Quantum algorithms (CO 781, Winter 2008)
Prof. Andrew Childs, University of Waterloo

LECTURE 21: Universality of adiabatic quantum computation

In this final lecture, we will see how adiabatic evolution can be used to implement an arbitrary quantum circuit. In particular, this can be done with a local, linearly interpolated Hamiltonian. We may think of such Hamiltonians as describing a model of quantum computation. We know that this model can be efficiently simulated in the quantum circuit model. In this lecture we will see how the circuit model can be efficiently simulated by the adiabatic model, so that in fact the two models have equivalent computational power (up to polynomial factors).

This does not necessarily mean that there is an efficient adiabatic *optimization* algorithm for any problem that can be solved efficiently by a quantum computer. For example, Shor's algorithm shows that quantum computers can factor integers efficiently, yet we do not know if there is an adiabatic factoring algorithm that works by optimizing some cost function (such as the squared difference between the integer and a product of smaller integers). In general, it does not seem that the constructions of universal adiabatic quantum computers give much insight into how one might design efficient quantum adiabatic optimization algorithms. Nevertheless, they show that there is some sense in which the idea of adiabatic evolution captures much of the power of quantum computation.

The Feynman quantum computer In a classic paper from the mid-1980s, Feynman presented a quantum mechanical model of a computer using local, time-independent Hamiltonian dynamics.[1] The motivation for this model was to show that quantum mechanics does not pose barriers to building a classical computer, despite quantum effects such as the uncertainty principle. Feynman showed that any sequence of reversible classical logic gates can be efficiently simulated using local Hamiltonian dynamics. However, his model applies equally well to simulate a quantum circuit.

Given a k-gate quantum circuit on n qubits, $U_k \cdots U_2 U_1$, let

$$H_F := \sum_{j=1}^{k} H_j \tag{1}$$

where

$$H_j := U_j \otimes |j\rangle\langle j-1| + U_j^\dagger \otimes |j-1\rangle\langle j| \,. \tag{2}$$

Here the first register consists of n qubits, and the second register stores a quantum state in a $(k+1)$-dimensional space spanned by states $|j\rangle$ for $j \in \{0, 1, \ldots, k\}$. The second register acts as a clock that records the progress of the computation. Later, we will show how to represent the clock using qubits, but for now, we treat it as a convenient abstraction.

If we start the computer in the state $|\psi\rangle \otimes |0\rangle$, then the evolved state remains in the subspace spanned by the $k+1$ states

$$|\psi_j\rangle := U_j \cdots U_1 |\psi\rangle \otimes |j\rangle \tag{3}$$

for $j \in \{0, 1, \ldots, k\}$. In this subspace, the nonzero matrix elements of H_F are

$$\langle \psi_j | H_F | \psi_{j\pm 1} \rangle = 1 \,, \tag{4}$$

[1] Feynman's Hamiltonian has also been useful in quantum complexity, namely in formulating a complete problem for a quantum analog of the complexity class NP.

so the evolution is the same as that of a free particle propagating on a discretized line segment. Such a particle moves with constant speed, so in a time proportional to k, the initial state $|\psi_0\rangle$ will evolve to a state with substantial overlap on the state $|\psi_k\rangle = U_k \cdots U_1 |\psi\rangle|k\rangle$, corresponding to the final state of the computation. For large k, one can show that

$$|\langle\psi_k|e^{-\mathrm{i}H_F k/2}|\psi_0\rangle|^2 = O(k^{-2/3})\,, \tag{5}$$

so that after time $k/2$, a measurement of the clock will yield the result k, and hence give the final state of the computation, with a probability that is only polynomially small in the total number of gates in the original circuit.

