Quantum algorithms (CO 781/CS 867/QIC 823, Winter 2013)
Andrew Childs, University of Waterloo
LECTURE 18: Approximating the Jones polynomial

In this final lecture, we discuss a very different class of quantum algorithms, ones that approximately solve various #P-complete problems. The best-known example of such a quantum algorithm is for approximating the value of a link invariant called the Jones polynomial.

The Hadamard test

The quantum algorithm for approximating the Jones polynomial uses a simple primitive called the *Hadamard test*. This is equivalent to phase estimation with a single bit of precision. Given a unitary operation U and a state $|\psi\rangle$, the Hadamard test provides a means of estimating $\langle\psi|U|\psi\rangle$. The test applies a controlled-U operation to the state $|+\rangle \otimes |\psi\rangle$ and measures the first qubit in the basis $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The state before the measurement is

$$\frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle) = \frac{1}{2}\big(|+\rangle(|\psi\rangle + U|\psi\rangle) + |-\rangle(|\psi\rangle - U|\psi\rangle)\big), \tag{1}$$

so

$$\Pr(\pm) = \frac{1}{4}\||\psi\rangle \pm U|\psi\rangle\|^2 \tag{2}$$
$$= \frac{1}{2}(1 \pm \mathrm{Re}\langle\psi|U|\psi\rangle). \tag{3}$$

In other words, the expected value of the outcome is precisely $\mathrm{Re}\langle\psi|U|\psi\rangle$. Replacing the states $|\pm\rangle$ by the states $|\pm i\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, a simple calculation shows that we can approximate $\mathrm{Im}\langle\psi|U|\psi\rangle$.

The Jones polynomial

The Jones polynomial is a central object in low-dimensional topology with surprising connections to physics. Witten showed that the Jones polynomial is closely related to topological quantum field theory (TQFT). Friedman, Kitaev, Larsen, and Wang investigated the relationship between TQFT and topological quantum computing, showing that quantum computers can efficiently simulate TQFTs (thereby approximating the Jones polynomial), and that in fact TQFTs essentially capture the power of quantum computation. Here we describe the quantum algorithm for approximating the Jones polynomial in a way that does not explicitly refer to TQFT, following the treatment of Aharonov, Jones, and Landau.

To define the Jones polynomial, we must first introduce the concepts of knots and links. A *knot* is an embedding of the circle in $\mathbb{R}^3$, i.e., a closed loop of string that may wrap around itself in any way. More generally, a *link* is a collection of any number of knots that may be intertwined. In an *oriented link*, each loop of string is directed. It is natural to identify links that are *isotopic*, i.e., that can be transformed into one another by continuous deformation of the strings.

The Jones polynomial of an oriented link L is a Laurent polynomial $V_L(t)$ in the variable $\sqrt{t}$, i.e., a polynomial in $\sqrt{t}$ and $1/\sqrt{t}$. It is a *link invariant*, meaning that $V_L(t) = V_{L'}(t)$ if the oriented links L and L' are isotopic. While it is possible for the Jones polynomial to take the same value on two non-isotopic links, it can often distinguish links; for example, the Jones polynomials of the two orientations of the trefoil knot are different.

An oriented link L can be specified by a *link diagram*, a drawing of the link in the plane with over- and under-crossings indicated. One way to define the Jones polynomial of a link diagram is as follows. First, let us define the *Kauffman bracket* $\langle L \rangle$, which does not depend on the orientation of L. Each crossing in the link diagram can be opened in one of two ways, and for any given crossing we have

$$\left\langle \diagup\!\!\!\!\diagdown \right\rangle = t^{1/4} \left\langle \,)\,(\, \right\rangle + t^{-1/4} \left\langle \asymp \right\rangle, \tag{4}$$

where the rest of the link remains unchanged. Repeatedly applying this rule, we eventually arrive at a link consisting of disjoint unknots. The Kauffman bracket of a single unknot is $\langle \bigcirc \rangle := 1$, and more generally, the Kauffman bracket of n unknots is $(-t^{1/2} - t^{-1/2})^{n-1}$. By itself, the Kauffman bracket is not a link invariant, but it can be turned into one by taking into account the orientation of the link, giving the Jones polynomial. For any oriented link diagram L, we define its *writhe* $w(L)$ as the number of crossings of the form $\nwarrow\!\!\!\!\nearrow$ minus the number of crossings of the form $\nearrow\!\!\!\!\nwarrow$. Then the Jones polynomial is defined as

$$V_L(t) := (-t^{-1/4})^{3w(L)} \langle L \rangle. \tag{5}$$

Computing the Jones polynomial of a link diagram is quite difficult. A brute-force calculation using the definition in terms of the Kauffman bracket takes time exponential in the number of crossings. Indeed, exactly computing the Jones polynomial is #P-hard (except for a few special values of t), as shown by Jaeger, Vertigan, and Welsh. Here #P is the class of counting problems associated to problems in NP (e.g., computing the number of satisfying assignments of a Boolean formula). Of course, approximate counting can be easier than exact counting, and sometimes #P-hard problems have surprisingly good approximation algorithms.

Links from braids

It is useful to view links as arising from *braids*. A braid is a collection of n parallel strands, with adjacent strands allowed to cross over or under one another. Two braids on the same number of strands can be composed by placing them end to end. The *braid group* on n strands is an infinite group with generators $\{\sigma_1, \ldots, \sigma_{n-1}\}$, where σ_i denotes a twist in which strand i passes over strand $i+1$, interchanging the two strands. More formally, the braid group is defined by the relations $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ and $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i - j| > 1$.

