Introduction to Quantum Computing

David Bromley

The Map is Not the Territory

There exists a distinction between the mathematical model and the physical realizations. We deal with the math

- Regular, "Classical" computer: bits
  - Mathematical Model: 0, 1
  - Physical Implementation: High/Low Voltage
- Quantum computer: qubits
  - Mathematical Model: To be continued...
  - Physical Implementation: Spin of an electron, many others

However, the model is informed by our current best understanding of physical reality, which turns out to be very weird

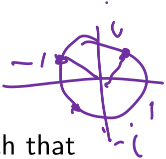
Whats in a Qubit?

Like a classical bit has a state: 0 or 1, a qubit has a state

- Two important states are $|0\rangle, |1\rangle$. Quantum analogies to 0, 1

However, the difference from classical is that a qubit can be in a superposition of states:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$



where α, β are complex numbers called amplitudes such that $|\alpha|^2 + |\beta|^2 = 1$

- Formally, the state is a unit vector in a two-dimensional complex vector space.
  - $|0\rangle, |1\rangle$ form an orthonormal basis

A Qubit by Any Other Name

We can examine a bit to determine if its 0 or 1.
However, we cannot examine a qubit to determine
$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$
Instead, when we look at a qubit, we see

- 0 with probability $|\alpha|^2$
- 1 with probability $|\beta|^2$

This is weird! Normally, there is a direct correspondence between what we see and our abstract model.
Further, after looking, the qubit changes!
If we saw 0, then $|\psi\rangle \to |0\rangle$. If we saw 1, then $|\psi\rangle \to |1\rangle$
The art of quantum algorithms is changing amplitudes so we get the "right" answer with high probability

Multiple Qubits

Two Qubit Case:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{1}\,|11\rangle$$

where, again, $\sum_{x\in\{0,1\}^2} \alpha_x = 1$

Note $|x_1 x_2\rangle = |x_1\rangle \otimes |x_2\rangle = |x_1\rangle\,|x_2\rangle$

What if we just measure just one? Then we get 0 with prob. $|\alpha_{00}|^2 + |\alpha_{01}|^2$ and if so the new state is

$$|\psi\rangle \to |\psi'\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}\,|00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}\,|01\rangle$$

In General, n qubits:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x\,|x\rangle$$

Weird! 2^n numbers evolving in time (but hidden)

Manipulation of Qubits

Much like we manipulate bits via logic gates, we manipulate qubits via quantum gates.

Important example: Hadamard Gate H

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$H(\alpha|0\rangle + \beta|1\rangle) = \alpha H(|0\rangle) + \beta H(|1\rangle) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

$$H(|00\rangle) = H(|0\rangle) \otimes H(|0\rangle) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Formally, H is a unitary matrix. This is true in general for quantum gates.

- Unitary: $H^{-1} = H^{\dagger}$ (note: reversible)

So What?

We will see an example of quantum weirdness being very useful

Problem:

Given a function $f : \{0,1\}^n \to \{0,1\}$, determine whether:

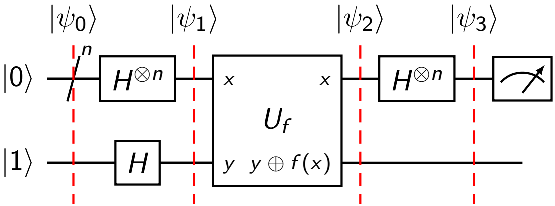
- f is balanced: $f(x) = 0$ for exactly $1/2$ of inputs
- Or f is constant: $f(x)$ is the same for all x

Classical: Need to evaluate $f(x)$ $2^{n-1} + 1$ times.

Quantum: Need just one evaluation!

Quantum Solution (Deutch-Jozsa Algorithm)

The quantum circuit:



We start with an initial state

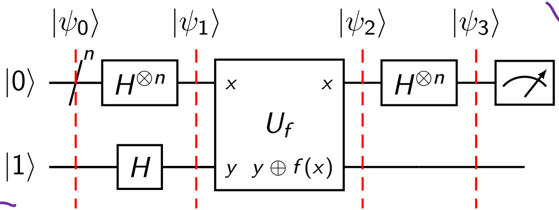
$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

We then apply the Hadamard gate to every qubit, yielding

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle (|0\rangle - |1\rangle)$$

Deutch-Jozsa Algorithm Continued

$U_f^2 = I$



$|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$

$\mapsto |x, y \oplus f(x) \oplus f(x)\rangle$

$y \oplus f(x) \oplus f(x) = y$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle \left(|0\rangle - |1\rangle\right)$$

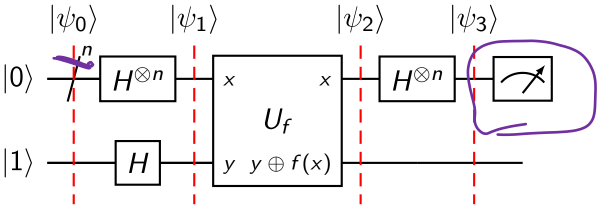
The quantum implementation of f maps $|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle \left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right)$$

We have moved $f(x)$ to the amplitude!

Deutch-Jozsa Algorithm Continued[2]



$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

We know apply the Hadamard gate on the first n qubits. We use the relation (exercise) $x = x_1 x_2 \cdots x_n,\ z = z_1 \cdots z_n$

$$H^{\otimes n}(|x\rangle) = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z} |z\rangle$$ $x \cdot z = x_1 z_1 \oplus + \dots x_n z_n$

to yield

$$|\psi_3\rangle = \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \frac{1}{2^n} (-1)^{x\cdot z + f(x)} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Deutch-Jozsa Algorithm Continued[3]

$$|\psi_3\rangle = \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{x\cdot z+f(x)}|z\rangle \left[\cancel{\frac{|0\rangle-|1\rangle}{\sqrt{2}}}\right]$$

We now measure the first n qubits.

Note that the state $|0\rangle^{\otimes n}$ has amplitude

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = \begin{cases} \pm 1 & f \text{ constant} \\ 0 & f \text{ balanced} \end{cases}$$

Thus, if we see all 0s, then f is constant, else its balanced!

This is an exponential speedup over classical solution