SAND2012-8563P

Quantum Information Processing and Error Correction

An Overview

Uzoma Onunkwo (09336)

Sandia National Laboratories
Albuquerque, NM

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the United States Department of Energy under Contract DE-AC04-94AL85000

October 4, 2012

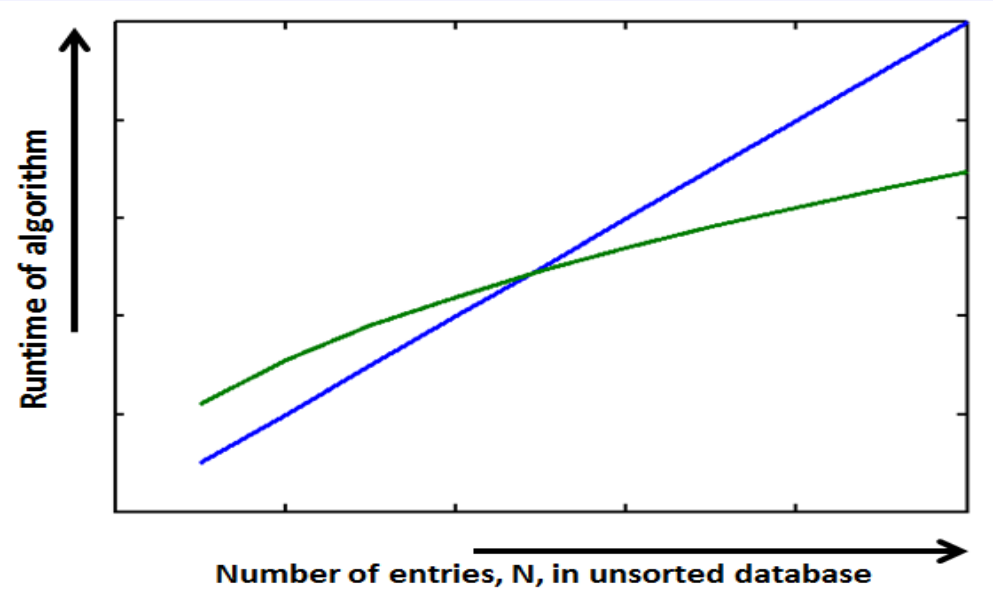
1. Why quantum computing
   - New realms of computational power and information security
   - In the news
   - Large funding and research focus
2. Realizing a quantum computer
   - Quantum computing 101: A compare and contrast approach
   - Pre-requisites for the existence of a quantum computer
   - Physical realization and models of quantum computing
   - Quantum computer vs. Classical computer
3. Error correction in quantum information processing
   - Overview of important quantum gates (operations)
   - A classical error correction example
   - Quantum error correction: an overview
4. Summary

Outline

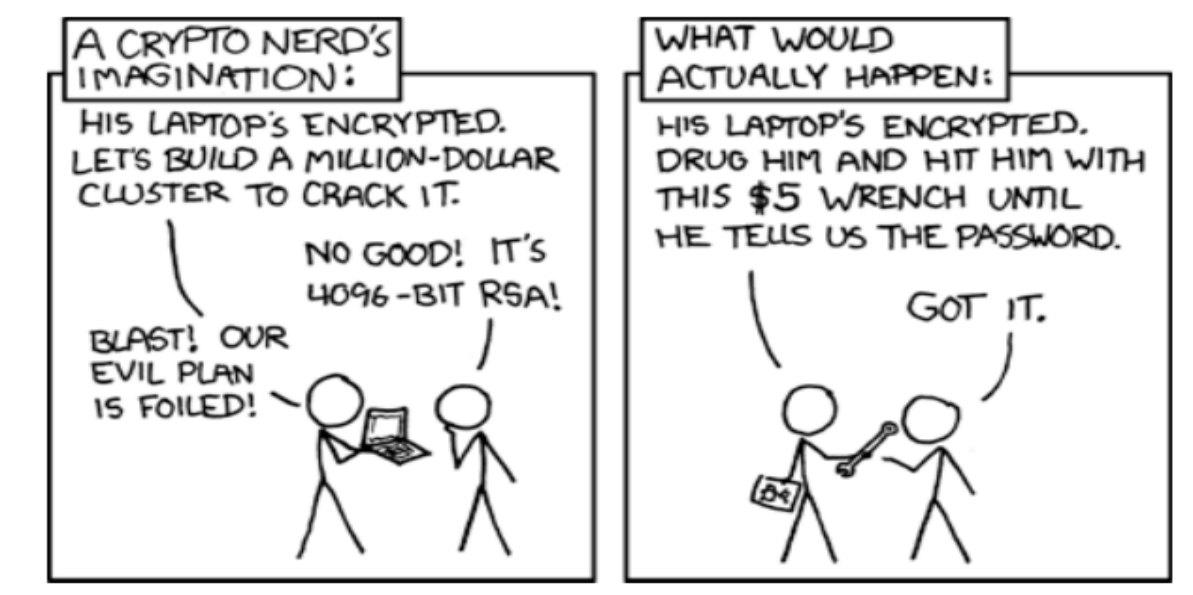
1. Why quantum computing
   - New realms of computational power and information security
   - In the news
   - Large funding and research focus
2. Realizing a quantum computer
   - Quantum computing 101: A compare and contrast approach
   - Pre-requisites for the existence of a quantum computer
   - Physical realization and models of quantum computing
   - Quantum computer vs. Classical computer
3. Error correction in quantum information processing
   - Overview of important quantum gates (operations)
   - A classical error correction example
   - Quantum error correction: an overview
4. Summary