The success probability of Feynman's computer can be made close to 1 by a variety of techniques. The simplest approach is to repeat the process $O(k^{2/3})$ times. Or we could pad the end of the computation with a large number of identity gates, boosting the probability that we reach a state in which the entire computation has been performed. Alternatively, as Feynman suggested, the success probability can be made arbitrarily close to 1 in single shot by preparing the initial state in a narrow wave packet that will propagate ballistically without substantial spreading. But perhaps the best approach is to make the process perfect by changing the Hamiltonian to

$$H_{FG} := \sum_{j=1}^{k} \sqrt{j(k+1-j)}\, H_j. \tag{6}$$

In this case, the choice $t = \pi$ gives the exact transformation $e^{-\mathrm{i}H_{FG}t}|\psi_0\rangle = |\psi_k\rangle$. This can be understood by viewing $|\psi_j\rangle$ as a state of total angular momentum $\frac{k}{2}(\frac{k}{2}+1)$ with z component $j - \frac{k}{2}$. Then H_{FG} is simply the x component of angular momentum, which rotates between the states with z component $\pm\frac{k}{2}$ in time π. Equivalently, H_{FG} can be viewed as the Hamiltonian in the Hamming weight subspace of a hypercube.

In the Hamiltonians (1) and (6), the clock space is not represented using qubits. However, we can easily create a Hamiltonian expressed entirely in terms of $k+1$ qubits using a unary representation of the clock. Let

$$|j\rangle := |\underbrace{0\cdots0}_{j}1\underbrace{0\cdots0}_{k-j}\rangle\,. \tag{7}$$

Then suppose we make the replacement

$$|j\rangle\langle j-1| \to \big(|01\rangle\langle 10|\big)^{(j-1,j)} \tag{8}$$

(and similarly for the adjoint), where the parenthesized superscript indicates which qubits are acted on. Then the subspace of states for which the clock register has the form (7) is invariant under the Hamiltonian, and within this subspace, its action is identical to that of the original Hamiltonian.

Notice that if the quantum circuit consists of one- and two-qubit gates, then the Hamiltonians (1) and (6) are local in the sense that the interactions involve at most four qubits. We call such a Hamiltonian 4-*local*.

This construction shows that even a time-independent Hamiltonian of a particularly simple form can be universal for quantum computation. Now let's see how we can modify the construction to use adiabatic evolution instead of a time-independent Hamiltonian.

An adiabatic variant The construction of an adiabatic quantum computer will again involve two registers, the first holding the state of the quantum computation and the second representing

a clock. The idea is to start from a Hamiltonian whose ground state is the initial state of the computation together with the initial configuration of the clock, and to slowly evolve to a Hamiltonian (essentially, minus the Feynman Hamiltonian (1)) whose ground state encodes not the final state of the computation, but rather a uniform superposition over the entire history of the computation.

As before, we will find it convenient to start with an abstract description of the clock register in terms of $k+1$ basis states $|0\rangle, |1\rangle, \ldots, |k\rangle$, without worrying about how these states are represented in terms of qubits. Later, we will consider issues of locality in this type of construction.

For the beginning Hamiltonian, we will use

$$H_B := -I \otimes |0\rangle\langle 0| + H_{\text{penalty}} \tag{9}$$

where

$$H_{\text{penalty}} := \sum_{j=1}^{n} \left(|1\rangle\langle 1|\right)^{(j)} \otimes |0\rangle\langle 0|. \tag{10}$$

Here the parenthesized superscript again indicates which qubit is acted on. The first term of (9) says that the energy is lower if the clock is in the initial state $|0\rangle$. Adding H_{penalty} gives an energy penalty to states whose clock is in the state $|0\rangle$, yet for which the state of the computation is not the initial state $|00\ldots0\rangle$. Thus the unique ground state of H_B is $|00\ldots0\rangle \otimes |0\rangle$.

For the final Hamiltonian (which we denote H_C, since it encodes the final result of an arbitrary circuit, rather than the solution of a particular problem), we will use

$$H_C := -H_F + H_{\text{penalty}} \tag{11}$$

where H_F is the Feynman Hamiltonian defined in (1). From (4), we see that the $-H_F$ has a degenerate ground state subspace, where any state of the form

$$|\eta\rangle := \frac{1}{\sqrt{k+1}} \sum_{j=0}^{k} |\psi_j\rangle \tag{12}$$

(with $|\psi_j\rangle$ defined in (3)), with an arbitrary initial state $|\psi\rangle$, has minimal energy. Adding H_{penalty} penalizes those states for which the initial state of the computation is not $|00\ldots0\rangle$, so that (12) with $|\psi\rangle = |00\ldots0\rangle$ is the unique ground state of H_C. This state is almost as good as the final state of the computation, since if we measure the clock, we obtain the result k with probability $1/(k+1)$, which is $1/\operatorname{poly}(n)$ assuming the length of the circuit is only $k = \operatorname{poly}(n)$. By repeating the entire process $\operatorname{poly}(k)$ times, we can obtain the final state of the computation with high probability.

