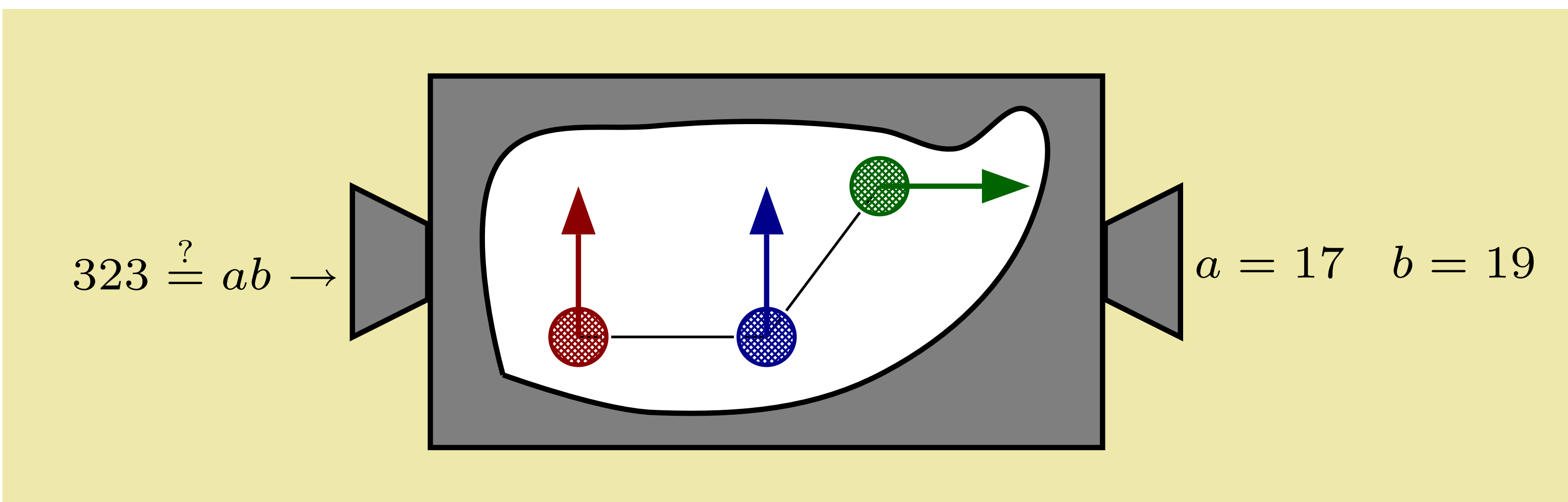
Quantum Computing with Ensembles

Strange Physics for Ordinary Tasks

David Collins

Department of Physics and Astronomy, Bucknell University, Lewisburg PA



Outline

"All information is physical."

- Classical computing and complexity.
- Quantum mechanics of qubits.
- Quantum computing: standard approaches.
- Quantum computing: ensemble approaches.

Classical mechanics governs the behavior and scope of conventional information processing devices (PCs, cell-phones, etc...).

Quantum mechanics extends information processing possibilities beyond those of conventional classical information processing devices.

Integer Multiplication

How difficult is integer multiplication?

- Two single digit integers:

$$7 \times 8 = 56.$$

- Two two digit integers:

$$\begin{array}{r} 27 \\ 18 \\ \hline 216 \\ 27 \\ \hline 486 \end{array}$$

- Two three digit integers:

$$\begin{array}{r} 727 \\ 348 \\ \hline 5816 \\ 2908 \\ 2181 \\ \hline 252996 \end{array}$$

- Two n digit integers:

Approximately n^2 single digit multiplications and additions.

Integer Factorization

How difficult is integer factorization?

- Two digit integer:

$$91 = a \times b$$
$$\Rightarrow a = 7 \quad \text{and}$$
$$b = 13$$

- Three digit integer:

$$713 = a \times b$$
$$\Rightarrow a = ? \quad \text{and}$$
$$b = ?$$

- Trial and error factorization of n digit integer N. Number of guesses:

$\sqrt{N} \simeq \sqrt{10^n} = 10^{n/2}$ **Exponential in n.**

Best known integer factorization is exponential:
$$O((\exp(n^{1/3}(\log n)))^{2/3})$$