High gain in unsorted database search

- Searching an unsorted database with N entries
  - Best known **classical** method, linear search of database, runs in time proportional to N
  - Best **quantum** algorithm is called *Grover's method* and runs in time proportional to $\sqrt{N}$
  - **Impact:** database searches, fast estimation of average of a set of numbers



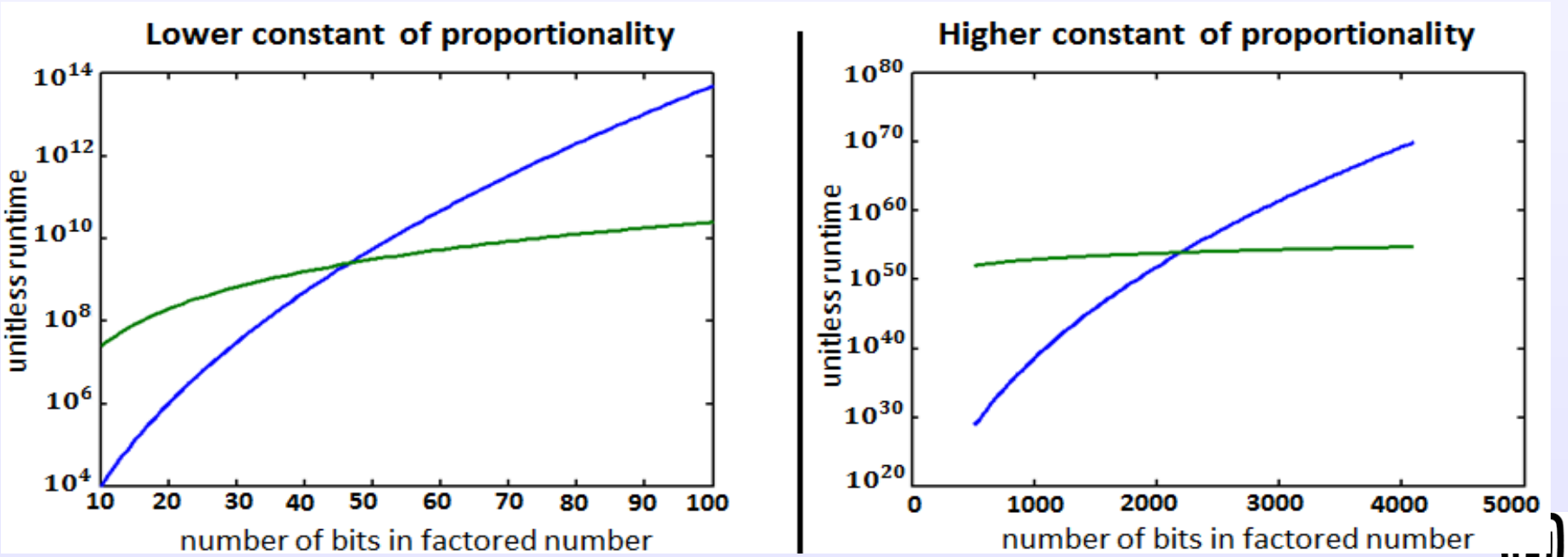
Extra-ordinary gain in prime-factoring of large numbers