Finally, we use linear interpolation to get from H_B to H_C, defining

$$H(s) := (1-s)H_B + sH_C\,. \tag{13}$$

If we begin in the state $|00\ldots0\rangle \otimes |0\rangle$ and evolve according to $H_T(t) := H(t/T)$ for a sufficiently large time T, the adiabatic theorem guarantees that the final state will be close to $|\eta\rangle$. It remains to estimate the gap $\Delta(s)$ to show that $T = \operatorname{poly}(k)$ is sufficient.

In fact, the $(k+1)$-dimensional *computational subspace* spanned by the states $|\psi_j\rangle$ with $|\psi\rangle = |00\ldots0\rangle$ is invariant under $H(s)$, so it suffices to compute the gap within this subspace. Let us examine how $H(s)$ acts within the computational subspace. Note that $H_{\text{penalty}}|\psi_j\rangle = 0$ for all $j \in \{0, 1, \ldots, k\}$. We have

$$\langle\psi_j|H_B|\psi_{j'}\rangle = -\delta_{j,j'}\delta_{j,0} \tag{14}$$

and

$$\langle \psi_j | H_C | \psi_{j'} \rangle = -(\delta_{j,j'+1} + \delta_{j,j'-1}) \,, \tag{15}$$

so we need to lower bound the gap between the smallest and second smallest eigenvalues of the matrix

$$\begin{pmatrix} s-1 & -s & 0 & \cdots & 0 \\ -s & 0 & -s & \ddots & \vdots \\ 0 & -s & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & -s \\ 0 & \cdots & 0 & -s & 0 \end{pmatrix} . \tag{16}$$

We will show

Lemma. *The gap between the smallest and second smallest eigenvalues of the matrix (16) for* $s \in [0,1]$ *is* $\Omega(1/k^2)$

Proof. The reduced Hamiltonian (16) essentially describes a free particle on a finite, discrete line, with a nonzero potential at one end. Thus the eigenstates are simply plane waves with a quantization condition determining the allowed values of the momentum. We will show the lower bound on the gap by analyzing this quantization condition.

We claim that the (unnormalized) eigenstates of (16), denoted $|E_p\rangle$, are given by

$$\langle \psi_j | E_p \rangle = \sin(p(k-j+1)) \tag{17}$$

for $j = 0, 1, \ldots, k$, and where p is yet to be determined. It is straightforward to verify that these states satisfy

$$\langle \psi_j | H(s) | E_p \rangle = E_p \langle \psi_j | E_p \rangle \tag{18}$$

for $j = 1, 2, \ldots, k$, with the energy given by

$$E_p = -2s \cos p. \tag{19}$$

(where p may be either real or imaginary). The allowed values of p are determined by the quantization condition obtained by demanding that (18) also holds at $j = 0$, i.e., that we have

$$-s \sin(kp) + (s-1) \sin((k+1)p) = E_p \sin((k+1)p) \,. \tag{20}$$

Using trigonometric identities, we can rewrite this condition as

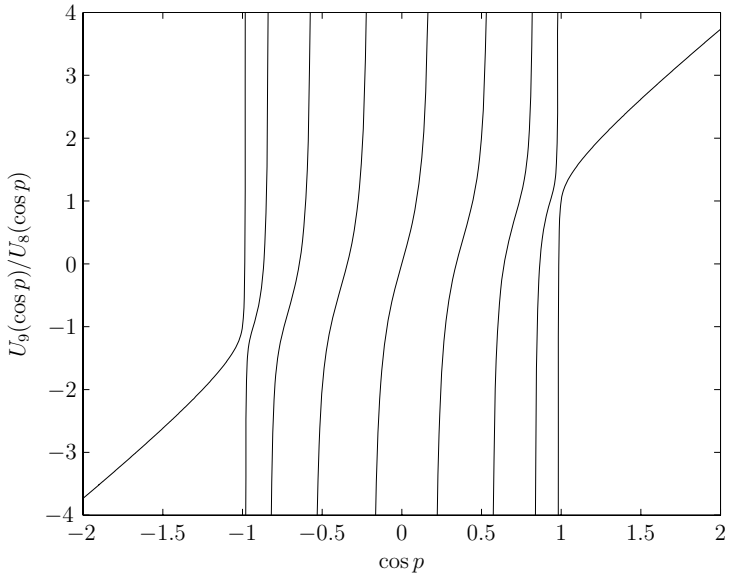
$$s \sin((k+2)p) = (1-s) \sin((k+1)p) \,, \tag{21}$$

