Quantum Computation

Instructor: Hossein Aghababa
School of Electrical and Computer Engineering
University of Tehran
Spring 2022

Course Schedule & Evaluation

- Class: Saturday & Monday 10:30—12:00
- TA: TBD
- Midterm:20%
- Final:40%
- Homework: 10%
- Project: 30%

References

- References:
  - Quantum Computation and Quantum Information, Michael A. Nielsen& Isaac L. Chuang, Cambridge, 2010.
    - The majority of slides in this course have been influenced by the materials of this book
  - Quantum Computing Explained, David McMahon, Wiley-IEEE Computer Society, 2007.
  - Quantum Machine Learning, Peter Wittek, Academic Press, 2016.
  - Wikipedia

- The other resources:
  - http://www-ctp.mit.edu/research-quantum.html
  - http://www.iqi.caltech.edu/
  - http://bqic.berkeley.edu/
  - https://uwaterloo.ca/institute-for-quantum-computing/
  - https://quantiki.org/
  - http://www.dwavesys.com/

Which disciplines are involved?

- Computer Science
- Physics
- Mathematics
- Electrical Engineering
- Computer Engineering
- And PHILOSOPHY !!!

Just to mention a few…

Where is the quantum computation now?

MAY 23, 2016 THE GUARDIAN

"It’s a mind-bending concept with the potential to change the world, and Canadian tech company D-Wave claims to have cracked the code

Ever since Charles Babbage’s conceptual, unrealised Analytical Engine in the 1830s, computer science has been trying very hard to race ahead of its time. Particularly over the last 75 years, there have been many astounding developments – the first electronic programmable computer, the first integrated circuit computer, the first microprocessor. But the next anticipated step may be the most revolutionary of all.

Quantum computing is the technology that many scientists, entrepreneurs and big businesses expect to provide a, well, quantum leap into the future."

Outline

- Fundamental Concepts I
- Quantum Computation II
- Quantum Information III

Fundamental Concepts I

- Introduction and Overview
- Introduction to Quantum Mechanics
- Introduction to Computer Science

Quantum Computation II

- Quantum Circuits
- The Quantum Fourier Transform and its Applications
- Quantum Search Algorithms
- Quantum Computers: Physical Realization

Quantum Information III

- Quantum Noise and Quantum Operations
- Distance Measures for Quantum Information
- Quantum Error-Correction
- Entropy and Information
- Quantum Information Theory

Part I: Fundamental concepts

Science offers the boldest metaphysics of the age. It is a thoroughly human construct, driven by the faith that if we dream, press to discover, explain, and dream again, thereby plunging repeatedly into new terrain, the world will somehow come clearer and we will grasp the true strangeness of the universe. And the strangeness will all prove to be connected, and make sense.
– Edward O. Wilson

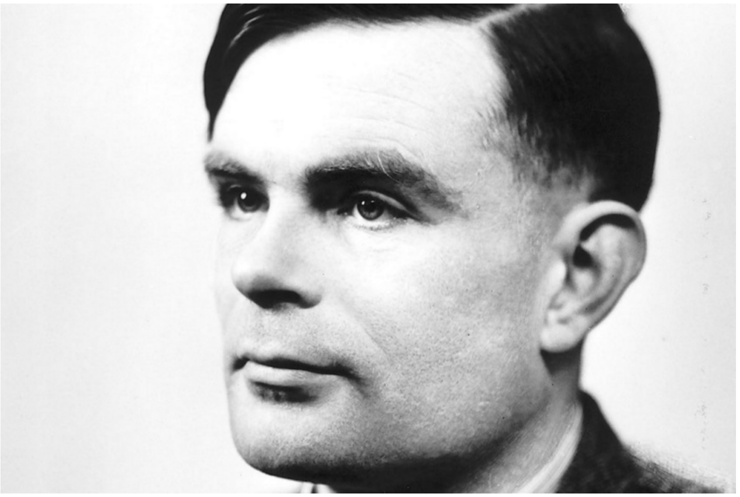
Information is physical.
– Rolf Landauer

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History of Quantum Computation and Quantum Information
  - Any algorithmic process can be simulated efficiently using a Turing machine
  - Any algorithmic process can be simulated efficiently using a probabilistic Turing machine

Alan Turing:

English computer scientist, mathematician, logician, cryptanalyst and theoretical biologist.



