}{[2]^{2n'-1}_\ell} \left| J(\widetilde{b}, e^{2\pi i/\ell}) \right|^2 - |\langle x^n 00 \cdots 0|U|x^n 00 \cdots 0\rangle|^2 \right| \leq \epsilon.$$

Moreover, there is an $O(\mathrm{poly}(n))$-time classical algorithm for determining such a braid from a description of $W_{x^n} U W_{x^n}$. By invoking the oracle A, we obtain a random variable Z satisfying

$$\Pr\left\{ \left| Z - \frac{1}{[2]^{2n'-1}_\ell} \left| J(\widetilde{b}, e^{2\pi i/\ell}) \right| \right| < 1/8 \right\} > 3/4.$$

Since $|a^2 - b^2| \leq 2|a - b|$ for $0 \leq a, b \leq 1$, the last two estimates can be combined via the triangle inequality to show that $\left| Z^2 - |\langle x^n 00 \cdots 0|U|x^n 00 \cdots 0\rangle|^2 \right| < 1/4 + \epsilon$ with probability at least $3/4$. Choosing $\epsilon = 1/8$ is sufficient to complete the proof. $\square$

The complexity class QCMA is a certain quantum analog of NP, consisting of those languages L for which a computationally unbounded oracle (generally personified as Merlin) can, with high probability, efficiently convince a computationally bounded verifier (Arthur) that each $x^n \in L$ is actually contained in L. Cheating is also discouraged, in that if $x^n \notin L$, the probability that Merlin will convince Arthur otherwise should be small. Formally, we say that a language L is in QCMA if there is a uniform family of quantum circuits $\{U_n\}$ of polynomial length such that for each length n string $x^n \in L$, there is a length m binary

string y^m for which $P(x^n, y^m) \equiv |\langle x^n y^m 00 \cdots 0 | U_n | x^n y^m 00 \cdots 0 \rangle|^2 \geq 3/4$, while if $x^n \notin L$, we have $P(x^n, y^m) \leq 1/4$ for every such y^m. We remark that the usual definition of QCMA (see e.g. [3] for the original definition) is phrased in terms of measurement probabilities of a single output qubit; by the remarks following the definition above of BQP, the definition we give here is equivalent. For the same reasons as with BQP, the exact value $3/4$ of the success probability is not important; what is important is that the square of the matrix element is *strictly* bounded away from $1/2$.

Given a complexity class C, a problem is said to be C-*hard* if it is at least as hard as any other problem in the class C, in the sense that access to an oracle which immediately computes the solution of that problem allows the solution of any problem in the class C in polynomial-time. If that problem is also contained in the class C, we say that it is C-*complete*. We will show that the following problem is QCMA-complete.

Problem 8.1 (Increase Jones Plat) *Given a braid $b \in B_{2n}$ with $O(\text{poly}(n))$ crossings, a fixed integer $\ell \geq 5$, $\ell \neq 6$, and a class of braids $\mathcal{C}_{2n} \subset B_{2n}$ of length $O(\text{poly}(n))$ for which membership can be decided in $O(\text{poly}(n))$ time on a classical computer, decide, with the promise that only these two cases can occur, whether there exists another braid $c \in \mathcal{C}_{2n}$ for which the absolute value of the normalized Jones polynomial of the plat closure*

$$\frac{1}{[2]_\ell^{n-1}} \left| J(\widetilde{cbc^{-1}}, e^{2\pi i/\ell}) \right|^2 \geq 3/4$$

or if it is $\leq 1/4$ for all braids $c \in \mathcal{C}_{2n}$.

Theorem 8.1 Increase Jones Plat *is* QCMA-*complete.*

Proof: To begin, we demonstrate that **Increase Jones Plat** is in QCMA. Given a braid $b \in B_{2n}$ of length $O(\text{poly}(n))$, Merlin begins by sending Arthur the classical description of the "witness" braid c. Next, Arthur checks to see if $c \in \mathcal{C}_{2n}$, which can be done in polynomial-time by definition. Because of the promise, Arthur only needs to learn the value of

$$\frac{1}{[2]^{n-1}} \left| J(\widetilde{c^{-1}bc}, e^{2\pi i/\ell}) \right|^2$$

with an accuracy of $< 1/2$ with probability $\leq 3/4$. For this, it is sufficient for him to run **Approximate Jones Closure** on a quantum computer with $\delta = 1/4$, which takes $O(\text{poly}(n))$-time.