Computational Complexity

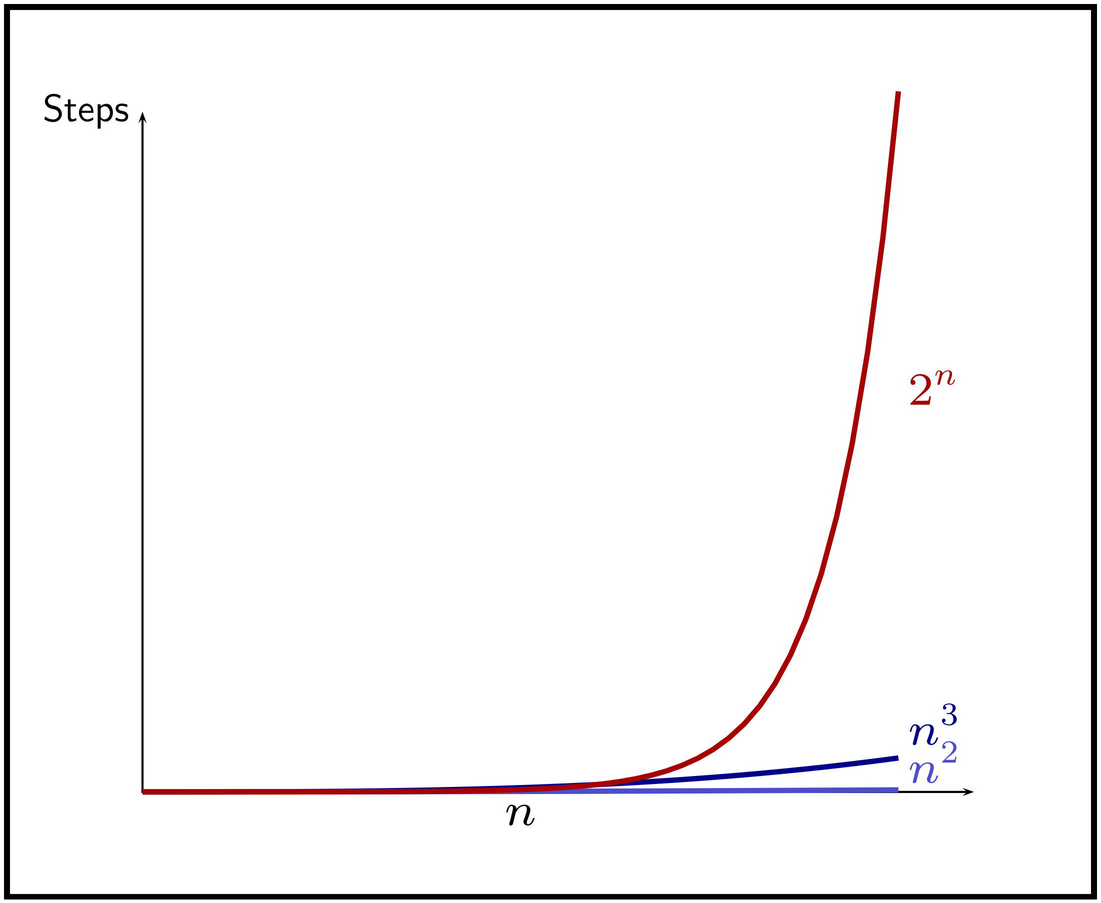
- How many additional digits to double the number of steps?
- Quadratic, $O(n^2)$:

$$n_{\text{new}} \simeq \sqrt{2}\, n_{\text{old}}$$

- Exponential, e.g. $O(2^n)$

$$n_{\text{new}} \simeq n_{\text{old}} + 1$$

Polynomial ⇜⇝ easy.
Exponential ⇜⇝ hard.



Classical Information Representation

Abstraction

- Binary digit (bit):

> State is **one of** 0 or 1.

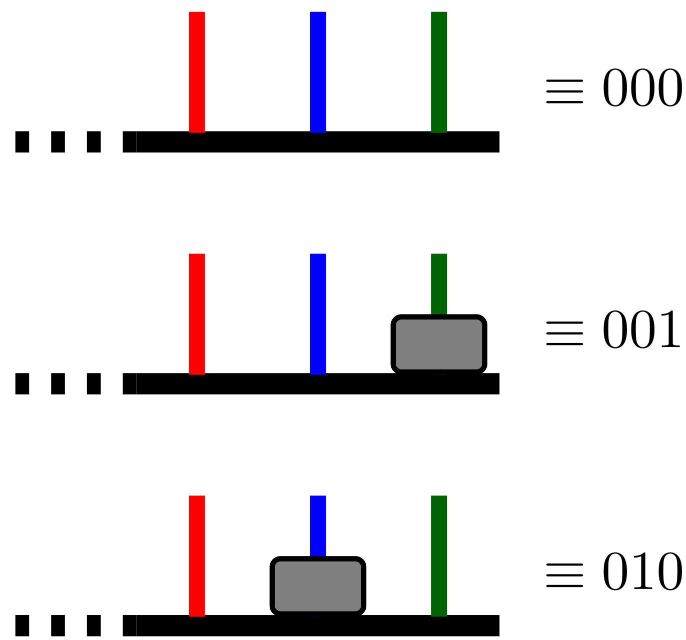
- Binary representation:

$$0 \equiv 000 \quad 1 \equiv 001 \quad 2 \equiv 010 \ldots$$

$$\text{PA} \equiv \underbrace{1001111}_{\text{P}}\ \underbrace{1000001}_{\text{A}}$$

Realization

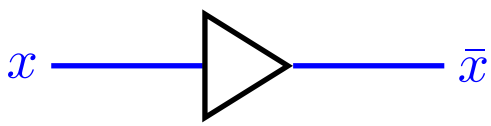
- Pegs and beads



Classical Information Processing - Basic Gates

Abstraction

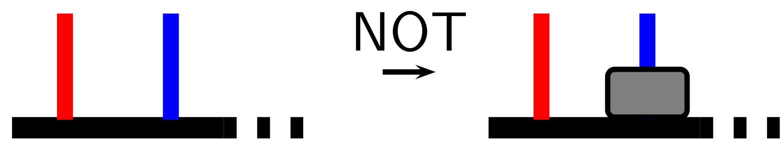
- **Example:** NOT gate:



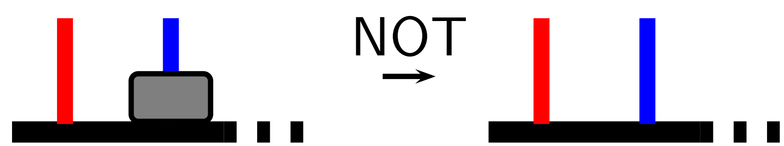
x	$\bar{x}$
0	1
1	0

Realization

- **Example:** NOT via pegs and beads:
- Implementation rules:
  - Add bead to blue peg.
  - Two beads on one peg $\longrightarrow$ remove both.
- NOT 0 on blue bit