Fundamental Concepts-Introduction and Overview-Global Perspectives

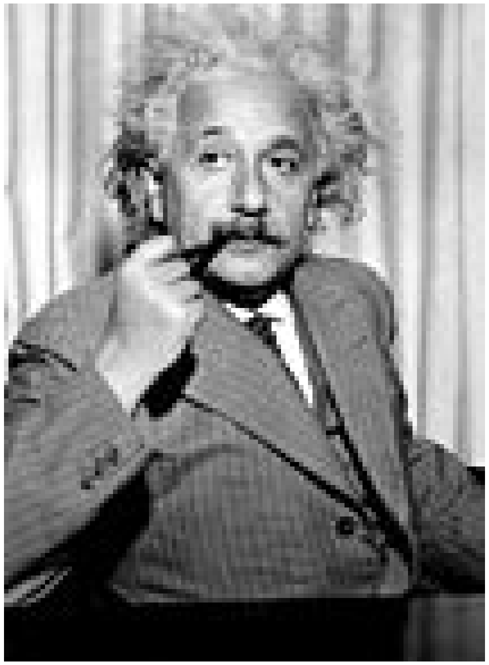
- History
  - Quantum Mechanics

Quantum mechanics has been an indispensable part of science ever since, and has been applied with enormous success to everything under and inside the Sun, including the structure of the atom, nuclear fusion in stars, superconductors, the structure of DNA, and the elementary particles of Nature.
What is quantum mechanics? Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories.

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Quantum Mechanics

The rules of quantum mechanics are simple but even experts find them counterintuitive, and the earliest antecedents of quantum computation and quantum information may be found in the long-standing desire of physicists to better understand quantum mechanics. The best known critic of quantum mechanics, Albert Einstein, went to his grave un-reconciled with the theory he helped invent.



Albert Einstein (1879-1955)

Theoretical Physicist

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Another intellectual triumph of the 20th century: **Computer Science**

    By the time of Hammurabi (circa 1750 B.C.) the Babylonians had developed some fairly sophisticated algorithmic ideas, and it is likely that many of those ideas date to even earlier times
  - Turing Machine (1936) → Universal Turing Machine → Church-Turing Thesis → Jon von Neumann theoretical model
  - Bardin, Brattain, and Shockley (1947) → Transistor
  - Gordon Moore (1965) prediction → Move to a different computing paradigm → possible answer is quantum computation

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Church–Turing thesis: *Any algorithmic process can be simulated efficiently using a Turing machine.*
  - *Efficient or inefficient → Computational complexity*
  - Roughly speaking, an efficient algorithm is one which runs in time polynomial in the size of the problem solved. In contrast, an inefficient algorithm requires super-polynomial (typically exponential) time.
  - *One possible challenge for Church-Turing thesis → Analog computers → There was a problem: Noise*
  - *The same challenge (Noise) for quantum computation → successfully solved by quantum error-correcting codes and fault-tolerant quantum computation*

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Another challenge to Church-Turing thesis: Randomized algorithms → an *ad hoc* modification:

    Any algorithmic process can be simulated efficiently using a probabilistic Turing machine.
  - David Deutsch (1985) → Universal Quantum Computer
  - Better choices in future? String theory, quantum gravity, … → we simply don't know