or equivalently, in terms of Chebyshev polynomials, as

$$\frac{U_{k+1}(\cos p)}{U_k(\cos p)} = \frac{1-s}{s} \tag{22}$$

where $U_k(x)$ is the kth Chebyshev polynomial of the second kind, satisfying $U_k(\cos\theta) = \sin((k+1)\theta)/\sin\theta$.

The left hand side of (22) is shown below for $k = 8$. The intersections of this curve with the constant function $(1-s)/s$, when multiplied by $-2s$, give the eigenvalues E_p. Note that since p can be imaginary, $\cos p$ can be larger than 1 or smaller than -1.



Since the roots of $U_k(x)$ are given by $\cos\frac{j\pi}{k+1}$ for $j = 1, 2, \ldots, k$, the left hand side of (22) has simple poles at those values (and zeros at $\cos\frac{j\pi}{k+2}$ for $j = 1, 2, \ldots, k+1$). One can show that left hand side of (22) is strictly increasing. So there is one solution of (22) to the left of the leftmost pole, one between each pair of poles, and one to the right of the rightmost pole, giving a total of $k+1$ solutions, and thus accounting for all the eigenvalues of (16).

It remains to show that the gap between the two rightmost solutions of (22) is not too small. It is easy to see that the gap is $\Omega(1/k^3)$, because the ground state has $\cos p \geq \cos\frac{\pi}{k+2}$ (since it must occur to the right of the rightmost root), and the first excited state has $\cos p \leq \cos\frac{\pi}{k+1}$ (since it must occur to the left of the rightmost pole). This shows the gap is at least $2s(\cos\frac{\pi}{k+2} - \cos\frac{\pi}{k+1}) = \Omega(1/k^3)$ for constant s (and it is easy to show that the gap is a constant for $s = o(1)$).

However, we might like to prove a tighter result. To do this, we can separately consider the cases where the value of p corresponding the ground state is real (giving a plane wave) and where it is imaginary (giving a bound state). Since $U_{k+1}(1)/U_k(1) = (k+2)/(k+1)$, the value of s separating these two regimes is $s^* := (k+1)/(2k+3)$.

For $s \leq s^*$, the ground state has $\cos p \geq 1$, whereas the first excited state has $\cos p \leq \cos\frac{\pi}{k+1}$ (as observed above). Therefore, the gap satisfies

$$\Delta(s) \geq 2s\Big(1 - \cos\frac{\pi}{k+1}\Big) = \Omega(1/k^2) \tag{23}$$

for constant s (and as mentioned above, it is easy to see that $\Delta(s) = \Omega(1)$ for $s = o(1)$).

For $s > s^*$, the ground state has $\cos p \geq \cos\frac{\pi}{k+2}$ (as mentioned above). For the first excited state, we will show that the solution of (22) not only lies to the left of the rightmost pole, but that its distance from that pole is at least a constant fraction more than the distance of that pole from $\cos p = 1$. In particular, for any constant $a > 0$, we have

$$\frac{U_{k+1}(1-(1+a)(1-\cos\frac{\pi}{k+1}))}{U_k(1-(1+a)(1-\cos\frac{\pi}{k+1}))} = \frac{\sin((k+2)\cos^{-1}((1+a)\cos\frac{\pi}{k+1} - a))}{\sin((k+1)\cos^{-1}((1+a)\cos\frac{\pi}{k+1} - a))} \tag{24}$$