Source: http://xkcd.com/538/

Extra-ordinary gain in prime-factoring of large numbers

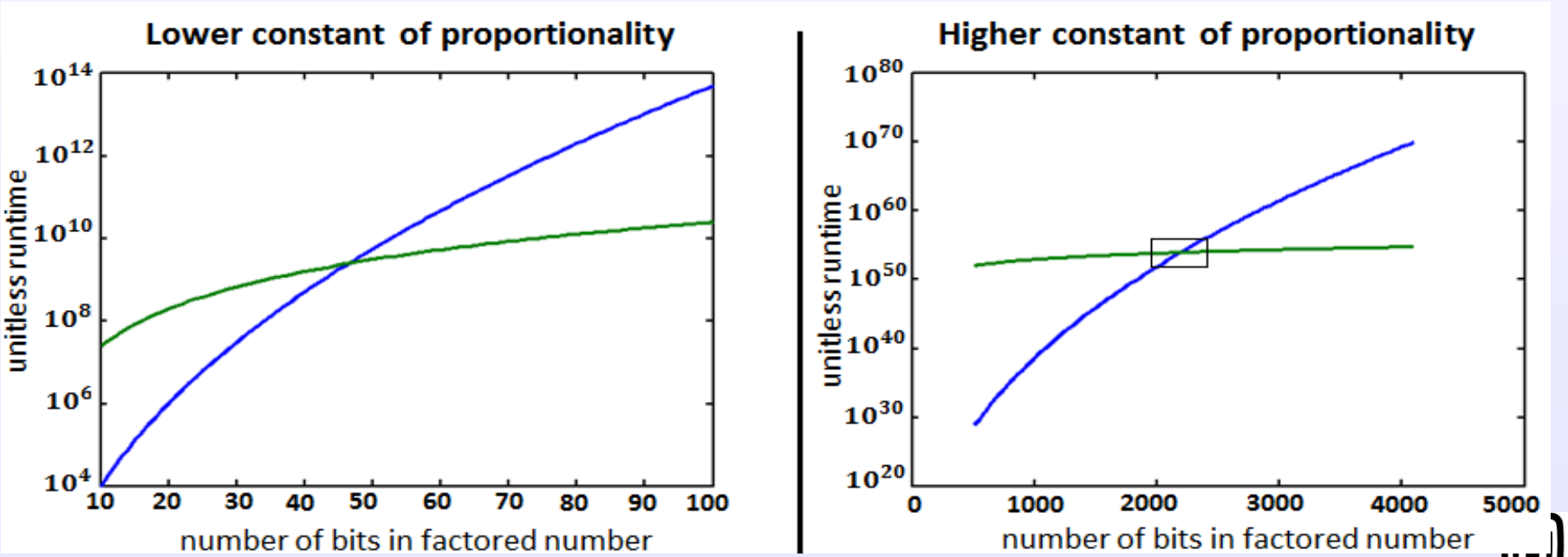
- Factorization of large numbers, N represented by b-bits
  - Best known **classical** method, known as *General Number Field Sieve (GNFS)* is very inefficient
    - Has exponential runtime of $\mathcal{O}\left(\exp\left(\left(\frac{8}{3}\sqrt{b}\log b\right)^{\frac{2}{3}}\right)\right)$
  - Best known **quantum** method known as *Shor's method* is efficient and faster than its GNFS counterpart
    - Has polynomial runtime of $\mathcal{O}\left(b^3\right)$
  - **Impact:** Public-key encryption using RSA security algorithm



Sandia National Laboratories

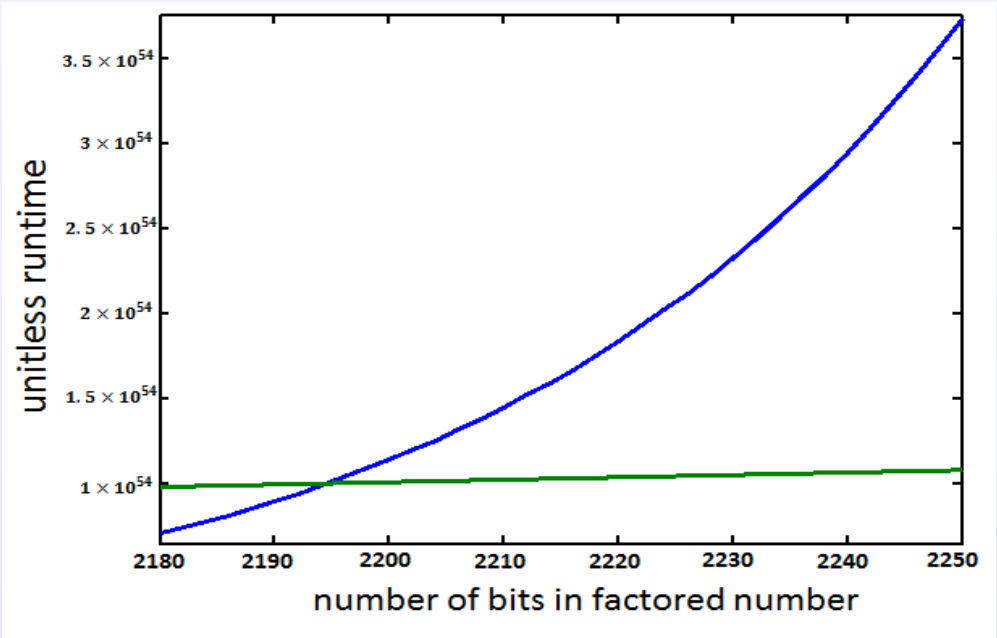
Extra-ordinary gain in prime-factoring of large numbers