Braids and links differ in that the ends of a braid are open, whereas a link consists of closed strands. We can obtain a link from a braid by connecting the ends of the strands in some way. One simple way to close a braid is via the *trace closure*, in which the ith strand of one end is connected to the ith strand of the other end for each $i = 1, \ldots, n$, without crossing the strands. A theorem of Alexander states that any link can be obtained as the trace closure of some braid. Another natural closure (for braids with an even number of strands) is the *plat* closure, which connects the first and second strands, the third and fourth strands, etc., at each end of the braid.

Representing braids in the Temperley-Lieb algebra

The Jones polynomial of the plat or trace closure of a braid can be expressed in terms of a representation of the braid group defined over an algebra called the Temperley-Lieb algebra. While the definition of this algebra is fairly straightforward, the description of its representations is somewhat technical, and we will not give the details here; instead we only mention some general features.

We consider the case where $t = e^{2\pi i/k}$ is a kth root of unity. For such values, the relevant representation of the braid group is unitary. The dimension of this representation is exponential in n (specifically, it is the number of paths of length n that start from one end of a path with $k-1$ vertices), so it corresponds to a unitary operation on $\mathrm{poly}(n)$ qubits. The Jones polynomial of the plat closure of a braid is proportional to the expectation $\langle\psi|U|\psi\rangle$ of the associated representation matrix U in a fixed quantum state $|\psi\rangle$.

A quantum algorithm

The description of the Jones polynomial in terms of a representation of the Temperley-Lieb algebra naturally suggests a quantum algorithm for approximating the Jones polynomial. Suppose that we can efficiently implement unitary operations corresponding to twists of adjacent strands on a quantum computer. By composing such operations, we can implement a unitary operation corresponding to the entire braid. Then we can approximate the desired expectation value using the Hadamard test.

With a suitable choice for an encoding of the basis states of the representation of the braid group using qubits, one can show that the braid group representation operators corresponding to elementary twists can indeed be performed efficiently on a quantum computer. Given an explicit description of the braid group representation, the details of this implementation are fairly straightforward.

Applying this approach to the relevant unitary representation of the braid group, one obtains a quantum algorithm for approximating the Jones polynomial of the plat closure of a braid at a root of unity. In particular, for a braid on n strands, with m crossings, and with $t = e^{2\pi i/k}$, there is an algorithm running in time $\mathrm{poly}(n, m, k)$ that outputs an approximation differing from the actual value $V_L(t)$ of the Jones polynomial by at most $(2\cos\frac{\pi}{k})^{3n/2}/(N \cdot \mathrm{poly}(n, k, m))$, with only exponentially small probability of failure. Here N is an exponentially larger factor derived from the representation of the braid group.

The Jones polynomial of the trace closure of a braid can be similarly approximated by noting that this quantity is given by the *Markov trace* of the representation of the braid. The Markov trace is simply a weighted version of the usual trace, so it can be approximated by sampling $\langle\psi_p|U|\psi_p\rangle$ from an appropriate distribution over states $|\psi_p\rangle$. Performing such a procedure, one obtains an approximation of the Jones polynomial with additive error at most $(2\cos\frac{\pi}{k})^{n-1}/\,\mathrm{poly}(n, k, m)$, again in polynomial time and with exponentially small failure probability.

Quality of approximation

Without knowing more about the possible values of the Jones polynomial, it is hard to say whether the approximations described above are good. Notice that the algorithms only provide additive approximations, meaning that the error incurred by the algorithm is independent of the value being approximated, which is undesirable when that value is small. Indeed, the additive error increases exponentially with n, the number of strands in the braid. For some braids, the error might be larger than the value being approximated. It would be preferable to obtain a multiplicative approximation, but no such algorithm is known.

However, it can be shown that obtaining the additive approximation described above for the

Jones polynomial of the plat closure of a braid is as hard as any quantum computation. In other words, this quality of Jones polynomial approximation is BQP-complete. This can be shown by demonstrating that, with an appropriate encoding of qubits, the representations of the braid group can be used to implement a universal set of quantum gates. Thus, in principle, any quantum algorithm can be described in terms of some braid whose plat closure has a Jones polynomial encoding the result of the computation, with exponentially differing values corresponding to yes and no outcomes. Therefore, it is unlikely that a classical computer can obtain the same approximation, since this would give a classical algorithm for simulating a general quantum computation.

Approximating the Jones polynomial of the trace closure of a braid to the level described above turns out to be substantially easier: such a computation can be performed using a quantum computer whose initial state has only one pure qubit and many maximally mixed qubits. Such a device can approximate $\operatorname{tr} U$ by supplying the maximally mixed state in place of the pure state $|\psi\rangle$ in the Hadamard test. This does not immediately show how to approximate the Jones polynomial of the trace closure, since the Markov trace is a weighted trace. However, by using a different representation of the braid group to describe the Jones polynomial, Jordan and Shor showed that a single pure qubit indeed suffices. Furthermore, they showed that this problem is complete for the one clean qubit model, and hence apparently unlikely to be solvable by classical computers.

Other algorithms

The results described above can be generalized to many other related problems. Wocjan and Yard showed how to evaluate the Jones polynomial of a generalized closure of a braid, and how to evaluate a generalization of the Jones polynomial called the HOMFLYPT polynomial. Work of Aharonov, Arad, Eban, and Landau shows how to approximate the Tutte polynomial of a planar graph, which in particular gives an approximation of the partition function of the Potts model on a planar graph; this problem also characterizes the power of quantum computation, albeit only for unphysical choices of parameters. More generally, there are efficient quantum algorithms to compute additive approximations of tensor networks, as shown by Arad and Landau. There are also related quantum algorithms for approximating invariants of manifolds.