To see that this problem is QCMA-hard, and is thus QCMA-complete, suppose that $L \in$ QCMA. Let U be the n'th circuit from the uniform family of quantum verifiers for L, and suppose that U acts on n' qubits while accepting witnesses of size m. Letting $\epsilon > 0$ be a constant to be determined at the end of the proof, Arthur precomputes a set of four braids $\mathcal{C}_8 \subset B_8$ which ϵ/m-approximate the circuits $\{X^{y_1} \otimes X^{y_2} : y_1, y_2 \in \{0, 1\}\}$ (obviously, there is nothing to compute when $y_1 = y_2 = 0$). This can be done in polynomial-time. Define $\mathcal{C}_{4n'} \subset B_{4n'}$ to consist of braids which act as the identity everywhere except for the strands $4n+1, \ldots 4n+4m$, where only a single braid from $\mathcal{C}_8$ can act on each group of eight strands $8i+1, \ldots, 8i+8$ within those strands. If we define V_{y^m} in an analogous manner to W_{x^n} in the proof of Theorem 8.0, where it acts only by flipping the witness qubits, it follows by (7.2) that for each braid c in $\mathcal{C}_{4n'}$, the corresponding unitary $\pi^{(2,\ell)}_{[2n',2n']}(c)$ ϵ-approximates V_{y^m} for one and only one y^m (this is because $\|V_{y^m} - V_{z^m}\|_\infty = 2$ whenever $y^m \neq z^m$). Arthur then

tells x^n to Merlin, who sends him a witness braid c from $\mathcal{C}_{4n'}$. Define W_{x^n} as in the proof of Theorem 8.0, except that it acts as the identity on the witness and ancillary qubits. By the first half of Theorem 7.1, Arthur may compute a braid b for which the circuit $W_{x^n} U W_{x^n}$ is ϵ-approximated by $\pi^{(2,\ell)}_{[2n',2n']}(b)$. Therefore, we obtain by (7.2) that $\pi^{(2,\ell)}_{[2n',2n']}(c^{-1}bc)$ is a 3ϵ-approximation of $W_{x^n} V_{y^m} U W_{x^n} V_{y^m}$. Since

$$\langle 00\cdots 0|W_{x^n} V_{y^n} U W_{x^n} V_{y^n}|00\cdots 0\rangle = \langle x^n y^m 00\cdots 0|U|x^n y^m 00\cdots 0\rangle,$$

we may apply the rest of Theorem 7.1 to obtain that

$$\left| \left| \langle x^n y^m 00\cdots 0|U|x^n y^m 00\cdots 0\rangle \right|^2 - \frac{1}{[2]^{2n'-1}} \left| J(\widetilde{c^{-1}bc}, e^{2\pi i/\ell}) \right|^2 \right| \le 3\epsilon.$$

In order to complete the proof, notice that because of the promise, it is sufficient to choose $\epsilon = 1/8$. $\square$

A rather large complexity class is PSPACE, which contains all languages which can be decided using only polynomial space. In [41], PSPACE is characterized as the class of languages which can be decided by applying the same polynomial-size circuit (possibly exponentially) many times. Formally, it is shown there that if $L \in$ PSPACE, then there exists a uniform family of polynomial-size quantum circuits $\{U_n\}$, together with a sequence of polynomial-time computable natural numbers e_n, for which, if $f\colon \{0,1\}^* \to \{0,1\}$ is such that $f^{-1}(1) = L$, then

$$\langle x^n 100\cdots 0|U_n^{e_n}|x^n 100\cdots 0\rangle = f(x^n).$$

Using this characterization, we will show that the following problem is PSPACE-complete.