- Factorization of large numbers, N represented by b-bits
  - Best known **classical** method, known as *General Number Field Sieve (GNFS)* is very inefficient
    - Has exponential runtime of $\mathcal{O}\left(\exp\left(\left(\frac{8}{3}\sqrt{b}\log b\right)^{\frac{2}{3}}\right)\right)$
  - Best known **quantum** method known as *Shor's method* is efficient and faster than its GNFS counterpart
    - Has polynomial runtime of $\mathcal{O}\left(b^3\right)$
  - **Impact:** Public-key encryption using RSA security algorithm



Extra-ordinary gain in prime-factoring of large numbers

- Factorization of large numbers, N represented by b-bits
  - Best known **classical** method, known as *General Number Field Sieve (GNFS)* is very inefficient
    - Has exponential runtime of $\mathcal{O}\left(\exp\left(\left(\frac{8}{3}\sqrt{b}\log b\right)^{\frac{2}{3}}\right)\right)$
  - Best known **quantum** method known as *Shor's method* is efficient and faster than its GNFS counterpart
    - Has polynomial runtime of $\mathcal{O}\left(b^3\right)$
  - **Impact:** Public-key encryption using RSA security algorithm



Physically vs. Computationally secure encrypted information

- Information security based on physical (nature) not computational constraint for exchanging secure keys
  - The physical constraints are due to natural phenomena:
    - we cannot clone a qubit; a qubit is the basis of information in quantum systems
    - a measured qubit conveys no information about its previous value
  - Commercial companies providing quantum key distribution (QKD) systems are:
    1. **id Quantique** in Geneva, Switzerland,
    2. **MagiQ Technologies** in New York, USA, and
    3. **QuintessenceLabs** in Australia.
  - Current state-of-the-art is secure communication of 1 Mbits/sec over 20 km
  - Impact: Provably secure communications, Cyber security

Motivation: In the news

- Excerpts from Science Daily (http://www.sciencedaily.com)
  - **Major Step Taken Towards 'Unbreakable' Message Exchange (August 3, 2012)**
    Photons have been produced and implemented into a quantum key distribution link, paving the way for unbreakable communication
  - **Quantum Physics: New Insights Into the Remote Control of Quantum Systems (August 6, 2012)**
    Answering questions on resource requirement for achieving quantum information processing
  - **Quantum Cryptography Theory Has a Demonstrated Security Defect (August 7, 2012)**
    Researchers at Tamagawa University challenge the present theory that unconditional security exist in the security theory of quantum key distribution based on true random sequence generation

Motivation: Large research focus

- **Sandia National Laboratories** Quantum Information Science group
- **Microsoft's Station Q** group with focus on topological form of quantum computing, and **Microsoft's QuArC** group with focus on scalable, programmable quantum computer and the optimization of algorithms
- **D-Wave, The Quantum Computing Company** (http://www.dwavesys.com)
- **IBM's Quantum Information** group with focus that includes fault tolerance, error-correction, authentication
- **Georgia Institute of Technology GTQI** group
- **MIT Center for Theoretical Physics**
- **California Institute of Technology IQI** group

Sandia National Laboratories

Outline

1. Why quantum computing
   - New realms of computational power and information security
   - In the news
   - Large funding and research focus
2. Realizing a quantum computer
   - Quantum computing 101: A compare and contrast approach
   - Pre-requisites for the existence of a quantum computer
   - Physical realization and models of quantum computing
   - Quantum computer vs. Classical computer
3. Error correction in quantum information processing
   - Overview of important quantum gates (operations)
   - A classical error correction example
   - Quantum error correction: an overview
4. Summary

Quantum computing 101: *A compare and contrast approach*

	Classical	Quantum
Basis of information	Bits: 0 or 1 2-level system	Qubits: $\|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ infinitely possible vectors or states with the restriction that $\|\|\psi\rangle\|_2 = 1$ e.g., $\|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\|\phi\rangle = \begin{pmatrix} 0.8 \\ 0.6 \end{pmatrix}$
Gates	AND, OR, NOT generally irreversible	Any unitary matrix, M: $(M^\dagger M = MM^\dagger = I)$ e.g., Identity or Idle rotation, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Bit-flip, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ reversible operations
Can transport (qu)bits	Yes	*Yes*
Can clone (copy) (qu)bits	Yes	No
Effect of measurement	Nothing	Destroys original qubit

Cloning qubits is impossible: *A No-go Theorem*

- One can make multiple copies of an *a priori* known qubit, but...
- One cannot make a gadget that makes copy of any arbitrary input qubit

Proof.

