18.405J/6.841J Advanced Complexity Theory March 15, 2001

Lecture 11

Lecturer: Dan Spielman *Scribe: Daniel Preda*

Quantum Complexity

Today we will define the quantum classes **EQP** and **BQP** (corresponding to the classical classes **P** and, respectively, **BPP**), and show that $\mathbf{P} \subseteq \mathbf{EQP}$ and $\mathbf{BPP} \subseteq \mathbf{BQP}$. We will also introduce the notion of *universal family of quantum gates.*

Recall from last lecture:

Definition 1 *A quantum gate is a unitary matrix U ($U^\dagger = U^{-1}$) of size $2^n \times 2^n$, where n is the number of input (and output) wires.*

Please note that, besides the wires that carry the desired input state, we also allow extra input wires set to a initially known value (for instance $|0\rangle$ or $|1\rangle$.)

In order to define the size of a quantum circuit, we restrict (like in the classical case) the circuit to have only gates with at most 3 inputs (3-bit gates).

Definition 2 *The size of a quantum circuit is the number of gates it has.*

Note: A quantum circuit may have a "distinguished" wire that says if the circuit accepts or rejects a certain input. From now on, we will assume that measurement is performed only at the end. It is easy to see that a measurement in the middle of the computation is equivalent to a measurement at the end.

Theorem 3 *Any quantum circuit C with n inputs and size $f(n)$ is equivalent to a circuit C' with $O(nf(n))$ inputs and of size $O(nf(n))$, where all measurements are performed at the end.*

Proof First of all, notice that, without loss of generality, we may as well assume that we measure in the z-basis (i.e. $\binom{1}{0}$ and $\binom{0}{1}$) (performing an appropriate change of basis if necessary). Because there are at most f(n) gates in the circuit, we can measure at most $O(nf(n))$ qubits (before or after a gate). For each qubit we measure, attach an extra wire which is initially set to $|0\rangle$. Then, replace the measurement with a Controlled-NOT gate (applies a NOT on the second qubit iff the first one is $|1\rangle$) between the qubit to be measured and the extra wire. WLOG, suppose we measure measure the first k qubits. Let the initial state be

$$\frac{1}{2^{k/2}} \sum_{i=0}^{2^k-1} a_i |i\rangle_k \otimes |\psi\rangle_{n-k} \otimes |0\rangle_k$$

After the application of the Controlled-NOT between each of the first k qubits and the corresponding extra qubit, we end up in the state:

$$\frac{1}{2^{k/2}} \sum_{i=0}^{2^k-1} \left(a_i |i\rangle_k \otimes |\psi\rangle_{n-k} \otimes |i\rangle_k\right)$$

This state evolves under the unitary operator U that acts on the first n qubits to:

$$\frac{1}{2^{k/2}} \sum_{i=0}^{2^k-1} \left[U\left(a_i |i\rangle_k \otimes |\psi\rangle_{n-k}\right) \otimes |i\rangle_k\right]$$

Now if we measure the last k qubits, we collapse the state into:

$$U\left(|i\rangle_k \otimes |\psi\rangle_{n-k}\right)$$

with probability $|a_i|^2$, for some $i = 0...2^k - 1$. This is exactly the same state we have ended up in if we had measured the first k qubits, got the same value of i, and then evolved under U. ■

Definition 4 **EQP**$=\{L \mid \exists$ *a family of quantum circuits* $\{Q_n\}_n$, *where* Q_n *takes* n *inputs, and a ptime turing machine* M *that on input* 1^n *outputs* Q_n *such that:*

$$w \in L \Leftrightarrow Pr\left[Q_{|w|}(w) = 1\right] = 1$$

$$w \notin L \Leftrightarrow Pr\left[Q_{|w|}(w) = 1\right] = 0 \ \}$$

Definition 5 **BQP**$=\{L \mid \exists$ *a family of quantum circuits* $\{Q_n\}_n$, *where* Q_n *takes* n *inputs, and a ptime turing machine* M *that on input* 1^n *outputs* Q_n *such that:*

$$w \in L \Leftrightarrow Pr\left[Q_{|w|}(w) = 1\right] \geq 2/3$$

$$w \notin L \Leftrightarrow Pr\left[Q_{|w|}(w) = 1\right] \leq 1/3 \ \}$$

Before proving that **P** $\subseteq$ **EQP** and **BPP** $\subseteq$ **BQP**, there are some remarks to be made:

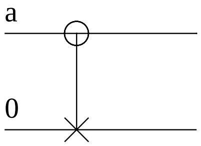
It can be proved that the transition amplitudes of the quantum gates need only be accurate to $poly(\log T)$ bits of precision for a quantum circuit of size T.