- NOT 1 on blue bit

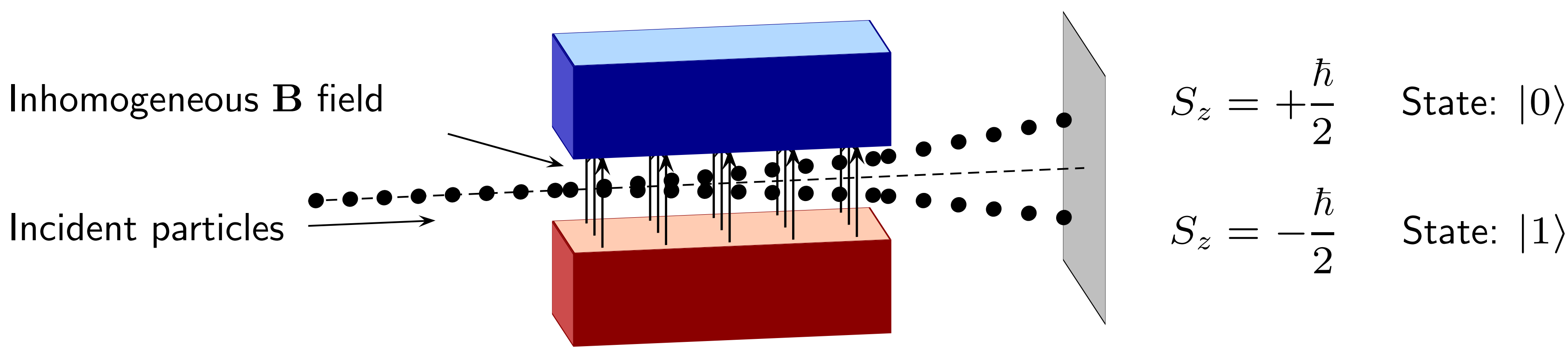


Number of basic algebraic operations $\sim$ number of basic gates.

Spin $\frac{1}{2}$ Quantum Systems

Spin = intrinsic **angular momentum** of subatomic and atomic scale particles.

- **Stern-Gerlach** measures component of angular momentum.

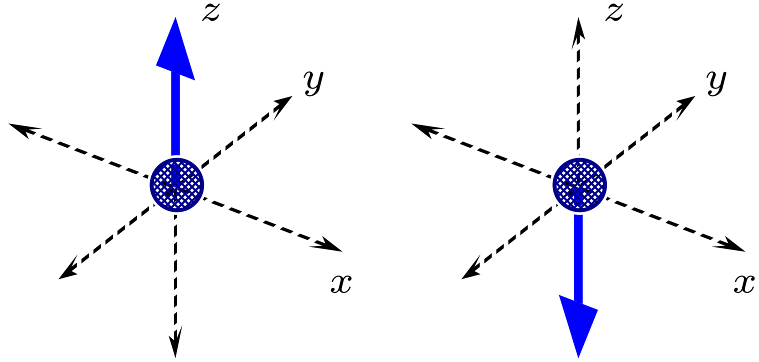


- **Example:** electron, proton, H, ^{13}C.

Quantum States and Information

Information is stored as a state of a spin $\frac{1}{2}$ quantum system **(qubit).**

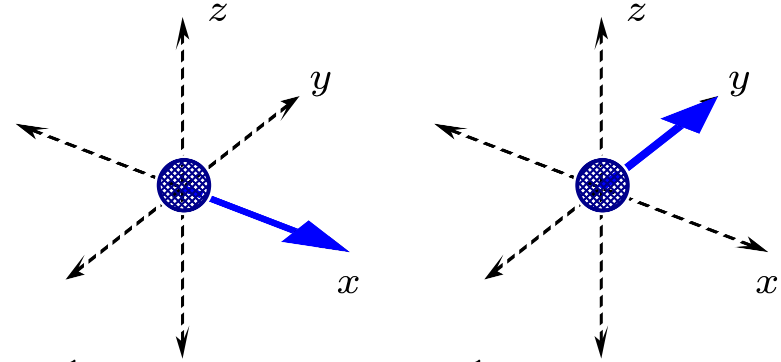
Energy Eigenstates



$|0\rangle$ $\quad$ $|1\rangle$

Classical bit state.

Superposition states



$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad$ $\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$

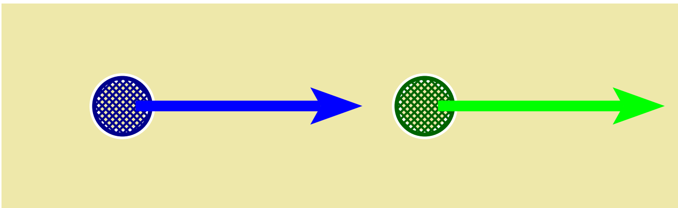
Beyond classical bit states!

General state: $|\boldsymbol{\psi}\rangle = \boldsymbol{\alpha}\,|\mathbf{0}\rangle + \boldsymbol{\beta}\,|\mathbf{1}\rangle \sim \begin{pmatrix} \boldsymbol{\alpha} \\ \boldsymbol{\beta} \end{pmatrix}$ where $|\alpha|^2 + |\beta|^2 = 1.$

Multiple Qubits

Unentangled States

- Products of single qubit states:

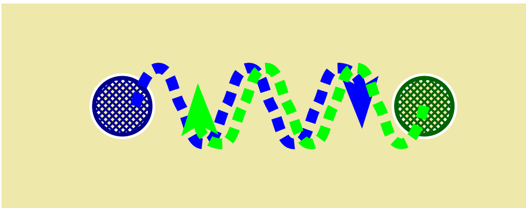


$$\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$$
$$= \frac{1}{2}\Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\Big)$$

- **Uncorrelated** states.

