An Introduction to Quantum Computation

Sandy Irani
Department of Computer Science
University of California, Irvine
“Simulating Physics with Computers”

“Simulating Physics with Computers”


Is it possible to build computers that use the laws of quantum mechanics to compute?
The Week in Tech:
Google’s Quantum Leap

The company can run esoteric calculations on exotic new hardware faster than is possible on a supercomputer. It’s an achievement of little practical use, but still important.
Church-Turing Thesis

“Until recently, every computer on the planet – from a 1960’s mainframe to your iPhone...- has operated by the same set of rules. These were the rules that Charles Babbage understood in the 1830’s and that Alan Turing codified in the 1930’s. Through the course of the computer revolution, all that has changed at the lowest level are the numbers: speed, amount of RAM and hard disk, number of parallel processors.”

“But quantum computing is different.”

--Scott Aaronson
NY Times Oct 30, 2019
What’s so special about a Quantum Computer?
Quantum Superposition

\[ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \]
Quantum Superposition

\[ \frac{1}{\sqrt{2}} \]
Quantum Superposition
Implementations of a “Qubit”

• Energy level of an atom
• Spin orientation of an electron
• Polarization of a photon.
• NMR, Ion traps,...
Information: 1 Bit Example (Schrodingers Cat)

- **Classical Information:**
  - A bit is in state 0 or state 1

- **Classical Information with Uncertainty**
  - Bit is 0 with probability $p_0$
  - Bit is 1 with probability $p_1$
  - State $(p_0, p_1)$

- **Quantum Information**
  - State is a superposition over states 0 and 1
  - State is $(\alpha_0, \alpha_1)$ where $\alpha_0, \alpha_1$ are complex.
Information: 1 Bit Example (Schrodinger’s Cat)

• **Classical Information:**
  – A bit is in state 0 or state 1

• **Classical Information with Uncertainty**
  – Bit is 0 with probability \( p_0 \)
  – Bit is 1 with probability \( p_1 \)
  – State \((p_0, p_1)\)

• **Quantum Information**
  – State is a superposition over states 0 and 1
  – State is \((\alpha_0, \alpha_1)\) where \(\alpha_0, \alpha_1\) are complex.
Information: 1 Bit Example
(Schroedinger's Cat)

- **Classical Information:**
  - A bit is in state 0 or state 1

- **Classical Information with Uncertainty**
  - State \((p_0, p_1)\)

- **Quantum Information**
  - State is partly 0 and partly 1
  - State is \((\alpha_0, \alpha_1)\) where \(\alpha_0, \alpha_1\) are complex.

\[
\alpha_1 \begin{aligned} \ket{0} \end{aligned} + \alpha_0 \begin{aligned} \ket{1} \end{aligned}
\]
Information: n Bit Example

- **Classical Information:**
  - State of $n$ bits specified by a string $x$ in $\{0,1\}^n$

- **Classical Information with Uncertainty**
  - State described by probability distribution over $2^n$ possibilities
  - $(p_0, p_1, \ldots, p_{2^n-1})$

- **Quantum Information**
  - State is a superposition over $2^n$ possibilities
  - $(\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1})$, where $\alpha$ is complex

$x = 011$
Information: n Bit Example

• **Classical Information:**
  – State of n bits specified by a string $x$ in $\{0,1\}^n$

• **Classical Information with Uncertainty**
  – State described by probability distribution over $2^n$ possibilities
  – $(p_0, p_1, \ldots, p_{2^n-1})$

• **Quantum Information**
  – State is a superposition over $2^n$ possibilities
  – $(\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1})$, where $\alpha$ is complex
Information: n Bit Example

- **Classical Information:**
  - State of n bits specified by a string \( x \) in \( \{0,1\}^n \)

- **Classical Information with Uncertainty**
  - State described by probability distribution over \( 2^n \) possibilities
  - \( (p_0, p_1, \ldots, p_{2^n-1}) \)

- **Quantum Information**
  - State is a superposition over \( 2^n \) possibilities
  - \( (\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}) \), where \( \alpha \) is complex
• A quantum kilobyte of data
  (8192 qubits)