Problem 8.2 (Approximate Concatenated Jones Plat) *Given a braid $b \in B_{2n}$ with $O\big(\mathrm{poly}(n)\big)$ crossings, a constant ℓ satisfying $\ell \ge 5$, $\ell \neq 6$, and a positive integer e which is describable by $O\big(\mathrm{poly}(n)\big)$ bits, decide, with the promise that only these two cases can occur, whether the squared absolute value of the normalized Jones polynomial of the plat closure of the concatenated braid b^e satisfies*

$$\frac{1}{[2]^{n-1}_\ell} \left| J(\widetilde{b^e}, e^{2\pi i/\ell}) \right|^2 \ge 3/4$$

or if it is $\le 1/4$.

Theorem 8.2 Approximate Concatenated Jones Plat *is* PSPACE-*complete.*

Proof: To see that this problem is PSPACE-hard, choose any language $L \in$ PSPACE, let U be the n'th quantum circuit from its associated uniform family and let $e = O\big(2^{\mathrm{poly}(n)}\big)$ be the corresponding exponent. Suppose that U acts on n' qubits. For a given x^n, we will show how to use an oracle for **Approximate Concatenated Jones Plat** to determine whether or not $x^n \in L$. Define the circuit W_{x^n} as in the proof of Theorem 8.0, except that it also flips the $n+1$st qubit. By choosing $\epsilon = \epsilon'/e = \Omega(2^{-\mathrm{poly}(n)})$ for a constant ϵ' to be determined later, we may obtain, via Theorem 7.1, a braid b with only $O\big(\mathrm{poly}(n)\big)$ crossings such that $\pi^{(2,\ell)}_{[2n',2n']}(b)$ ϵ-approximates $W_{x^n} U W_{x^n}$. Note that

$$f(x^n) = \langle x^n 100\cdots 0|(W_{x^n} U W_{x^n})^e|x^n 100\cdots 0\rangle = \langle 00\cdots 0|W_{x^n} U^e W_{x^n}|00\cdots 0\rangle.$$

Because $\epsilon'/e = \epsilon$, it follows by (7.2) that $\pi^{(2,\ell)}_{[2n',2n']}(b^e)$ ϵ'-approximates the circuit $W_{x^n}U^eW_{x^n}$. Choosing any $\epsilon' < 1/2$ is sufficient to complete the proof of PSPACE-hardness. All that is left to do is to check that this problem is contained in PSPACE as well. First, it is clear that **Approximate Concatenated Jones Plat** is contained in BQPSPACE, as our local qubit implementation of Section 4 requires only polynomial space. On the other hand, Watrous has shown [37] that PSPACE = BQPSPACE, completing the proof. $\square$

Another class of computational tasks is comprised of *counting problems*, which ask, for a given function $f\colon \{0,1\}^* \to \{0,1\}$, "how many $x^n \in \{0,1\}^n$ satisfy $f(x^n) = 1$?" The class #P contains those counting problems arising from a function f for which $f^{-1}(1) \in$ P. We refer the reader seeking more detail to [30] for a more rigorous definition.

Theorem 8.3 *Given a braid $b \in B_{2n}$ with $O(\mathrm{poly}(n))$ crossings and a fixed integer $\ell \geq 5$, $\ell \neq 6$, computing the n most significant bits of the absolute value of the normalized Jones polynomial of the plat closure of b*

$$\frac{1}{[2]_\ell^{n-1}} \left| J(\widetilde{b}, e^{2\pi i/\ell}) \right|$$

is #P-hard.

Proof: Suppose $f\colon \{0,1\}^n \to \{0,1\}$ is computable in polynomial-time on a classical computer. It is well-known (see e.g. [31]), that there is a quantum circuit U, acting on $n' = O(\mathrm{poly}(n))$ qubits, which computes f reversibly and exactly, namely

$$U|x^n\rangle|y\rangle|00\cdots0\rangle = U|x^n\rangle|y \oplus f(x^n) \oplus 1\rangle|00\cdots0\rangle.$$