If such a gadget existed, then it should do the following: $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \equiv |\psi\psi\rangle$. Let such a gadget be represented by the linear operator, $\mathcal{C}$. The requirement for linearity of the operator comes from Schrödinger's equation. Then,

$$\mathcal{C}\,|\psi\rangle = |\psi\psi\rangle$$

By the same token, we expect

$$\mathcal{C}\,|0\rangle = |00\rangle \quad (1)$$

$$\mathcal{C}\,|1\rangle = |11\rangle \quad (2)$$

$$\mathcal{C}\,(|0\rangle + |1\rangle) = (|00\rangle + |11\rangle) \quad (3)$$

The last line comes from the linearity property of the operator $\mathcal{C}$, which contradicts the expected result of

$$\begin{aligned}\mathcal{C}\,(|0\rangle + |1\rangle) &= (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ &\neq (|00\rangle + |11\rangle)\end{aligned}$$

Thus, no such gadget can exist; we call this the *No-cloning Theorem*. □

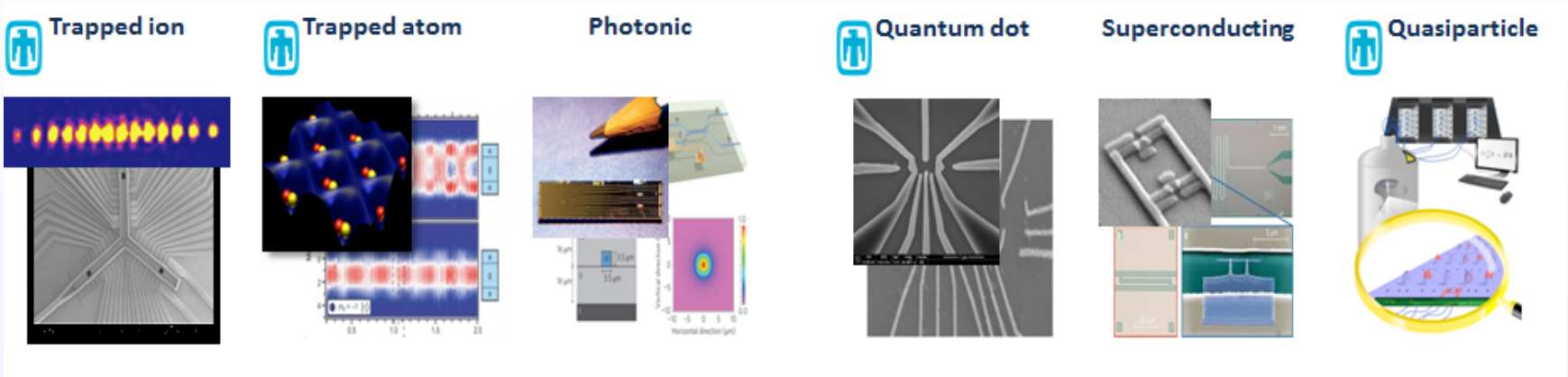
Quantum measurements are "destructive"

- Measurements are projective: qubits are collapsed to an eigenbasis of the measurement operator
- *Think of measurements as observations that done in a chosen reference frame*
- In classical computing, we have the single frame of "1" or "0" for bits, but for quantum computing, we have an infinite set of such reference frame
- A complete set of projective operators, Π_i, $i \in \{0, ..., n-1\}$, for quantum measurement satisfies
  1. $\Pi_i^2 = \Pi_i, \ \forall i$
  2. $\sum_{i=0}^{n-1} \Pi_i = I$
  3. A qubit $|\psi\rangle$ observed with the projection, Π_i, becomes $\Pi_i |\psi\rangle$ with probability $\sqrt{\langle\psi|\Pi_i|\psi\rangle}$
  4. An example is a single-qubit measurement in the *standard* basis with $n = 2$, $\Pi_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\Pi_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Pre-requisites for the existence of a quantum computer[1]