David Deutsch:
Israeli-born
British physicist at
the University of Oxford

Fundamental Concepts-Introduction and Overview-Global Perspectives

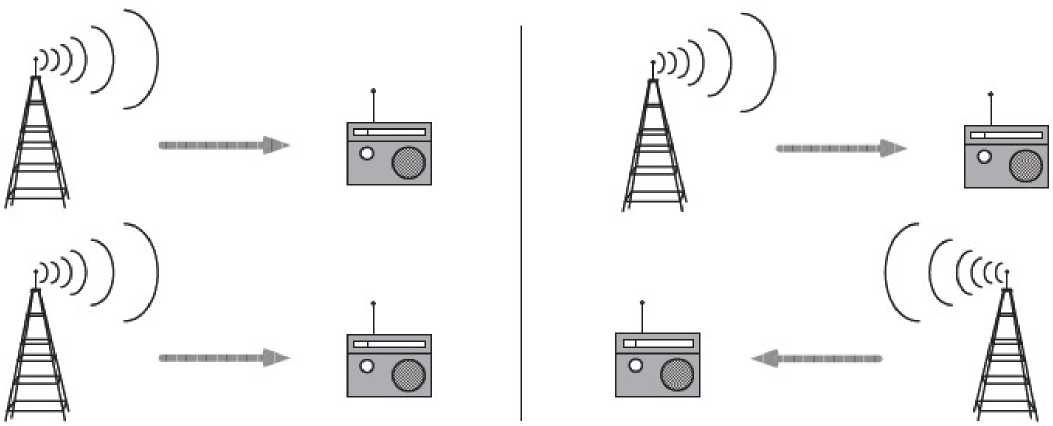
- History
  - Peter Shor (1994) →
    - finding the prime factors of an integer
    - ‘discrete logarithm’ problem
  - Lov Grover (1995) →
    - search through some unstructured search space
  - To design good quantum algorithms:
    - Turn off classical intuition
    - Better than any existing classical algorithm

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Claude Shannon (1948) → Information Theory
  - Ben Schumacher (1995) → Quantum bit (qubit) → Quantum information theory
  - Peter Shor et al (1996) → Quantum error-correcting codes →protect the quantum states against noise
  - Charles Bennett and Stephen Wiesner (1992) → transmitting two classical bits of information while only transmitting one quantum bit → dubbed as super-dense coding

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Cryptography



Classically, if we have two very noisy channels of zero capacity running side by side, then the combined channel has zero capacity to send information. Not surprisingly, if we reverse the direction of one of the channels, we still have zero capacity to send information. Quantum mechanically, reversing one of the zero capacity channels can actually allow us to send information!

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - The most important distinction is between *private key cryptosystems and public key cryptosystems.*
  - quantum mechanics can be used to do key distribution in such a way that Alice and Bob's security can not be compromised → Quantum cryptography
  - Observation in general disturbs the system being observed → eavesdropper will be visible
  - *RSA cryptosystem*→ the most widely deployed public key cryptosystem → a fine balance of security and practical usability → factoring is a problem hard to solve on a classical computer

Shor's fast algorithm for factoring on a quantum computer could be used to break RSA!

Fundamental Concepts-Introduction and Overview-Global Perspectives

- History
  - Quantum Entanglement → the most important effect in quantum computation and information applications → entanglement is iron to the classical world's bronze age

History of quantum computation and information in summary
Quantum Mechanics
Computer Science
Information Theory
Cryptography

Fundamental Concepts-Introduction and Overview-Global Perspectives

- *Future Directions:*
  - *Think physically about computation*
  - *Think computationally about physics*

Fundamental Concepts-Introduction and Overview-Quantum Bits

- Bit → fundamental concept of classical computation and classical information

- Quantum bit (qubit) → fundamental concept of quantum computation and quantum information

Fundamental Concepts-Introduction and Overview-Quantum Bits

- What is a qubit? Just as a classical bit has a *state* – *either 0 or 1 – a qubit also* has a state.
- Two possible states for a qubit are the states

$$|0\rangle \qquad\qquad |1\rangle$$

- $|\ \rangle$ *is called Dirac notation* → states in quantum mechanics
- The difference between bits and qubits is that a qubit can be in a state *other than* $|0\rangle$ *or* $|1\rangle$

Fundamental Concepts-Introduction and Overview-Quantum Bits

- Linear combinations of states → super-positions:

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

- α and β → complex numbers
- When we measure a qubit we get either the result 0, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$
- $|\alpha|^2 + |\beta|^2 = 1$, since the probabilities must sum to one.

Fundamental Concepts-Introduction and Overview-Quantum Bits

- a qubit can exist in a *continuum of states*
- For example, a qubit can be in the state

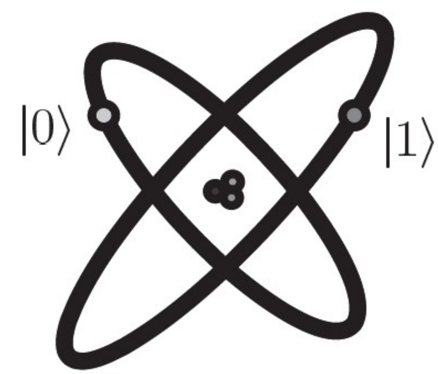
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle ,$$

- when measured, gives the result 0 fifty percent ($|1/\sqrt{2}|^2$) of the time, and the result 1 fifty percent of the time.

