Quantum Computation 101 for Physicists

Class exercise 5

1 Quantum Phase Estimation

Note: this section does not a apear in Mermin's book. A good reference is chapter 5 in the book by Nielsen and Chuang here.

The quantum Fourier transform is a basis not only to Shor's algorithm, but to a family of algorithms based on quantum phase estimation. At home you will see that in fact, Shor's algorithm is a quantum phase estimation algorithm.

Suppose we have a unitary U and a qubit register in a state $|\psi\rangle$, which is an eigenstate of U, $U|\psi\rangle = \lambda$, and we want to know λ. Note that U is not necessarily Hermitian, so we cannot just measure it. Since U is unitary, λ is of magnitude 1, $\lambda = e^{2\pi i\phi}$. Estimating the phase ϕ is then all we need for estimating λ. We write the phase as a bit string $\phi = 0.\phi_1\phi_2\dots$.

1.1 Question 1

1. Assume you have a circuit that applies U, a qubit registry in an eigenstate $|\psi\rangle$ of U, and one ancilla qubit started at $|0\rangle$. Use the Fourier transform to find the first bit of ϕ. Hint: use a controlled-U gate, which we are guaranteed to be able to implement.

2. Use the answer for (1) to write a protocol for estimating the first n bits of ϕ.

1.2 Solution

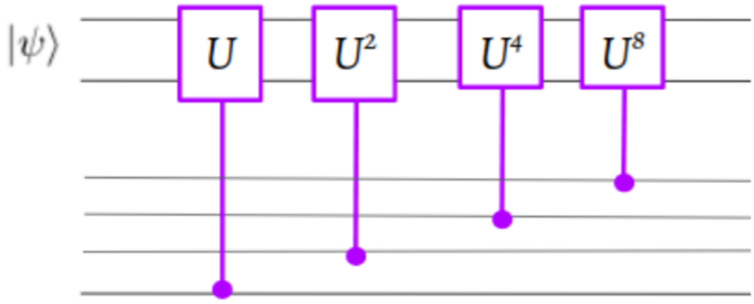
1. We start by applying a Hadamard on our ancilla qubit, so our state is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle$. Now we apply U on the second register only if the ancilla qubit is in state $|1\rangle$, basically, a controlled-U (we know that we can create such a unitary out of our basic set of gates). Our state is now $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\phi}|1\rangle)|\psi\rangle = \frac{1}{\sqrt{2}}\sum_{j=0}^{1} e^{2\pi i\phi j}|j\rangle|\psi\rangle$. The two registers are disentangled, so we will stop carrying the second register from now on. We notice that the state of the first register looks a little like a Fourier transform. It in fact is the discrete Fourier transform of $\phi \cdot 2^n$ for $n = 1$, which is our case, 2ϕ. So if we apply a reverse Fourier transform, we will get 2ϕ, which is the first bit of ϕ.

2. If we want n bits, we will need n ancilla qubits. We apply $H^{\otimes n}$ on the ancilla qubits to get $\frac{1}{2^{n/2}}\sum_j |j\rangle|\psi\rangle$. In order to get the state in the same form as in (1), $\frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1} e^{2\pi i\phi\cdot j}|j\rangle|\psi\rangle$, we need to apply U^j on the second register based on the state of the first register, j. This is still a unitary, so it can be applied. We now apply a reverse Fourier transform, and get $\phi \cdot 2^n$, which is (up to a rounding of the number) the first n bits of ϕ.

1.3 Question 2

For $n = 4$, draw explicitly the circuit that applies the unitary $\sum_j |j\rangle\langle j| \otimes U^j$. Deduce: for which type of unitaries is the phase estimation protocol relevant?

1.4 Solution



We see that we need to apply an exponential number of U gates (this is in fact by definition, since we apply U^j for all j from 0 to $2^n - 1$). Quantum phase estimation is thus relevant when U^{2^k} can be implemented efficiently, like we saw in class with b^x.

So now we can already guess that Shor's algorithm is in fact phase estimation. U implements multiplication by b (modulo N). Next week we will look at Phase estimation when the second register is in some combination of eigenstates of U and get the full understanding.

1.5 Question 3

Assume we have some unitary U for which U^{2^k} can be implemented efficiently, and a state $|\psi\rangle$ which is some combination of U's eigenstates, $U|\psi\rangle = U\sum_m \psi_m|m\rangle = \sum_m \psi_m e^{i2\pi\phi_m}|m\rangle$. Use the Quantum phase estimation to find one arbitrary eigenvalue of U up to n bits.

1.6 Solution

Let's just start with applying the quantum phase estimation protocol as is: We start with a register in the state $|0\rangle^{\otimes n}$ along with a second register in the state $|\psi\rangle$, and apply $H^{\otimes n}$ on the first register, to get:

$$\frac{1}{2^{n/2}}\sum_{j,m}\psi_m|j\rangle|m\rangle.$$

We now apply $\sum_j |j\rangle\langle j| \otimes U^j$ on our two registers, to get:

$$\frac{1}{2^{n/2}}\sum_{j,m}\psi_m e^{i2\pi j\phi_m}|j\rangle|m\rangle.$$

The two registers are now entangled (the coefficient of $|j\rangle|m\rangle$ depends both on j and m), so we cannot just ignore the second register as we did above. Later we will see that we can measure it (as we did in Shor's algorithm or Simon's algorithm), but for now we will just carry it with us. We write our state as

$$\frac{1}{2^{n/2}}\sum_m \psi_m \sum_j e^{i2\pi j\phi_m}|j\rangle|m\rangle = \sum_m \psi_m U_{FT}|2^n\phi_m\rangle|m\rangle.$$

We can now apply the reverse Fourier transform on the first register, to get

$$\sum_m \psi_m|\phi_m 2^n\rangle|m\rangle.$$

We want ϕ_m for some m. We see that all we need is to measure the first register. We will get ϕ_m with probability $|\psi_m^2|$.

What can we do with this tool we just got? First thing to do is to notice that unitary operators are exponentials of observables, $U = e^{iH}$. As Moshe have mentioned before, estimation ground state energy of Hamiltonians can be used in order to solve a lot of computational problems. When we have some sort of an optimization problem, we can write a Hamiltonian for which the ground state will be the optimal answer, and then search for its ground state. This is in fact a known method in classical optimization and data science as well, not only in quantum computation.

Finding the ground state of a general Hamiltonian is a hard problem, and it belongs to a class called QMA-complete. This means that finding the ground state energy for some Hamiltonians will take exponential time for a quantum computer. But we already know that quantum phase estimation doesn't always work - we require a unitary for which U^{2^k} can be implemented efficiently, and also, if ψ_0 is the ground state and $|\langle\psi_0||\psi\rangle|^2 = p$, the chance to get the ground state energy is p. If the ground state is some eigenstate of the computational basis, and we have no prior assumptions about it, then in general the chance to get the ground state energy is $\frac{1}{2^n}$. It's still worth trying to find the ground state of some of the Hamiltonians.

Note: Throughout this class, we skipped the part where we calculate the error in the calculation of the phase or the number of measurements we need to preform in order to get a good estimation of the expectation value. If you are interested in this, You can read the notes by Neilsen and Chuang and email me your questions.