Entangled States

- Not product of single qubit states:



$$\alpha_0|0\rangle|0\rangle + \alpha_1|0\rangle|1\rangle + \alpha_2|1\rangle|0\rangle + \alpha_3|1\rangle|1\rangle$$
$$\neq |\Psi_1\rangle \otimes |\Psi_2\rangle$$

Multiple qubits give highly **correlated states.**

Quantum Measurements and Information Extraction

Information is extracted via **quantum measurements**.

- Measurements of z component of single qubit spin are not deterministic:

$$\alpha |0\rangle + \beta |1\rangle \rightsquigarrow \begin{cases} S_z = +\hbar/2 \text{ with probability } |\alpha|^2 \\ S_z = -\hbar/2 \text{ with probability } |\beta|^2 \end{cases}$$

- Assign bit values by measuring z component of spin:

S_z	Bit value
$+\hbar/2$	0
$-\hbar/2$	1

Quantum Dynamics and Information Processing

Information is processed via **controlled time evolution**.

- Unitary transformation **(quantum "gate"):**

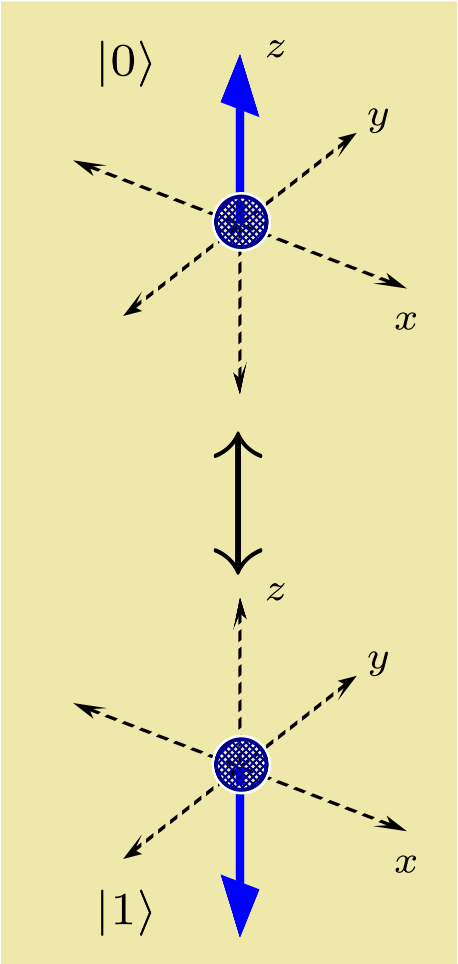
$$|\psi_{\text{final}}\rangle = \hat{U}\ |\psi_{\text{initial}}\rangle \quad \text{where} \quad \hat{U}^\dagger \hat{U} = \hat{I}.$$

- **Example:** Single qubit quantum NOT gate

$$\hat{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

transforms

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$



Quantum Gates

Reduction to **basic one and two qubit operations.**

Abstraction

- **Example:** Single bit rotation

$$|\psi\rangle \;—\; \boxed{\hat{R}_y(\theta)} \;—\; \hat{R}_y(\theta)\,|\psi\rangle$$

$$\hat{R}_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

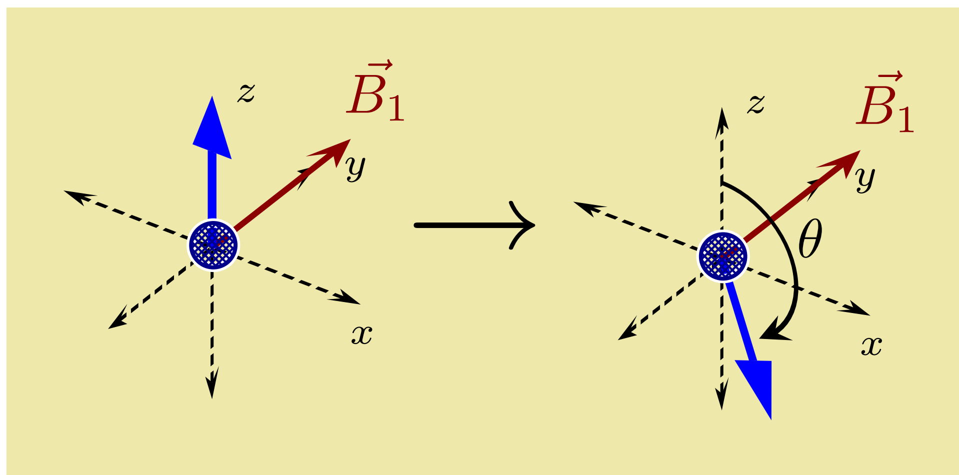
- Creates superpositions:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}$$

Realization

- **Example:** $\hat{R}_y(\theta)$ for spin $\frac{1}{2}$:

Apply magnetic field $\vec{B}_1$ along $\hat{y}$ axis.



Classical Computing with Qubits

Classical Bit States

- Restrict to:

$$0 \equiv |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$1 \equiv |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Classical Gates

- Matrix representation:

$$\text{NOT} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- **Example:** NOT on 0:

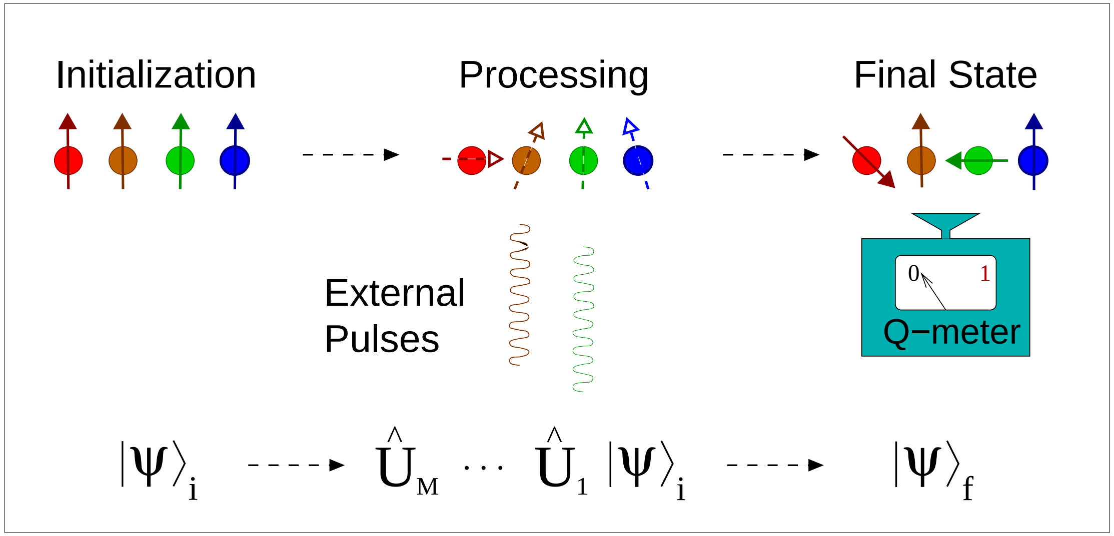
$$\text{NOT } 0 \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv 1$$

Any classical computation can be implemented using qubits.
Quantum computing allows greater possibilities via
superpositions of states.

Quantum Computing Scheme

- Uses distinguishable qubits.



- Evolution steps:
  - generate superpositions and entangled states,
  - sequence of basic one and two qubit gates.

Quantum algorithms provide speedups **(fewer basic gates)**.

Quantum Algorithms

- **"Toy" algorithms:**
  - Global properties of functions.
  - Exponential speedup.
  - Deutsch-Jozsa algorithm.
  - Bernstein-Vazirani algorithm.
  - Simon's algorithm.

- **Searching (Grover):**
  - Search unstructured database.
  - Quadratic speedup.

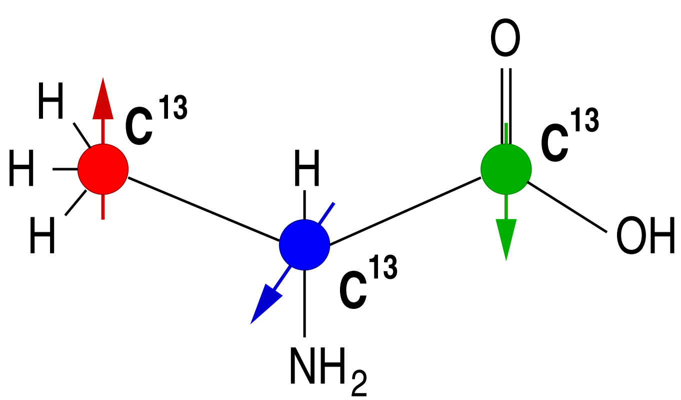
- **Integer factorization (Shor):**
  - Factorize integer $N = pq$.
  - Problem size $L := \log_2 N$.
  - Classical: $O(exp(L^{1/3}(\log L)))^{2/3}$.
  - Quantum: $O(L^3)$.

Decimal digits	Classical	Quantum
100	$\sim 10^{13}$	$\sim 10^{7}$
200	$\sim 10^{17}$	$\sim 10^{9}$
300	$\sim 10^{20}$	$\sim 10^{10}$
400	$\sim 10^{23}$	$\sim 10^{10}$

  - Age of universe $\sim 10^{17}$s.
  - Can break RSA code.

Nuclear Magnetic Resonance: Nuclear Spin Spectroscopy

- Spin $\frac{1}{2}$ nuclei in strong magnetic field, $\vec{B}_0$.
- Manipulation via external magnetic fields.
- Precession detected via readout coils.
- **Example:** H and ^{13}C nuclei of alanine.



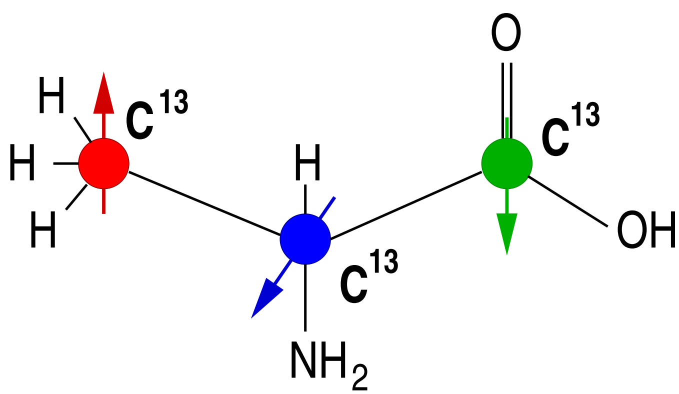
Source: Stoltz Group, Dept. of Chemistry, Caltech.

NMR Quantum Computing

NMR: an accessible technology for small scale quantum computers.

Qubits

- Nuclear spins provide qubits.
- **Example:** Alanine ^{13}C $\longrightarrow$ 3 qubits



- Single qubit gates: external magnetic fields.
- Two qubit gates: spin-spin coupling.

Issues

- Readily available technology.
- Weak interactions with environment $\Rightarrow$ slow information degradation.
- Algorithm implementation:
  - Shor factorization - 7 qubits.