The state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x^n \in \{0,1\}^n} |x^n\rangle|1\rangle|00\cdots0\rangle$$

can clearly be prepared efficiently. Observe that

$$\langle\psi|U|\psi\rangle \;=\; \frac{1}{2^n}\sum_{x^n}\langle 1|f(x^n)\rangle = \frac{N_1}{2^n},$$

where $N_1 = |f^{-1}(1)|$ is the solution to the #P problem of counting the solutions to f. Let W be the unitary circuit which acts with Hadamard gates on the first n qubits, flips the next qubit, while leaving the rest alone, and set $\epsilon = 4^{-n-2}$. Clearly $W|00\cdots0\rangle = |\psi\rangle$. Since $|a - b| \leq \sqrt{|a^2 - b^2|}$ for $0 \leq a, b \leq 1$, it follows by Theorem 7.1 that, given a description of the circuit $W^{-1}UW$, we may, in polynomial-time, compute a braid b for which

$$\left| |\langle 00\cdots0|W^{-1}UW|00\cdots0\rangle| - \frac{1}{[2]^{2n'-1}} \left| J(\widetilde{b}, e^{2\pi i/\ell}) \right| \right| \leq \sqrt{\epsilon} = 2^{-n-1}.$$

In particular, this means that the n most significant bits of the two terms in the above absolute value agree. Therefore, an oracle which gives the $4n'$ most significant bits of that evaluation of the Jones polynomial can be used to obtain all n bits of the number N_1. $\square$

In fact, n bits is more than enough bits for #P-hardness. Learning just $\Omega(n^\delta)$ of the most significant bits, for any constant $\delta > 0$, is #P-hard as well. This can be seen by padding with

a sufficiently large, but polynomial, number of extra qubits. On the other hand, we will see that learning just the highest order bit of the Jones polynomial is PP-hard.

The complexity class PP, introduced in [15], contains those languages recognized by some uniform family of polynomial-size probabilistic classical circuits with probability greater than $1/2$. Equivalently, L is in PP if there is a nondeterministic polynomial-time machine which accepts $x^n \in L$ on more than half of its paths.

Theorem 8.4 *Given a braid* $b \in B_{2n}$ *with* $O\big(\mathrm{poly}(n)\big)$ *crossings and a fixed positive integer* $\ell \geq 5$, $\ell \neq 6$, *computing the most significant bit of the absolute value of the normalized Jones polynomial of the plat closure of* b

$$\frac{1}{[2]_\ell^{n-1}} \left| J(\widetilde{b}, e^{2\pi i/\ell}) \right|$$

is PP-*hard.*

Proof: The proof follows by exactly the same manner as in the proof of #P-hardness. The only difference is that the most significant bit of the Jones polynomial is sufficient for deciding if the number is solutions is greater than 2^{n-1}. $\square$

9   Conclusions

We showed how to implement the unitary Jones-Wenzl representations of the braid group at a primitive ℓ'th root of unity in polynomial-time on a quantum computer. We constructed the image of each generator using a number of local two-qubit unitaries which was polynomial in the number n of strands, independent of how ℓ grows with n. We then used this model to give algorithms for obtaining additive approximations of one-variable HOMFLYPT polynomials $H^{(k)}$ on a quantum computer. These algorithms run in time which is polynomial in the number of crossings and the inverse of the desired accuracy, independent of how fast ℓ grows with these parameters, provided that k is a constant. While our circuits implementing the Jones-Wenzl representations $\pi^{(k,\ell)}$ are of length $O\big(\mathrm{poly}(n,k)\big)$, it appears that the classical part of our algorithm causes the running time to scale exponentially with k.

Other authors have approached the problem of implementing the Jones representations on a quantum computer. In [22], a representation of the three-strand braid group was given in a qubit architecture. Another approach toward implementing the Jones representations is contained in [35]; however, the final conclusions of that paper rested on an incorrect assumption that unitary matrix elements could be measured precisely in a single time step. Finally, a recent article [14] drew on a connection between topological quantum field theories and spin networks in order to outline a quantum algorithm for approximating the colored Jones polynomial; those authors left as an open question whether their algorithm could be efficiently implemented on a local quantum computer.