Because any quantum gate U is unitary, U^{-1} is also unitary and hence every quantum gate is reversible. As a parentheses, there has been extended work in the field of reversible computation well before the emergence of quantum computing. The Landauer's principle states that when a bit of information is erased, it must either be transfered to another bit or be dissipated as $k_B \ln 2$ entropy (k_B is Boltzmann's constant, approx. $1.38 \times 10^{-23} J/K$). Hence, erasing one bit creates heat in an amount of $k_B T \ln 2$, where T is the temperature.

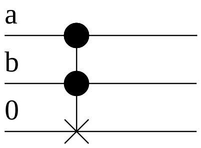
Theorem 6 **P** $\subseteq$ **EQP**

Proof Suppose we have a classical circuit C that computes $f : \{0,1\}^n \to \{0,1\}^m$, has only AND, OR or NOT gates and has size $s(n)$. We construct a quantum circuit C' of size $O(s(n) + m)$ computing $Q_f : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ that maps each pair (x, y) into $(x, y \oplus f(x))$, $x \in \{0,1\}^n$, $y \in \{0,1\}^m$, using at most $s(n)$ additional qubits, initially set to $|0\rangle$.

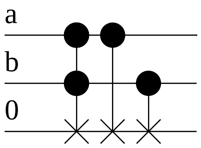
First we replace each classical gate with its quantum version:
NOT:



The Control is done here on first bit being $|0\rangle$. The last qubit ends up in state $|\bar{a}\rangle$
AND:



The Control is done here on $|1\rangle$. The last qubit ends up in state $|a \wedge b\rangle$
OR:



The Control is done here on $|1\rangle$. The last qubit ends up in state $|a \vee b\rangle$. Note that OR can also be built from NOT and AND.

We design the quantum circuit as follows: we use one wire for each input ("input" qubits), one for each (classical) gate (initially set to $|0\rangle$) ("gate" qubits), and one for each output (initially set to $|0\rangle$) ("output" qubits). Then, using the quantum gates described above, and following the description of the classical circuit, we assign to each of the "gate" qubits the value of the output bit of that classical gate. When we finished all the gates, we just attach Controlled-NOTs between the "gate" qubits corresponding to the classical output bits, and the "output" qubits, thus copying the output into the "output" bits.

If we wish to return the "gate" qubits to $|0\rangle$, we could apply all the gates in reverse order (note that a Control applied twice is identity). This is useful because otherwise the "output" qubits remain entangled with the "gate" qubits and this can mess up further computations on the "input" and "output" qubits. ■

Theorem 7 **BPP $\subseteq$ BQP**

Proof The idea is simple: use same proof as above, but also add some "random" qubits initially set to $|0\rangle$. Then apply Hadamards on all those qubits, turning them into $1/\sqrt{2}(|0\rangle + |1\rangle)$. Whenever we want to flip a coin, do a Controlled-NOT on one of those qubits (use different qubits for different coin tosses). At the end, measure all the "random" qubits, and obtain ($|0\rangle$ or $|1\rangle$) with probability $1/2$. By an argument similar to that used in Theorem 3, this is equivalent to measuring them in the middle of the computation and using the random value right away. ■

Theorem 8 *Any quantum gate can be built from quantum gates with at most 3-bit inputs (and even with at most 2-bit inputs)*

We may attempt to prove this theorem next lecture. For now, we will focus on finding a family of at most 3-bit input gates that can be used as the above theorem claims. Clearly, what we would like is to be able to generate any 3-bit input gate.