1. Existence of a scalable physical system with well characterized qubits
2. Capability to initialize the state of the qubits to a simple pure state
3. Existence of long relevant decoherence times, much longer than the gate operation time
4. Existence of a universal set of quantum gates
5. Existence of a qubit-specific measurement
6. Capability to inter-convert stationary and "flying" qubits
7. The ability to faithfully transmit flying qubits between specified locations

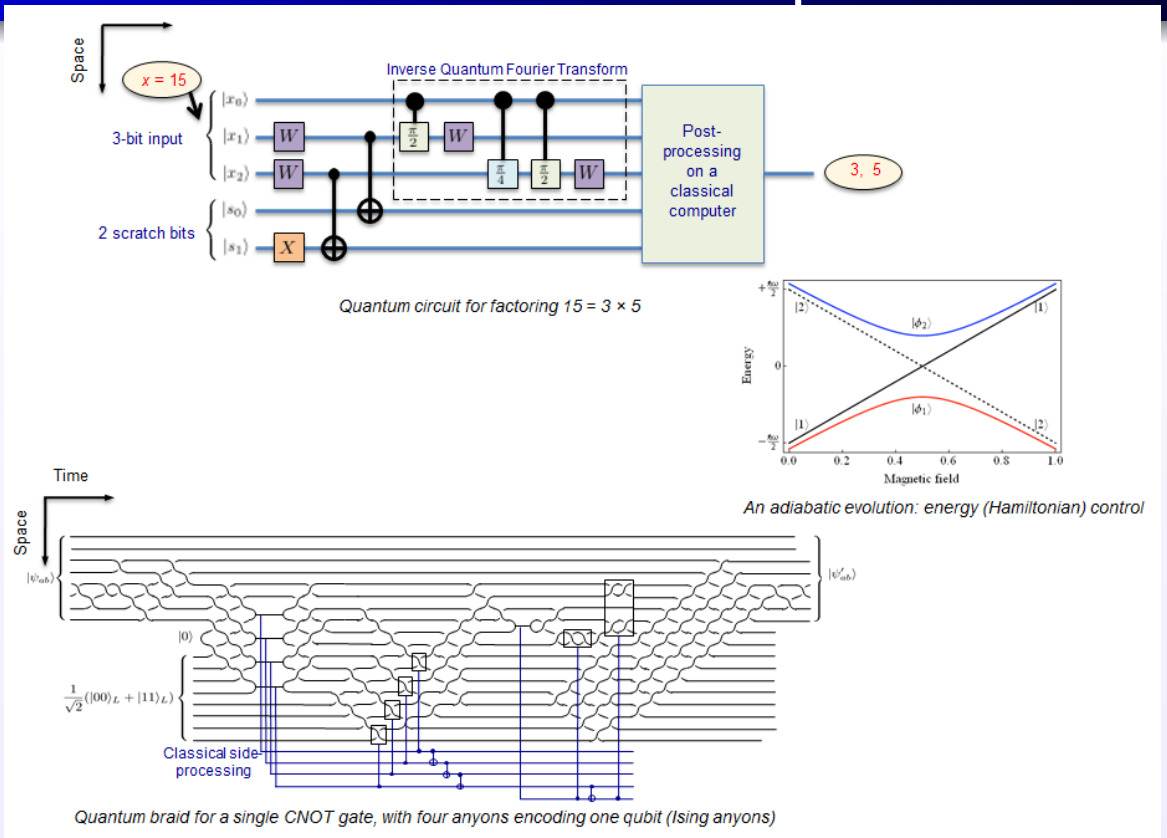
Physical realization and models of quantum computing



Source: Technical Overview presentation on AQUARIUS Grand Challenge (Third EAB)

- Physical realization of qubits; *think of vacuum tubes and transistors for bits*
  - Quantum dots (*non-mobile*)
  - Ion traps (*mobile*)
  - Neutral atom laser (*non-mobile?*)
  - Photons (*mobile*)
  - Superconducting flux (*non-mobile*)

Physical realization and models of quantum computing



Source: Technical Overview presentation on AQUARIUS Grand Challenge (First EAB)

- Models of quantum computing
  - Circuit or network model
  - Adiabatic quantum computing model
  - One-way (Cluster state) computing model

Quantum computer vs. Classical computer

- A quantum algorithm vs. a classical algorithm
  - *Fact*: Every problem that can be solved on a classical computer (CC) can be solved just as "efficiently" on a quantum computer (QC)
  - *Fact*: There are problems (such as factoring) that have significantly more efficient algorithms in a QC than a CC
  - **Hence, the high motivation to have a quantum computer**
  - *What we do not know*: There exists problems that a QC can solve more efficiently than CC