On a classical computer, if the number of strands is constant (i.e. not included in the complexity estimate), then the Jones polynomial of the trace closure of a braid with m crossings can be computed exactly by simply multiplying representation matrices of the braid group, requiring time which is polynomial in m. However, accounting for the number of strands, the matrices will be exponentially large in the number n of strands. On a quantum computer, however, multiplication of exponentially large matrices is not a problem, provided

that they are sufficiently "sparse," or rather, that they arise via local unitary transformations of the state space of the quantum computer. On the other hand, there is a sense in which such large unitary matrices are not explicitly observable; an exponential number of queries seem to be required in order to learn the trace of the matrix representing the unitary evolution of a quantum circuit. Nonetheless, the additive approximation of the Jones polynomial we achieved with a quantum algorithm is unobtainable on a classical computer, unless of course BPP $\neq$ BQP.

On the other side of the fence, we have simplified the proof from [12, 13] which shows how to simulate the standard quantum circuit model with braids. By using four strands per qubit, rather than the three of the original proof, we simplified the representation theory dramatically. The four-periodicity of our encoding means that shifting the eight-strand braid which represents a given local unitary on two qubits by a multiple of four strands realizes the same gate on another pair of qubits. The original result of [12] requires consideration of two different cases, depending on whether the first qubit is located at an even or an odd site. Our encoding applies to schemes for topological quantum computation based on the braiding of nonabelian anyons with label $\frac{1}{2}$ in $SU(2)_{\ell-2}$ Chern-Simons field theories with $\ell \geq 5$, $\ell \neq 6$. On the other hand, our local qubit implementation of the Jones-Wenzl representations allows efficient simulation of the braiding of particles with label $\frac{1}{2}$ in $SU(k)_{\ell-k}$ Chern-Simons theories. While slightly less general than the results of [10], as the only mapping class group our methods apply to is the braid group, we have tried to make our presentation accessible to readers who are unfamiliar with the intricacies of topological quantum field theories.

10   Acknowledgments

1. L. Adleman, J. Demarrias, M. A. Huang, "Quantum computability," *SIAM Journal on Computing,* vol. 5, pp. 1524–1540, 1997.
2. D. Aharonov, V. F. R. Jones, Z. Landau, "A Polynomial Quantum Algorithm for Approximating the Jones Polynomial," *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, 2006, `arXiv:quant-ph/0511096`.
3. D. Aharonov, T. Naveh, "Quantum NP – a survey," `arXiv:quant-ph/0210077`.
4. S. Bigelow, "Braid groups and Iwahori-Hecke algebras," `arXiv:math.GT/0505064`.
5. J. Birman, *Braids, Links and Mapping Class Groups,* Princeton University Press, 1974.
6. J. Birman, H. Wenzl, "Braids, link polynomials and a new algebra," *Transactions of the American Mathematical Society,* vol. 313, no. 1, 1989.
7. M. Bordewich, M. Freedman, L. Lovász, D. Welsh, "Approximate counting and quantum computation," *Combinatorics, Probability and Computing*, vol. 14, pp. 737–754, 2005.
8. C. M. Dawson, M. A. Nielsen, "The Solovay-Kitaev algorithm," *Quantum Information and Computation,* vol. 6, no. 1, pp. 80–95, 2006, `arXiv:quant-ph/0505030`.

9. C. M. Dawson, H. L. Haselgrove, A. P. Hines, D. Mortimer, M. A. Nielsen, T. J. Osborne, "Quantum computing and polynomial equations over the finite field $\mathbb{Z}_2$," *Quantum Information and Computation*, vol. 5, no. 2, pp. 102–112, 2005, `arXiv:quant-ph/0408129`.

10. M. H. Freedman, A. Y. Kitaev, M. J. Larsen, "Simulation of topological quantum field theories with quantum computers," *Communications in Mathematical Physics,* vol. 227, no. 3, pp. 605–622, 2002, `arXiv:quant-ph/0001071`.

11. M. H. Freedman, A. Y. Kitaev, M. J. Larsen, Z. Wang, "Topological quantum computation," *Bulletin of the American Mathematical Society*, vol. 40, no. 1, pp. 31–38, 2003.

12. M. H. Freedman, M. J. Larsen, Z. Wang, "A modular functor which is universal for quantum computation," *Communications in Mathematical Physics,* vol. 227, no. 3, pp. 587–603, 2002, `arXiv:quant-ph/0001108`.