Encodes $2^{8192}$ complex numbers

$2^{8192} \sim 10^{2466}$

(Number of atoms in the universe $\sim 10^{82}$)
• State of n qubits \((\alpha_0, \ldots, \alpha_{2^n-1})\) stores \(2^n\) complex numbers:

Rich in information

How to use it?
How to access it?
Quantum Measurement

• State of n qubits \( (\alpha_0, \ldots, \alpha_{2^n-1}) \)

• If all n qubits are examined:
  – Outcome is 010 with probability \(|\alpha_{010}|^2\).
Quantum Measurement

- State of n qubits \((\alpha_0, \ldots, \alpha_{2^n-1})\)

- If all n qubits are examined:
  - Outcome is 010 with probability \(|\alpha_{010}|^2\).
  - The measurement causes the state of the system to change:
    » The state “collapses” to 010
Ingredients in Computation

- Store information about a problem to be solved
- Manipulate the information to solve the problem
- Read out an answer
Computer Circuits

The diagram illustrates the operation of a simple computer circuit that uses AND, OR, and NOT gates to process inputs. The inputs are labeled as 0/1, and the outputs are also labeled as 0/1, indicating binary states.
Quantum Circuits

\[
|0\rangle \quad U_1 \quad U_2 \quad U_3 \quad U_4 \quad U_5 \quad U_6 \quad U_7 \quad U_8 \quad M
\]

Input

Time

Read the output by measurement
Interference

[Image from www.thehum.info, due to Dr. Glen MacPherson]
INTERFERENCE

Destructive  Constructive

=  =

[Figure from gwoptics.org]
Quantum Algorithms

Manipulate data so that negative interference causes wrong answers to have small amplitude and right answers to have high amplitude, so that when we measure output, we are likely to get the right answer.
Factoring

• Given a positive integer, find its prime factorization.

• $24 = 2 \times 2 \times 2 \times 3$

Input  Output
Factoring

• RSA-210 =
  2452466449002782119765176635730880184
  6702678767833275974341445171506160083
  0038587216952208399332071549103626827
  1916798640797767232430056005920356312
  4656121846581790410013185929961993381
  7012149335034875870551067
Can Quantum Computers Be Built?

- Key challenge: prevent decoherence (interaction with the environment).
- Can factor N=15 on a quantum computer
- Larger problems will require quantum error correcting codes.
Quantum supremacy using a programmable superconducting processor

Select a “random” quantum circuit (set of interactions)
Then repeatedly sample the outcome.
   One repetition -> one 53-bit string
How Do You Check a Quantum Computer?

• Google estimated that it would take 10,000 years to check using 100,000 conventional computers running the fastest algorithms currently known.

  Simulating the 53 qubit machine requires storing
  \[2^{53} = 9 \text{ quadrillion} = 9 \times 10^{15}\] complex numbers

• Instead...check smaller versions of the same problem – still using massive amounts of computing power.
IBM casts doubt on Google’s claims of quantum supremacy

By Adrian Cho | Oct. 23, 2019, 5:40 AM

Google researchers in Santa Barbara, California, say their advance may lead to near-term applications of quantum computers. ISTOCK.COM/JHVEPHOTO
Next Steps...

• Simulate quantum physics of chemical reactions.
• Quantum error correction
Quantum Computing and Information

- Classical Simulation Of Quantum Systems
- Physical Implementation Of Quantum Computers
- Quantum Information Theory
- Quantum Cryptography
- Quantum Complexity Theory
- Algorithm Design For Quantum Circuits
Research on Quantum Algorithms

• What problems can we compute with an idealized quantum computer of the future?
  1000+ Error-Corrected Qubits

• What problems can we compute more efficiently with ~100 noisy qubits?
  NISQ computers: Near-term Intermediat-Scale Quantum Computers
Quantum Computers for Simulation in Physics
My Research

• Design efficient algorithms on a quantum (or classical) computer that will \textit{provably} compute properties of a quantum system.

  – For what kinds of systems is this possible?

  – Or: give mathematical evidence that there is no efficient way to solve this problem.
Ways to Learn More

- **CS 166 Quantum Computing**
  Prerequisites:
  - Linear Algebra (ICS 6N or Math 3A)
  - Design and Analysis of Algorithms (CS 161)

- Quantum Computing Club @ UCI
  [https://www.qc-uci.club](https://www.qc-uci.club)