Algebra and Computation Course Instructor: V. Arvind

Lecture 21: Quantum simulation of Boolean circuits and more

Lecturer: V. Arvind *Scribe: Vipul Naik*

1 Postulates of quantum mechanics

1.1 The state space postulate

The state space of an isolated physical system is a $\mathbb{C}$-vector space (equipped with inner product) and the possible outcomes form an orthonormal basis for this space.

Note that we require the physical system to be *isolated*. In fact, one of the concrete problems with implementing quantum computers in reality is the inability to sufficiently isolate the quantum computer from the outside world.

1.2 The evolution postulate

The state space of an isolated physical system evolves under the action of a unitary operator.

In other words, if $|\psi\rangle$ is the state at time t_1 and $|\psi'\rangle$ is the state at time t_2, then there exists a unitary operator U_{t_1,t_2} that maps $|\psi\rangle$ to $|\psi'\rangle$.

The unitary operator can thus be viewed as acting in discrete time, according to a "clock" whose clock pulse is $t_2 - t_1$.

Continuous-time evolution, if we are interested in that, is governed by a Hermitian operator, called the Hamiltonian of the system. That is:

$$ih\frac{d}{dt}|\psi\rangle = H|\psi\rangle$$

This is obtained by differentiating the unitary operator with respect to time.

When we only assume the physical system to be closed and do *not* assume it to be isolated, then we get a time-varying Hamiltonian, and hence the evolution is not given by a unitary operator.

1.3 The measurement postulate

Definition 1. *A* measurement is a collection of linear operators M_m such that:

$$\sum_m M_m^* M_m = I$$

The measurement is said to be *measurement(projective) if it measures components with respect to an orthogonal direct sum decomposition.*

The measurements we have talked of so far are projective measurements where we look at a *complete* orthogonal direct sum decomposition, that is, a decomposition as a sum of pairwise orthogonal one-dimensional subspaces.

2 The Deutsch-Josza problem

2.1 Statement of the problem

The Deutsch-Josza problem is a somewhat artificial problem that illustrates that in the query model, deterministic quantum computation can be far faster than deterministic classical computation. By query model, we mean a model where the complexity is measured by the number of queries that need to be made to an oracle, to answer a question about something hidden within that oracle.

Here is the precise statement:

Problem:

$f : \{0,1\}^n \to \{0,1\}$ is a Boolean function with the "promise" that f is either constant (that is, $f(x) = f(y)$ for all $x, y \in \{0,1\}^n$) or balanced (that is, $\left|f^{-1}(0)\right| = \left|f^{-1}(1)\right|$). We have a query oracle for f, that can take in $x \in \{0,1\}^n$ and output $f(x)$. We need to use this query oracle to find where f is constant or balanced. The complexity of our procedure is determined by the number of queries (calls) made to the oracle.

2.2 Classical deterministic and randomized complexities

The deterministic complexity of the Deutsch-Josza problem is $2^{n-1}+1$. This is because if the function is actually constant, then we need to know its value at at least that many points to be sure that it is constant.

The randomized complexity of the Deutsch-Josza problem is constant, in the sense that we can, given any ϵ, make a constant number of queries

dependent only on ϵ such that the probability of error is bounded above by ϵ (note that in this case the error is one-sided).

2.3 Rules for the quantum algorithm

In the quantum algorithm, what we want to do is to use the fact that there are an equal number of 0s and 1s, to get the 0s and 1s to *cancel* one another. First, however, we need to be clear as to what exactly is *given* in the quantum algorithm. The quantum algorithm does not oracle-query f, rather it oracle-queries U_f, the unitary operator associated to f.

Further, the "input" that we send to U_f need not be a "pure" outcome, it could be a state with any mix of amplitudes of the various outcomes.

2.4 The Hadamard gate

Consider a qubit (state space is $\mathbb{C}^2$). The Hadamard gate takes this as input and outputs another qubit, and its action on the basis $|0\rangle, |1\rangle$ is defined as follows:

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$|1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

The Hadamard gate (called H) can be thought of as a particular instance of what we will later see as a *rotation gate* – it rotates the basis by an angle of $\pi/4$.

The Hadamard gate acts on each qubit. Hence, if the state space has n qubits, we can consider the n^{th} tensor power of the Hadamard gate. This is a unitary operator that does the Hadamard on *each* gate. This tensor power is often denoted as $H^{\otimes n}$.

Let's see what happens if we apply $H^{\otimes n}$ to $|0\rangle^{\otimes n}$. We'll get:

$$\begin{aligned} H^{\otimes n}(|0\rangle^{\otimes n}) &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \\ \implies H^{\otimes n}(|0\rangle^{\otimes n}) &= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \end{aligned}$$

Note that applying the inverse of the Hadamard gate again retrieves for us the origina $|0\rangle^{\otimes n}$.

2.5 The solution

The idea is to use the Hadamard gate to *cancel* the effect of the 0s and the 1s.

1. Start with a state where all qubits are $|0\rangle$
2. Apply the Hadamard transform $H^{\otimes n}$ to get a state where all qubits are $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. By the calculation done above, the new state is $1/2^{n/2}$ times the sum of all possible outcomes (classical states) of the state space.
3. Tensor with the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
4. Now apply the operator U_f. Note that U_f applied to a pure outcome x is:

$$x \otimes \frac{|f(x)\rangle - |1 + f(x)\rangle}{2^{(n+1)/2}}$$

which simplifies to:

$$x \otimes (-1)^{f(x)} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Hence the effect of U_f on the current state is:

$$\sum_{x \in \{0,1\}^n} x \otimes (-1)^{f(x)} \frac{|0\rangle - |1\rangle}{2^{(n+1)/2}}$$

2.6 For a constant function

In the case that f is constant, the second term in the tensor product becomes constant, and pulling the $(-1)^{f(x)}$ out (which after all only controls the phase), we'll get:

$$(\sum_{x} \in \{0,1\}^n x) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Now, applying the inverse Hadamard transform to the first n qubits, we retrieve $|0\rangle^{\otimes n} \otimes \frac{|0\rangle-|1\rangle}{2^{(n+1)/2}}$. Thus, performing a measurement on the first n coordinates yields $|0\rangle^{\otimes n}$ with certainty.

2.7 For a balanced function

In the case that f is balanced, we get exactly half the x's added with a positive sign, and half the x's added with a negative sign. Now, when we apply the inverse Hadamard transform to this state, we will get a quantum state that will have nonzero coefficients for all the places where the function takes the value 1.

2.8 The upshot

The upshot is as follows:

- We use the Hadamard transform to obtain a uniform superposition of all the possible input states, and then apply the unitary operator to this, tensored with $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- We then again apply the inverse Hadamard transform to the output qubit and obtain the "aggregate" value of the function, hence any measurement gives us the answer.