Definition 9 *We define a "universal family of quantum gates" to be a family of gates of dimension of up to 8×8 such that any 8×8 unitary matrix is near a matrix generated by this family.*

We now define what "near" means:

Definition 10 *Let*

$$|M| = \sum_{i,j} |m_{i,j}|$$

We want a family $\mathcal{F}$ such that $\forall U, \epsilon > 0$, $\exists U^{'}$ generated by gates in family such that $|U - U^{'}| < \epsilon$ and only need *poly* $(1/\epsilon)$ gates to construct $U^{'}$ (actually it can be proved that we can do this even with *polylog* $(1/\epsilon)$ gates)

Theorem 11 *Let v be a unit vector, and U, $U^{'}$ two unitary matrices such that $|U - U^{'}| < \epsilon$. Then the angle between Uv and $U^{'}v$ is at most ϵ, for ϵ small.*

Proof Let $A = U - U^{'}$. The length of the vector $Uv - U^{'}v$ is:

$$\| Av \| = \sqrt{\sum_i \mid \sum_j A_{ij} v_j \mid^2} \leq \sum_i \mid \sum_j A_{ij} v_j \mid \leq \sum_{ij} \mid A_{ij} v_j \mid$$

But $\mid v_j \mid \leq 1$, so we get:

$$\| Av \| \leq \sum_{ij} \mid A_{ij} \mid \leq \epsilon$$

This completes the proof, as $\| Uv \| = \| U^{'}v \| = 1$ ■

Now we can show that if we have m gates, each with error ϵ, the errors add up:

Theorem 12 *Let U_i, and respectively $U_i^{'}$, $i = 1...m$ be unitary matrices of $N \times N$. If, $\forall i$, $|U_i - U_i^{'}| < \epsilon$, then $\forall v$, the angle between $U_1 U_2 ... U_m v$ and $U_1^{'} U_2^{'} ... U_m^{'} v$ is at most $m\epsilon$, for ϵ small.*

Proof We'll prove by induction. We already proved the base case. Inductive step:
Suppose the angle between $U_1^{'}..U_k^{'} U_{k+1} ... U_m v$ and $U_1 ... U_m v$ is at most $k\epsilon$. The angle between $U_{k+1}^{'} ... U_m v$ and $U_{k+1} ... U_m v$ is at most ϵ and because unitary matrices preserve the angle, we have that the angle between $U_1^{'}..U_k^{'} U_{k+1}^{'} ... U_m v$ and $U_1^{'}..U_k^{'} U_{k+1} ... U_m v$ is at most ϵ. Thus, the angle between $U_1^{'}..U_k^{'} U_{k+1}^{'} ... U_m v$ and $U_{k+1} ... U_m v$ is at most $(k+1)\epsilon$. ■

The above theorems prove that if $\epsilon = o(1/m)$ then we have almost infinite precision. Now we will try to define a "universal" family of 1-bit gates.

Fact 13 *Any 2×2 unitary matrix can be decomposed as:*

$$\begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix} \cdot \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & \cos\theta/2 \end{pmatrix} \cdot \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix}.$$

This is true as any element of $SU(2)$ is generated by rotations and phase shifts. The first matrix in the above expansion is just an overall phase.

All we need to do is to find a value θ_0 such that, $\forall \theta \in [0, 2\pi]$, $\mid k\theta_0 - \theta \mid mod\ 2\pi \leq \epsilon$, and k is bounded by (and can be computed in) some polynomial in $1/\epsilon$.

Claim 14 *$2\pi/\sqrt{2}$ is a good value for θ_0 above.*

The above result can be intuitively understood by observing that multiples of θ_0 land uniformly on the circle. In *"Quantum complexity theory"* (available at http://http.cs.berkeley.edu/ vazirani/), E. Bernstein and U. Vazirani prove that $\theta_0 = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}$ is a good value for θ_0 and they give a *polylog*$(1/\epsilon)$ algorithm that outputs a k bounded by a polynomial in $1/\epsilon$.

If we want to generalize the above results for 3-bit gates, the idea (which may be expanded next lecture) is to create gates Control-Control-Rotation and Control-Control-Phase, with the same θ_o as above.