Outline

1. Why quantum computing
   - New realms of computational power and information security
   - In the news
   - Large funding and research focus
2. Realizing a quantum computer
   - Quantum computing 101: A compare and contrast approach
   - Pre-requisites for the existence of a quantum computer
   - Physical realization and models of quantum computing
   - Quantum computer vs. Classical computer
3. Error correction in quantum information processing
   - Overview of important quantum gates (operations)
   - A classical error correction example
   - Quantum error correction: an overview
4. Summary

Pauli operations (I)

- $I \equiv \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$: Identity/no-operation/memory.
- $X \equiv \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$: Bit-flip.
- $Z \equiv \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$: Phase-flip.
- $Y \equiv \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, where $i = \sqrt{-1}$: Phase- and Bit-flip.
- The set of all possible Pauli operations on a single qubit is $\mathcal{P}_1 = \{I, X, Y, Z\}$, modulo-$\{\pm 1, \mp i\}$
- NOTE: $\forall G \in \mathcal{P}_k$, $G^\dagger = G$ and $G^2 = I$ (unitary), $\forall k \in \mathbb{N}$. Thus, all Pauli operations are valid quantum gates!

Pauli operations (II)

- Any valid quantum gate, U, can be expressed as a sum of Pauli gates. Simple case, take a generic $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \in \mathbb{C}^{2x2}$, then

$$U = \frac{u_{11} + u_{22}}{2} I + \frac{u_{12} + u_{21}}{2} X + \frac{i(u_{12} - u_{21})}{2} Y + \frac{u_{11} - u_{22}}{2} Z.$$

  In fact, this actually works for all matrices, but this is irrelevant to us in our current scope.

- Simple case can be seen with the Hadamard gate, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{X}{\sqrt{2}} + \frac{Z}{\sqrt{2}}$.

Clifford gates

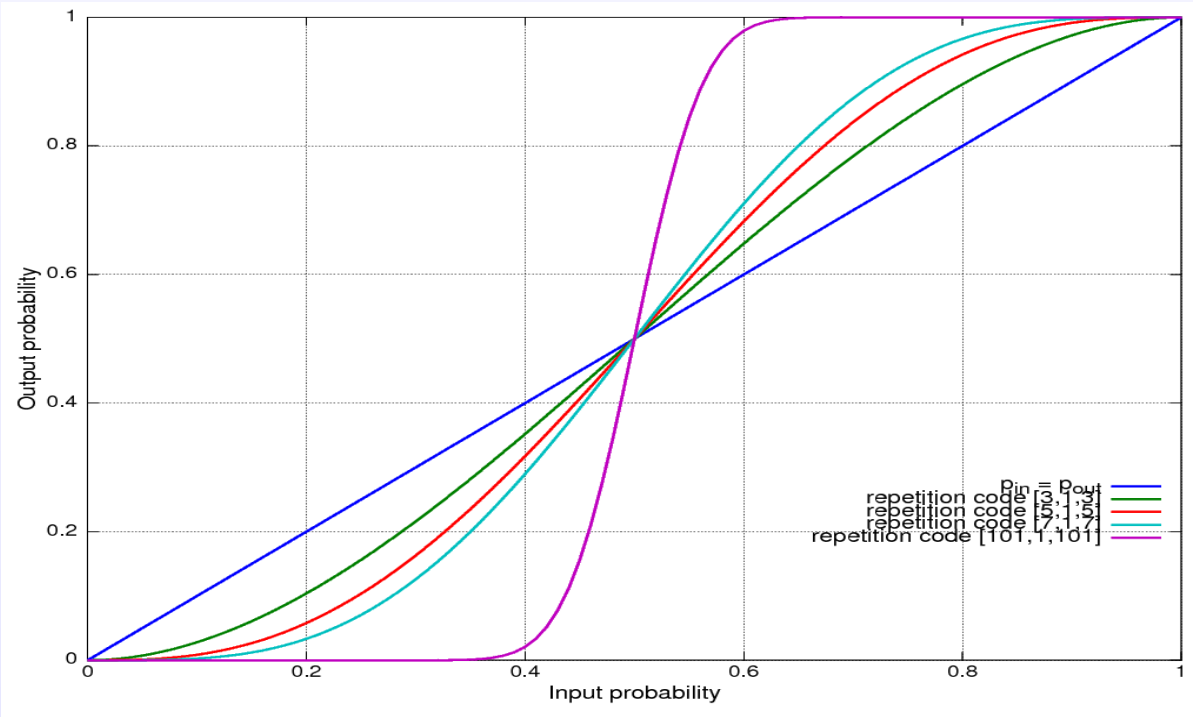
- Clifford gates.
  - *Definition:* Any quantum gate, G, that maps a Pauli operation to the same or a different Pauli operation. Essentially, any gate that satisfies the property

$$G\mathcal{P}G^{\dagger} \in \mathcal{P}.$$

  - Note that all Pauli gates are Clifford gates.
  - There are other Clifford gates. The set of all single qubit Clifford gates is the set generated by the group $\mathcal{C} = \mathcal{P} \cup \{H, S\}$.
  - Quantum circuits with only Clifford gates and Pauli errors can be simulated efficiently on a classical computer.