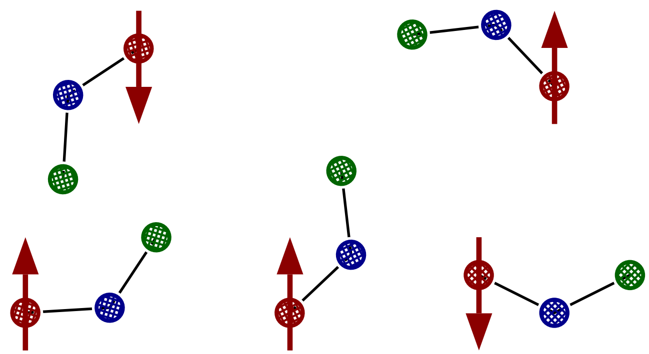
    Vandersypen et.al, Nature 414, 883-7 (20 Dec. 2001).
  - Grover search - 3 qubits.

    Vandersypen et.al, App. Phys. Lett. 76, 646-8 (2000).
- Ensemble of computers: **initialization and readout?**

Ensemble Quantum Computing

Ensemble of Identical Computers

- NMR sample $\approx 10^{20}$ identical molecules.



- Rapid molecular motion $\Rightarrow$ no intermolecular interactions.
- **Identical, independent computer ensemble.**

Statistically Mixed States

- Thermal equilibrium:

$$|0\rangle \text{ with prob } \approxeq \frac{1}{2}\left(1 + \frac{\hbar\omega}{2k_B T}\right)$$

$$|1\rangle \text{ with prob } \approxeq \frac{1}{2}\left(1 - \frac{\hbar\omega}{2k_B T}\right)$$

$\omega =$ precession frequency about $\vec{B}_0$.

- Weak polarization:

$$\hbar\omega/2k_B T \approx 10^{-4}$$

Mixed state input $\Rightarrow$ alternative initialization.
Ensemble average output $\Rightarrow$ alternative readout.

Ensembles: Initialization and Readout

Initialization

- Non-unitary scheme $\longrightarrow$ pseudo-pure state.

Thermal equilibrium state

$\downarrow$

Completely random $+$ pure state

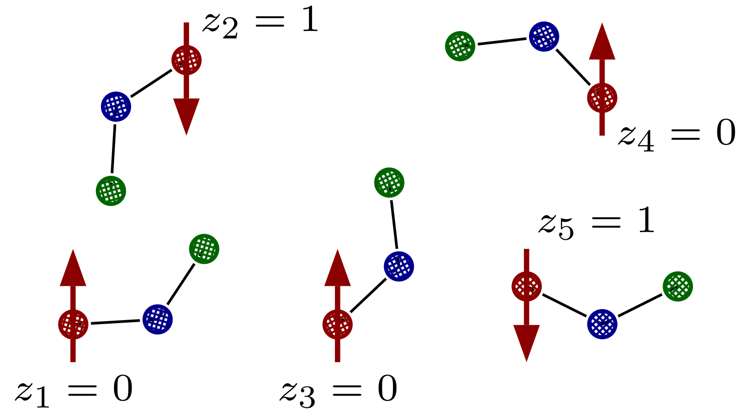
$$\rho_{\mathrm{i}} = \frac{1-\varepsilon}{2^n}\hat{I}^{\otimes n} + \boldsymbol{\varepsilon} \left|\boldsymbol{\psi}_{\mathrm{i}}\right\rangle \left\langle\boldsymbol{\psi}_{\mathrm{i}}\right|$$

- Effectively provides correct initial state $|\psi_{\mathrm{i}}\rangle$ required for algorithm.
- **Polarization $\boldsymbol{\varepsilon}$** $\sim$ fraction of molecules in correct initial state typically weak:

$$\varepsilon \sim 10^{-4}$$

Readout

- M ensemble members $\longrightarrow$ sample average



$$\overline{z} = \sum z_i / M$$

- Majority vote decisions: $\overline{z} \overset{?}{>} 1/2$.

Non-deterministic output.

Modified Algorithms for Ensemble QC

Readout

- Converted "deterministic" algorithms
  - Grover search (one marked item) - unnecessary.
  - Grover search (few marked items) - few runs plus filtering.
  - Shor factorization - duplication of quantum computers.
- Modified algorithms require fewer steps:

Grover search can be truncated.

D. Collins, Phys. Rev. A 65, 052321 (2002).

Initialization

- Use noisy thermal equilibrium input states?
- **Bernstein-Vazirani algorithm:**
  - Standard thermal equilibrium state plus unmodified algorithm plus expectation values appears satisfactory.
- **Deutsch-Jozsa algorithm:**
  - Existing "one pure qubit plus maximally mixed state" approach unsatisfactory.

  Arvind, D. Collins, Phys. Rev. A 68, 052301 (2003).
- **Grover, Shor:** - ?

Single Bit Output: Statistics

Framework

- Standard algorithm $\longrightarrow$ **deterministic output on single qubit.**
- Ensemble with polarization ε, individual computer:

$$\Pr(\text{correct}) = \frac{1+\varepsilon}{2}$$

$$\Pr(\text{incorrect}) = \frac{1-\varepsilon}{2}$$

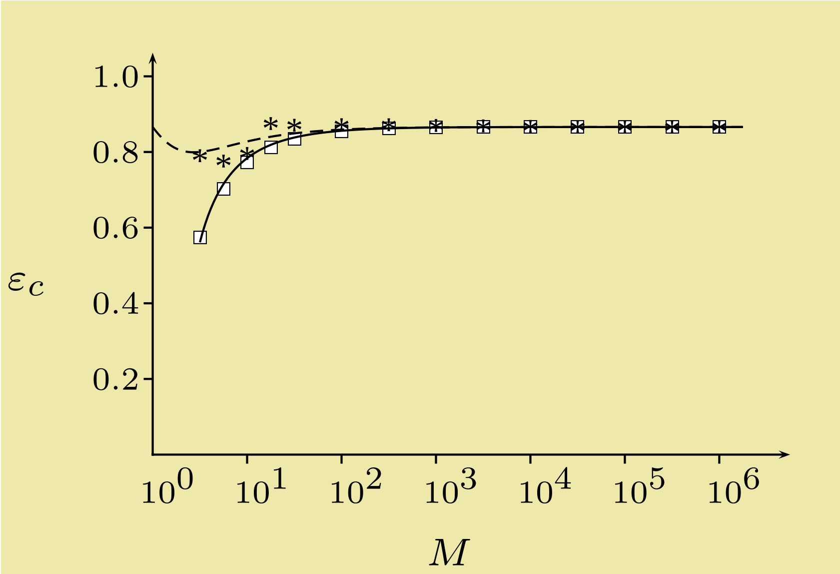
When does quantum ensemble failure probability exceed classical failure probability?