13. M. H. Freedman, M. J. Larsen, Z. Wang, "The two-eigenvalue problem and density of Jones representation of braid groups," *Communications in Mathematical Physics,* vol. 228, no. 1, pp. 177–199, 2002, `arXiv:math.GT/0103200`.

14. S. Garnerone, A. Marzuoli, M. Rasetti, "Quantum automata, braid group and link polynomials," `arXiv:quant-ph/0601169`.

15. J. Gill, "Computational complexity of probabilistic Turing machines," *SIAM Journal on Computing,* vol. 6, pp. 675–695, 1977.

16. P. Freyd, D. Yetter, J. Hoste, W. Lickorish, K. Millet, A. Ocneanu, "A new polynomial invariant of knots and links," *Bulletin of the American Mathematical Society*, vol. 12, pp. 239–246, 1985.

17. V. F. R. Jones, "Index for subfactors," *Inventiones Mathematicae*, vol. 72, pp. 1–25, 1983.

18. V. F. R. Jones, "A polynomial invariant for links from Von Neumann algebras," *Bulletin of the American Mathematical Society*, vol. 12, 1985.

19. V. F. R. Jones, "Hecke algebra representations of braid groups and link polynomials," *Annals of Mathematics*, vol. 126, pp. 335–388, 1987.

20. V. F. R. Jones, "The Jones polynomial," *preprint*, 2005.

21. L. H. Kauffman, "State models and the Jones polynomial," *Topology*, vol. 3, no. 26, 395–407, 1987.

22. L. H. Kauffman, "Quantum computing and the Jones polynomial," `arXiv:math.QA/0105255`.

23. S. J. Lomonaco and L. H. Kauffman, "Topological quantum computing and the Jones polynomial," *Proceedings of SPIE.,* vol. SPIE-6244, pp. 247–264, 2006, `arXiv:quant-ph/0605004`.

24. A. Y. Kitaev, "Quantum computations: algorithms and error correction," *Russian Mathematical Surveys,* vol. 52(6), pp. 1191–1249, 1997.

25. W. B. R. Lickorish, *An Introduction to Knot Theory*, Springer-Verlag New York, Inc., 1997.

26. W. Lickorish, K. Millet, "The reversing result for the Jones polynomial," *Pacific Journal of Mathematics*, vol. 124, pp. 173–176, 1987.

27. C. Marriott, J. Watrous, "Quantum Arthur-Merlin Games", *Computational Complexity*, vol. 14 (2), pp. 122–152, 2005, `arXiv:cs.CC/0506068`.

28. K. Murasugi, *Knot Theory and its Applications*, Birkhäuser Boston, 1997.

29. T. Ohtsuki, *Quantum Invariants: A Study of Knots, 3-Manifolds, and Their Sets*, World Scientific Publishing Co. Pte. Ltd., 2002.

30. C. H, Papadimitriou, *Computational Complexity*, Addison-Wesley Publishing Company, Inc., 1994.

31. J. Preskill, unpublished lecture notes.

32. J. H. Przytycki, P. Traczyk, "Invariants of links of Conway type," *Kobe Journal of Mathematics*, vol. 4, no. 2, pp. 115–139, 1988.

33. J.K. Slingerland and F.A. Bais, "Quantum groups and nonabelian braiding in quantum Hall systems", *Nucl.Phys.*, vol. B612, pp. 229-290, 2001, `arXiv:cond-mat/0104035`.

34. Solovay, unpublished.

35. V. Subramaniam, P. Ramadevi, "Quantum computation of Jones' polynomials," `arXiv:quant-ph/0210095`.

36. H. Temperley, E. Lieb, "Relations between the 'percolation' and 'colouring' problem and other graph-theoretical problems associated with regular planar lattices: Some exact results for the 'percolation' problem," *Proceedings of the Royal Society of London A*, vol. 322(1549), pp. 251-280,

1971.

37. J. Watrous, "Relationships between quantum and classical space-bounded complexity classes," *Proc. Thirteenth Annual IEEE Conference on Computational Complexity,* pp. 210–227, 1998.

38. H. Wenzl, "Hecke algebras of type A_n and factors," *Inventiones Mathematicae*, vol. 92, pp. 349–383, 1988.

39. D. J. A. Welsh, *Complexity: Knots, Colourings and Counting,* London Mathematical Society, Lecture Notes Series 189, Cambridge University Press, 1993.

