An Introduction to Quantum Computation and Quantum Information

Ben Johnson

Graduate Group in Applied Math
University of California, Davis

March 13, 2009
A bit of history

- Benioff 1982: First paper published mentioning quantum computing
- Feynman 1982: Use a quantum computer for quantum simulation
- Deutch 1985: First formal definition of a quantum computer and examples of quantum algorithms
Basics of quantum computation

- Qubit: Quantum bit - fundamental element of quantum computation
- 1 qubit in superposition

\[ \alpha_0 |0\rangle + \alpha_1 |1\rangle, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1 \]

- \( p(0) = |\alpha_0|^2 \), and \( p(1) = |\alpha_1|^2 \)
Qubits continued

- 2 qubits in superposition of 4 basis states:
  \[ \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \]

- \( p(00) = |\alpha_{00}|^2 \), etc., and
  \[ |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \]

- \( n \) qubits live in a Hilbert space, \( \mathcal{H} \sim \mathbb{C}^{2^n} \)
Qubits continued

- Distinct 1-qubit states with identical probabilities
  \[ H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \quad \text{and} \quad H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \]

- Important states for quantum computation
Operators on qubits

- Require operator to be norm preserving and reversible
- $\Rightarrow$ unitary operators ($UU^* = I$)
- Examples: Hadamard gate and Z gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- *Exception*: Measurement. Non-reversible operation that fixes the qubit into a particular state.
Consider $f : \{0, 1\} \rightarrow \{0, 1\}$. $f(x) = y$ There are 4 such functions:

<table>
<thead>
<tr>
<th>$x = 0$</th>
<th>$x = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_0$</td>
<td>0</td>
</tr>
<tr>
<td>$f_1$</td>
<td>0</td>
</tr>
<tr>
<td>$f_2$</td>
<td>1</td>
</tr>
<tr>
<td>$f_3$</td>
<td>1</td>
</tr>
</tbody>
</table>

Claim: With one function call, $U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$, we can determine if $f$ is a constant ($f_0$ or $f_3$) or not.
Deutsch continued

- Start input and output tapes as $|0\rangle|0\rangle$, apply NOT gate, then Hadamard gate to both registers.

\[
(H \otimes H)(X \otimes X)|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\]

\[
= \frac{1}{2} (|0\rangle|0\rangle - |1\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle)
\]

- Use this as input to operator $U_f$:

\[
\frac{1}{2} (|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1 + f(0)\rangle + |1\rangle|1 + f(1)\rangle)
\]
Deutsch continued

- If $f(0) = f(1)$, we have
  \[
  \frac{1}{\sqrt{2}} \left[ (|0\rangle - |1\rangle) \frac{1}{\sqrt{2}} (|f(0)\rangle - |1 + f(0)\rangle) \right]
  \]

- If $f(0) \neq f(1)$ we have
  \[
  \frac{1}{\sqrt{2}} \left[ (|0\rangle + |1\rangle) \frac{1}{\sqrt{2}} (|f(0)\rangle - |1 + f(0)\rangle) \right]
  \]

- Apply Hadamard gate to input register...
Deutsch finale

- If $f(0) = f(1)$, we get
  \[ |1\rangle \frac{1}{\sqrt{2}} (|f(0)\rangle - |1 + f(0)\rangle) \]

- If $f(0) \neq f(1)$, we get
  \[ |0\rangle \frac{1}{\sqrt{2}} (|f(0)\rangle - |1 + f(0)\rangle) \]

- Input bit $|0\rangle$ or $|1\rangle$ tells us with probability 1 if $f$ is constant or not!

- More generally: if $x \in \{0, 1\}^n$, only need 1 call, versus up to $\frac{2^n}{2} + 1$ for classical
We may apply the above ideas to more practical situations

- Bernstein-Vazirani problem:
  \[ f(x) = a \cdot x = a_0 x_0 \oplus ... \oplus a_{n-1} x_{n-1} \] for some \( a < 2^n \), find \( a \).

- Classical computer, require \( n \) calls to determine the \( n \) bits of \( a \).

- Quantum: 1 call to \( f \)
More applications

- Simon’s Problem: $f$ is periodic under bit-wise addition, 
  \[ f(x \oplus a) = f(x) \] for all $x$. Find $a$.
- Classical computer: exponential in $n = |a|$
- Quantum: linear ($\sim n + 20$)
- Uses probabilistic aspects of computation
Density matrices

- Let a quantum system be in state $|\psi_i\rangle$ with probability $p_i$. Consider the ensemble $\{p_i, |\psi_i\rangle\}$.
- A density matrix $\rho$, with $\text{tr}(\rho) = 1$ that describes the state of the quantum system

$$\rho := \sum_i p_i |\psi_i\rangle \langle \psi_i|$$

- e.g. $|\phi\rangle = \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 1|)$ has density matrix

$$\rho_\phi = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$
Von Neumann Entropy

- Quantum analog to Shannon entropy

\[ S(\rho) = -\text{tr}(\rho \log \rho) \]

or

\[ S(\rho) = -\sum_x \lambda_x \log \lambda_x, \text{ where } \lambda_x \in \Lambda(\rho) \]

- Compute entropy from previous example. Eigenvalues of \( \rho_\phi \) are 1, 1. \( \Rightarrow S(\rho_\phi) = 1 \), as expected.
Properties

- Non-negative: $S(\rho) \geq 0$.
- Bounded: $S(\rho) \leq \log |\mathcal{H}| (= n$ for $n$ qubits$)$
- Joint entropy: $S(A, B) = -\text{tr}(\rho_{AB} \log \rho_{AB})$
- Conditional entropy: $S(A|B) = S(A, B) - S(B)$
- Mutual information: $S(A; B) = S(A) + S(B) - S(A, B) = S(A) - S(A|B) = S(B) - S(B|A)$
Difference between Von Neumann and Shannon entropy

Let $|AB\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$

$S(A, B) = 0$ (pure state)

But $\rho_A = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\Rightarrow S(B|A) = S(A, B) - S(A) < 0$ - not possible with Shannon entropy