Classical vs Quantum Ensemble

- For given ensemble size, M:

Polarization required for quantum to outperform classical probabilistic using comparable resources?

- Deutsch-Jozsa



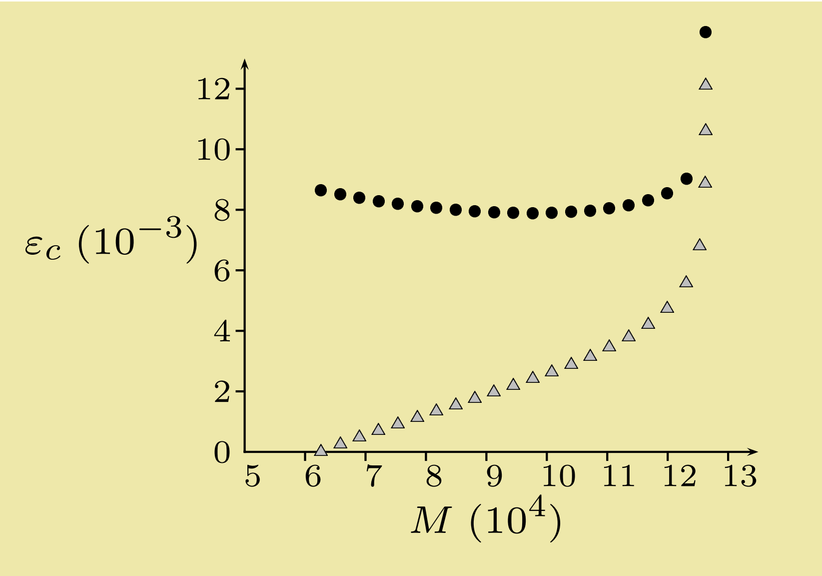
B. Anderson, D. Collins, Phys. Rev. A 72, 042337 (2005).

Grover Search Algorithm: Statistics

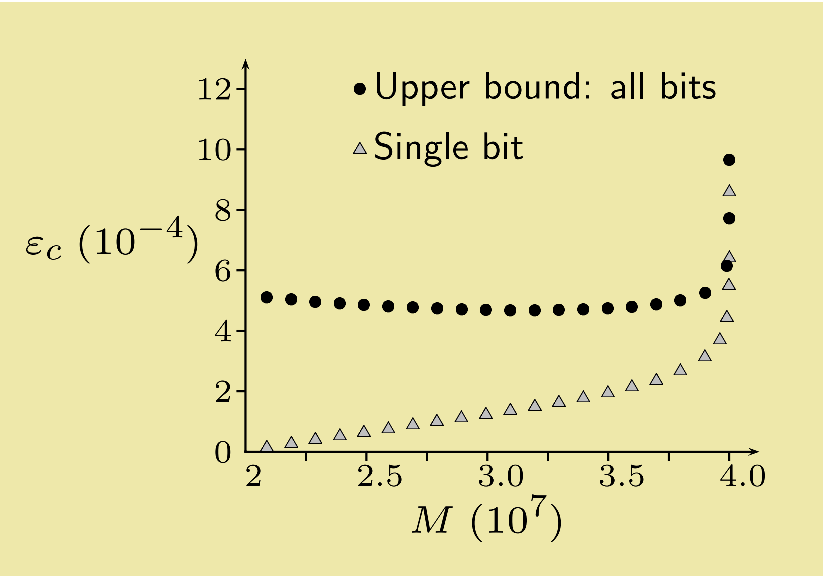
- Search database of size $N = 2^n$ for single marked item.
- Nearly **deterministic output on n qubits.**
- Correlated measurement outcomes:

> Polarization required for Grover search to outperform classical probabilistic search on all n bits?