$$= 1 + \frac{\pi\sqrt{1+a}\cot(\pi\sqrt{1+a})}{k} + O(1/k^2) \tag{25}$$

where the second line follows by Taylor expansion. In comparison,

$$\frac{k+2}{k+1} = 1 + \frac{1}{k} + O(1/k^2)\,. \tag{26}$$

So if we fix (say) $a = 1$, then for k sufficiently large, (25) is larger than (26), which implies that the first excited state has $\cos p \leq 2\cos\frac{\pi}{k+1} - 1$. In turn, this implies that

$$\Delta(s) \geq 2s\left(\cos\frac{\pi}{k+2} - 2\cos\frac{\pi}{k+1} + 1\right) = \Omega(1/k^2)\,, \tag{27}$$

which completes the proof. □

Locality The Hamiltonian (13) is local in terms of the computational qubits, but not in terms of the clock. However, it is possible to make the entire construction local.

The basic idea is again to use a unary representation of the clock, as in (7). We saw above that this makes H_F 4-local. However, H_B and H_{penalty} remain nonlocal with this clock, since they include the projector $|0\rangle\langle 0|$ acting on the clock register, which involves all $k+1$ of the clock qubits. Thus we must modify the construction slightly.

Let's try adding a term to H_{penalty} that penalizes clock states which are not of the correct form. To do this, it will be useful to change the unary representation from (7) to a form that can be checked locally, this time with $k+2$ qubits:

$$|j\rangle := |\underbrace{0\cdots 0}_{j+1}\underbrace{1\cdots 1}_{k-j+1}\rangle \tag{28}$$

for $j \in \{0, 1, \ldots, k\}$. (Note that the first qubit is always in the state $|0\rangle$, and the last qubit is always in the state $|1\rangle$.) Now we can verify that the clock state is of the form (28) by ensuring that there is no occurrence of the string "10" in the clock register, that the first bit is not "1", and that the last bit is not "0"; then we can check whether the clock is in its initial state by checking whether the second clock qubit is in the state $|1\rangle$. Thus, let us redefine

$$H_{\text{penalty}} := \sum_{j=1}^{n} \left(|1\rangle\langle 1|\right)^{(j)} \otimes \left(1 - |1\rangle\langle 1|\right)^{(1)} + I \otimes \left(|1\rangle\langle 1|\right)^{(0)} + \sum_{j=1}^{k} I \otimes \left(|10\rangle\langle 10|\right)^{(j,j+1)} + I \otimes \left(|0\rangle\langle 0|\right)^{(k+2)} \tag{29}$$

where the parenthesized superscripts again indicate which qubits are acted on. We also redefine the beginning Hamiltonian as

$$H_B := -I \otimes \left(1 - |1\rangle\langle 1|\right)^{(1)} + H_{\text{penalty}}\,, \tag{30}$$

and in the Feynman term H_F of the computational Hamiltonian H_C, we make the replacement

$$|j\rangle\langle j-1| \to \left(|001\rangle\langle 011|\right)^{(j-1,j,j+1)} \tag{31}$$

(and similarly for the adjoint). With these redefinitions, the overall Hamiltonian $H(s) = (1 - s)H_B + sH_C$ is 5-local, assuming as before that the gates in the quantum circuit to be simulated involve at most two qubits each.

As with the original nonlocal-clock construction, H_B and H_C have unique ground states $|0\ldots 0\rangle \otimes |01\ldots 1\rangle$ and $\frac{1}{\sqrt{k+1}}\sum_{j=0}^{k} U_j \cdots U_1 |0\ldots 0\rangle \otimes |0^{j+1}1^{k-j+1}\rangle$, respectively. Again, the computational

subspace spanned by the states $|\psi_j\rangle$ from (3) (but now with the clock representation (28)) is invariant under $H(s)$; and within this subspace, the Hamiltonian acts according to (16), which has a gap of $\Omega(1/k^2)$. Overall, this shows that there is a 5-local Hamiltonian $H(s)$ implementing an arbitrary quantum circuit by adiabatic evolution.

By suitable engineering, it's possible to produce variants of this construction with even better locality properties. One can even make the Hamiltonian *spatially* local, with nearest-neighbor interactions between qubits on a two-dimensional square lattice. (In fact, this has recently been improved to a one-dimensional array of quantum systems, although not with qubits, but with higher-dimensional particles.)