40. E. Witten, "Quantum field theory and the Jones polynomial," *Communications in Mathematical Physics,* vol. 121, pp. 351-399, 1989.

41. P. Wocjan, D. Janzing, T. Decker, T. Beth, "Measuring 4-local n-qubit observables could probabilistically solve PSPACE," *Proceedings of the winter international synposium on Information and communication technologies,* 2004, `arXiv:quant-ph/0308011`.

Appendix A

Proof of Lemma 6.1:   Introduce an extra system labeled $\mathcal{C}$ which holds a single control qubit and denote the Hilbert space of the qubits acted on by U by $\mathcal{A}$. Because U consists of $O(\text{poly}(n))$ gates, then so does the controlled unitary $V\colon \mathcal{AC} \to \mathcal{AC}$, defined by $V|\psi\rangle|0\rangle = |\psi\rangle|0\rangle$ and $|\psi\rangle|1\rangle = (U|\psi\rangle)|1\rangle$. Initialize the qubit in the state $\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)^{\mathcal{C}}$, and prepare the state $|\psi\rangle^{\mathcal{A}}$. Applying the controlled unitary places everything into the state

$$|\Psi\rangle^{\mathcal{AC}} = \frac{1}{\sqrt{2}}\big(|\psi\rangle|0\rangle + (U|\psi\rangle)|1\rangle\big).$$

Writing $\psi = |\psi\rangle\langle\psi|$, the reduced density matrix $\tau^{\mathcal{C}}$ of the extra qubit is then equal to

$$\begin{aligned}
\tau^{\mathcal{C}} &= \text{Tr}_{\mathcal{A}}\,|\Psi\rangle\langle\Psi|^{\mathcal{C}\mathcal{A}} \\
&= \frac{1}{2}\,\text{Tr}_{\mathcal{A}}\begin{pmatrix} \psi & \psi U^{\dagger} \\ U\psi & U\psi U^{\dagger} \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 & \langle\psi|U^{\dagger}|\psi\rangle \\ \langle\psi|U|\psi\rangle & 1 \end{pmatrix} \\
&= \frac{1}{2}\Big(1_2 + \sigma_X \text{Re}\langle\psi|U|\psi\rangle + \sigma_Y \text{Im}\langle\psi|U|\psi\rangle\Big).
\end{aligned}$$

Since the ± 1 eigenstates of σ_X are $|\pm\rangle = \frac{1}{2}\big(|0\rangle \pm |1\rangle\big)$, measuring σ_X on the qubit yields a classical random variable $X \in \{+1, -1\}$ for which $\mathbb{E}\,X = \text{Re}\langle\psi|U|\psi\rangle$ as required. Similarly, by running the algorithm a second time, we can sample from Y, which satisfies $\mathbb{E}\,Y = \text{Im}\langle\psi|U|\psi\rangle$. $\square$

Proof of Lemma 7.2:   By the triangle inequality,

$$\big|\langle\phi|U|\psi\rangle\big|^2 = \big|\langle\phi|U'|\psi\rangle + \langle\phi|(U - U')|\psi\rangle\big|^2 \le \big|\langle\phi|U'|\psi\rangle\big|^2 + \big|\langle\phi|(U - U')|\psi\rangle\big|^2.$$

The operator norm satisfies $\|M\|_{\infty} = \max\{|\text{Tr}\,MX| : \|X\|_1 = 1\}$, where the *trace norm* $\|X\|_1$ of a square matrix X is defined to be the sum of its singular values. Thus,

$$\big|\langle\phi|(U - U')|\psi\rangle\big|^2 = \big|\text{Tr}(U - U')|\psi\rangle\langle\phi|\big|^2 \le \big\|U - U'\big\|_{\infty}^2 \le \epsilon^2 \le \epsilon,$$

Therefore, $\big|\langle\phi|U|\psi\rangle\big|^2 - \big|\langle\phi|U'|\psi\rangle\big|^2 \le \epsilon$. A similar argument gives the same bound with U and U' swapped, proving the lemma. $\square$