Critical Polarization: $N = 10^{10}$

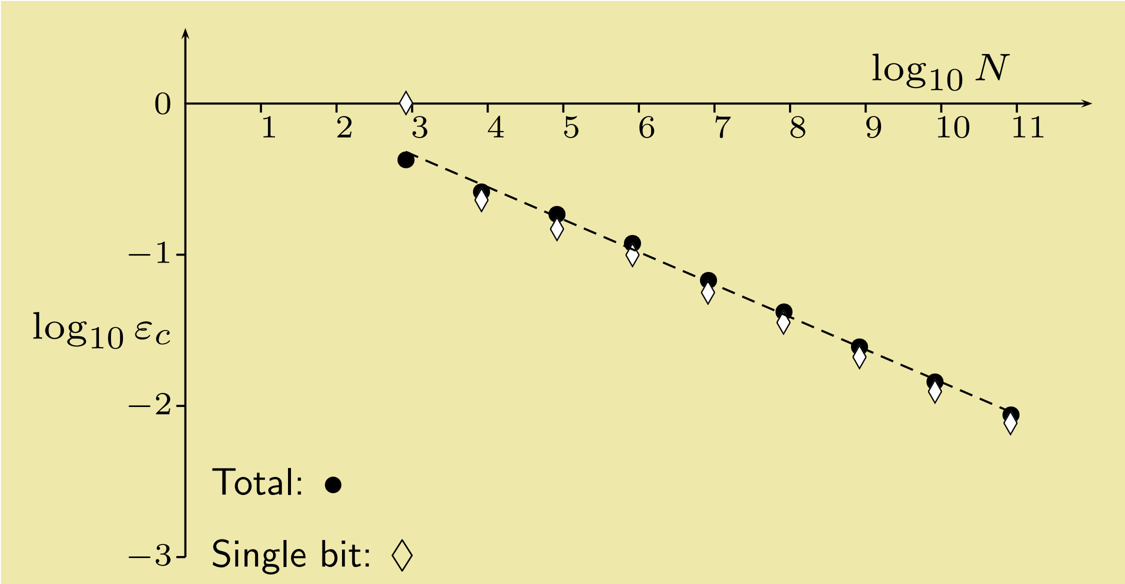


Critical Polarization: $N = 10^{15}$



Grover Search: Critical Polarization Lower Bound

- Compute ε_c for largest M before classical algorithm succeeds with certainty.
- Numerical evaluation:



- Best fit:

$$\varepsilon_c = \frac{2.1}{N^{0.215}}$$

Quantum Information Arena

Theory

- Quantum Cryptography
- Quantum Teleportation
- Superdense Coding
- Decoherence and Error Correction
- Entanglement
- Quantum Channels

Practice

- NMR
- Photons
- Trapped Ions
- Quantum Dots
- Doped Silicon
- Superconducting Circuits

Undergraduate Involvement

Mathematical/Computer Background

- Linear algebra.
- "Physicist's" probability theory.
- Interest in numerical calculations.

Physics Background

- Quantum mechanics: wavefunctions (less useful).
- Quantum mechanics: fundamental level (more useful).

Projects

- Ensemble quantum computing: statistics.
- Ensemble quantum computing: algorithms.
- Distinguishing unitaries.
- General measurements.
- Pulse design.

Project Nature

- Theory/mathematical.
- Some numerical calculations.
- Some analytical calculations.

Future Directions

Ensemble QC

- Can other standard quantum algorithms and applications be tailored for ensemble QC?
- What resources does ensemble QC require to outperform classical probabilistic computing?
- Where does ensemble QC lie in relation to standard QC and classical computation?

General

- Quantum mechanics provides new information processing paradigm.
- Quantum systems incorporate information processing possibilities distinct from classical systems. Why? What does this tell us about quantum mechanics?

Deutsch-Jozsa Algorithm

Deutsch problem concerns properties of simple binary functions.

Single Bit Binary Functions

- Maps

$$\{0,1\} \xrightarrow{f} \{0,1\}$$

$$x \mapsto f(x) = ax \oplus b$$

where $a, b \in \{0,1\}$.

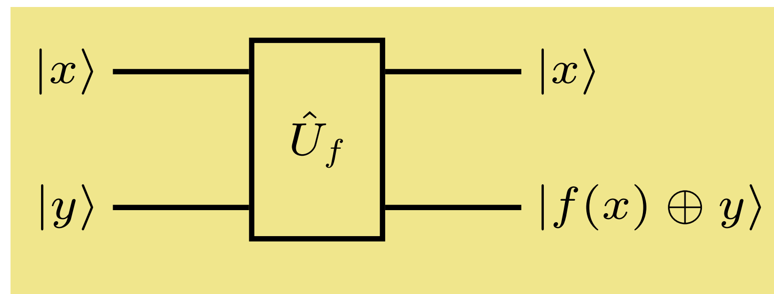
- Addition modulo 2:

$$0 \oplus 0 := 0 \qquad 0 \oplus 1 := 1$$
$$1 \oplus 0 := 1 \qquad 1 \oplus 1 := 0$$

- Task: **Find a.**

Function Evaluation

- Use unitary function evaluation:



for $x, y \in \{0,1\}$.

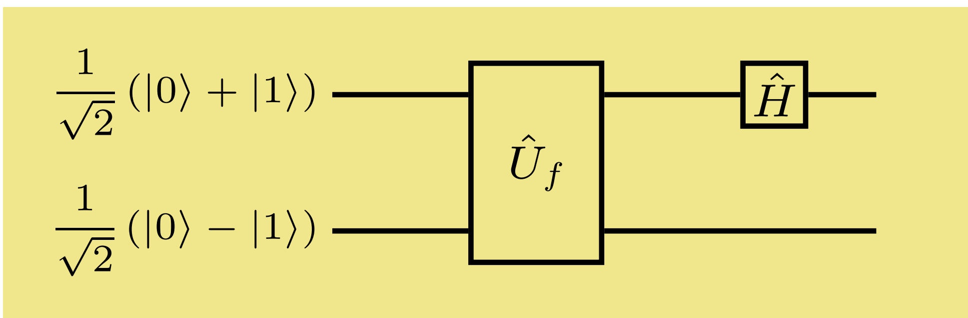
- **"Classical"** approach requires **two function evaluations**:

$$\begin{aligned} |0\rangle\,|0\rangle &\quad\longrightarrow\quad |0\rangle\,|b\rangle \\ |1\rangle\,|0\rangle &\quad\longrightarrow\quad |1\rangle\,|a \oplus b\rangle \end{aligned}$$

Deutsch-Jozsa Algorithm

Quantum superposition helps to solve the Deutsch problem with **just one function evaluation!**

- Use **quantum superpositions.**



$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Upper qubit state **before Hadamard:**

If a = 0 : $\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

If a = 1 : $\frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

- Upper qubit state **after Hadamard:**

If a = 0 : $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$

If a = 1 : $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$

Spin z measurement yields a.