Fundamental Concepts-Introduction and Overview-Quantum Bits

- Qubits are real:
  - as the two different polarizations of a photon
  - as the alignment of a nuclear spin in a uniform magnetic field
  - as two states of an electron orbiting a single atom

Qubit represented by two electronic levels in an atom.



Fundamental Concepts-Introduction and Overview-Quantum Bits

- Since, $|\alpha|^2 + |\beta|^2 = 1$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \longrightarrow |\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right),$$

- Θ, ϕ, and ɣ are real numbers but we will see later that $e^{i\gamma}$ has no observable effect →

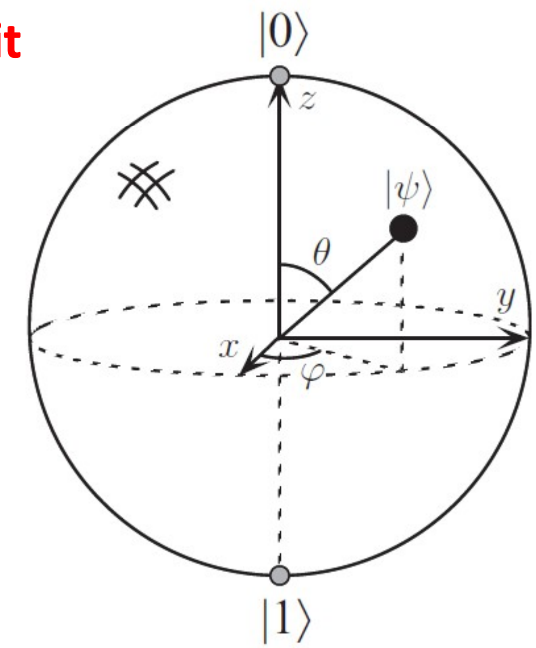
$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \longrightarrow$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle.$$

Fundamental Concepts-Introduction and Overview-Quantum Bits

- Θ and ϕ define a point on the unit three-dimensional sphere → Bloch Sphere

Bloch sphere representation of a qubit



Fundamental Concepts-Introduction and Overview-Quantum Bits

- How much information is represented by a qubit? entire text of Shakespeare in the infinite binary expansion of θ ??!!
- measurement *changes* the state of a qubit, collapsing it from its superposition *to the specific state* consistent with the measurement result (**Philosophical Controversy**)
- this behavior is simply one of the *fundamental postulates of quantum mechanics*
- how much information is represented by a qubit *if we do not measure it?* Nature conceals a great deal of 'hidden information'

Fundamental Concepts-Introduction and Overview-Quantum Bits

- Multiple Qubits

Hilbert space is a big place.
– Carlton Caves

  - two classical bits → possible states, 00, 01, 10, and 11
- Correspondingly, a two qubit system has four *computational basis states* $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- A pair of qubits can also exist in superpositions of these four states → a complex coefficient → amplitude
- $$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

Fundamental Concepts-Introduction and Overview-Quantum Bits

- Similar to the case for a single qubit, the measurement result x (= 00, 01, 10 or 11) occurs with probability $|\alpha_x|^2$

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

- For a two qubit system, we could measure just a subset of the qubits, say the first qubit
- measuring the first qubit alone gives 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, leaving the post-measurement state:

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

Fundamental Concepts-Introduction and Overview-Quantum Bits

- An important two qubit state is the *Bell state or EPR pair*

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

John Stewart Bell (1928 - 1990), a truly deep and serious thinker, was one of the leading experts on the foundations of quantum mechanics

- This innocuous-looking state is responsible for many surprises in quantum computation especially in quantum teleportation and super-dense coding, which we'll come to later

Fundamental Concepts-Introduction and Overview-Quantum Bits

- The Bell state has the property that upon measuring the first qubit, one obtains two possible results: 0 with probability 1/2, *leaving the post-measurement state* $|\varphi'\rangle = |00\rangle$
- and 1 with probability 1/2, *leaving* $|\varphi'\rangle = |11\rangle$
- As a result, a measurement of the second qubit always gives the same result as the measurement of the first qubit. That is, the measurement outcomes are *correlated.*
- *We will return to the properties of Bell State later!*