CS 410/510 Introduction to Quantum Computing

Lecture 3

Portland State U, Spring 2017 — *April 11, 2017*

Lecturer: Fang Song — *Scribe: Ben Hamlin*

VERSION: APRIL 24, 2017

1 Measurement

What is it doing?

Measurement in the standard, or "computational" basis:

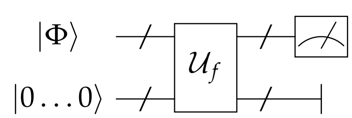
$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{C}^2 \qquad \text{where } |\alpha|^2 + |\beta|^2 = 1$$

- α and β are "amplitudes".
- Projects $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ onto one of $\begin{pmatrix}0\\ 1\end{pmatrix}$ or $\begin{pmatrix}1\\ 0\end{pmatrix}$.
- Probability is magnitude: $|\alpha|^2$ or $|\beta|^2$.

We can also measure in other orthonormal bases, e.g., the diagonal basis:

$$\{|+\rangle, |-\rangle\} = \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} \right\}$$

2 A General Quantum Circuit



- $|\Phi\rangle$ is an n-qubit register.
- The lower register are poly(n) scrap—or "ancillary"—qubits.
- We measure m qubits at the end and discard the rest.

Note that we only measure at the end. Is this too restrictive? No

Principle of Deferred Measurement:

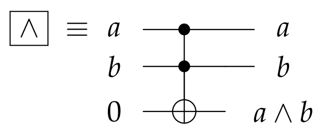
Theorem 1. *Informally: A quantum circuit with intermediate measurement can be simulated by a quantum circuit thet only measures at the end with linear overhead.*

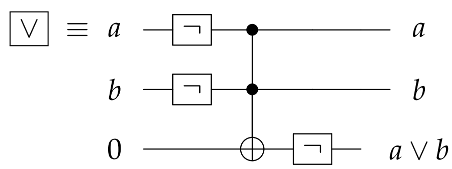
How? For any intermediate measurement on register A, replace it by introducing an ancillary register B and apply CNOT gate with A being the control and B as the target. A goes through whatever operation that comes next and B is left untouched till the endo of computation at which point it gets measured (i.e. discarded). The actual output registers will have the same distribution as the original circuit. Clearly the *overhead* of the transformation is only linear in the size of the original circuit.

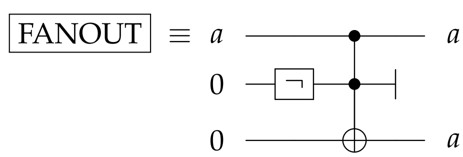
3 Reversible Computation

Is a quantum circuit at least as powerful as a classical circuit? Yes.

- Since quantum gates are unitary matrices, they are reversible (bijective).
- Classical gates like $\boxed{\wedge}$ are *not* reversible.
- We can simulate classical gates reversibly with extra bits and Toffoli gate:

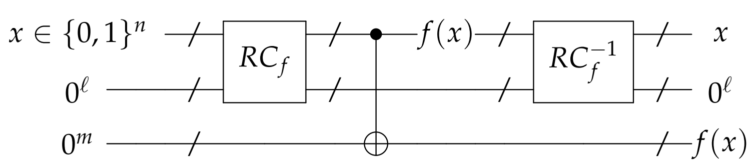






Theorem 2. *Informally: A classical circuit C_f implementing an arbitrary function $f : \{0,1\}^n \to \{0,1\}^m$ using $\boxed{\wedge}$, $\boxed{\vee}$, and $\boxed{\neg}$ can be simulated by a reversible circuit RC_f using poly(n) $\boxed{\neg}$ and Toffoli gates. Such a reversible circuit will have an additional $\ell = poly(n)$ junk input bits and an additional $n + \ell - m$ output junk bits.*

We can clean up the junk bits from Theorem 2. Given RC_f, we construct RC_f^{-1} by flipping the order of application. Then we construct $U_f : (x, 0^m) \mapsto (x, f(x))$ by composing the two:



4 The Power of Quantum Circuits

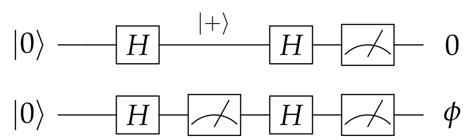
U_f can be implemented as a quantum circuit, since it is unitary. And since the above construction is polynomial in time and space complexity,

$$P \subseteq BQP$$

And since a quantum circuit has randomness (via applying H and measuring),

$$BPP \subseteq BQP$$

Can quantum algorithms do better than their classical counterparts? Consider the following toy example:



(1)

(2)

$$\phi = \begin{cases} 0 & \text{w.p. } \frac{1}{2} \\ 1 & \text{w.p. } \frac{1}{2} \end{cases}$$

In (1), defering measurement allow amplitudes to interfere, eliminating the possibility of evaluating to 1, whereas in (2), measuring after each gate limits us to classical probabilities.

Quantum speedup uses interference to

- reinforce the amplitudes of outcomes we want, and
- cancel out the amplitudes of "undesired" outcomes.

5 Query Model

Given:

- An oracle $O_f : (|x\rangle \otimes |y\rangle) \mapsto (|x\rangle \otimes |f(x) \oplus y\rangle)$ for the function $f(\cdot)$.
- O_f is a quantum circuit that can be queried in superposition.

Goal:

- Compute some information about $f(\cdot)$ by querying O_f.
- Complexity calculated in number of queries.
- Ideally pre-/post-processing is also time-efficient (polynomial), but that's not the emphasis.

Why do we study this model?

- Simple and easy to analyze.
- Captures the essence of QC and provides insight.
- Despite its generality, captures concrete problems, such as factoring.

6 Deutsch's Problem and Algorithm

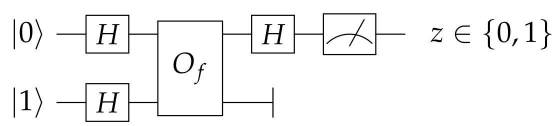
Given:

- A function $f : \{0,1\} \to \{0,1\}$.
- Classically, 2 queries are necessary and sufficient.

Goal: Decide whether $f(\cdot)$ is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$).

Classical algorithms: no matter deterministic or randomized, it is easy to verify that 2 queries are both sufficient and necessary to solve this problems. However, there is a *quantum* algorithm that needs only **1** query.

Quantum Algorithm:



- $f(\cdot)$ is balanced iff $z = 1$.
- 1 query is sufficient.