A classical error correction example

- Let us start with what we have good familiarity: *classical repetition code*
  - Assume a binary symmetric error channel (0 and 1 have equal probability of getting flipped)
  - Replace a logical-0 bit by $\underbrace{00\ldots0}_{\bar{0}}$ and a logical-1 bit by $\underbrace{11\ldots1}_{\bar{1}}$
  - *Majority vote at the output is the name of the game*



Quantum error correction: nomenclature

- Qubits and quantum gates are highly sensitive to different noise sources: "detaching"-nature (decoherence), temperature, control noise, and quantization error.
- *Notation*: An $[\![n, k, d]\!]$ error-correcting code is one where there are k logical bits, n physical bits used to represent them, and d is the "distance" of the code. An $[\![n, k, d]\!]$ code can fix erroneous sets of n-length bits as long as there are less than $\frac{d}{2}$ bits in error
- Re-visit error correction in classical computing
  - A $[\![3, 1, 3]\!]$ repetition code: $0 \mapsto 000$, $1 \mapsto 111$
    - We can correctly fix any single error by majority voting
    - We can also fix double errors by majority voting, but incorrectly!
  - Quantum error-correcting code: similar idea but qubits are protected against a wider spectrum of errors

Quantum error correction: The *Stabilizer* formalism (I)

- We denote the stabilizers of a code by the set S; this set does not change the state of any codeword.
- We denote the errors by the set E; this set causes the codeword to change state and anti-commutes with S.
- We denote the logical operators of the code by L; this set does a valid operation on a codeword and can result in another codeword; they do *commute* with the stabilizers, S
- An example: the quantum repetition code (only fixes bit-flip, X)
  - Codewords: $|0\rangle \mapsto |000\rangle$, $|1\rangle \mapsto |111\rangle$
  - $S = \{III, ZZI, ZIZ, IZZ\}$. Note: $III \equiv I \otimes I \otimes I$ (Kronecker/Tensor product)
  - $L = \{XXX, ZZZ, \ldots\}$
  - $E = \{XII, \ldots\}$

Quantum error correction: The *Stabilizer* formalism (II)

- Two matrices, A and B, commute if $AB = BA$ and anti-commute if $AB = -BA$
- The X and Z matrices anti-commute with each other, but obviously commute with themselves
- Suppose that a single bit-flip error (X) occurred, then it will anti-commute with at least one of the repetition code stabilizers and we can fix it
- **In general, there are infinitely many single qubit errors that do not fit bit-flip and so require more general code to fix**

Summary

- Quantum computers are now strongly believed to be highly more efficient than classical computers for certain problems.
- By their nature, error correction is inevitably needed for sensible quantum information processing.
- This area of research still has significant challenges to overcome, ranging from universal quantum computing to fault-tolerance

Questions

Thank you for being here!

Q & A

[1] D. P. DiVincenzo, "The physical implementation of quantum computation," *arXiv:0002077*

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[3] D. Gottesman, "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation," *Proceedings of Symposia in Applied Mathematics*, vol. 68, pp. 13 - 45+, 2010.

Teasers

So, you still want to know more (Teasers)

How can we still correct errors, when we cannot make a copy

- Granted, we cannot copy an arbitary qubit, we can *copy* the error on the qubit
- Unlike in classical computing where a perfect observation (measurement) gives the value of a bit with certainty, ...
- ...a perfect quantum measurement is still probabilistic; wrap your mind around this reality
- A measurement always projects the input qubit into one of its eigenbasis
- However, coupling qubits with helper or *ancilla* qubits allows us to do two things
  1. Replicate the error on our data qubit onto a set of ancilla qubits
  2. Apply projective measurements on the ancilla qubits
  3. Decode the error that most likely occurred and apply the error-mitigation method
- Thus, we have the power to do quantum error-correction without copying or observing the data directly
- *Caveat*: the data qubits must be encoded in a sufficient error-detecting or error-correcting code