Quantum Computing with Ensembles

David Collins

Department of Physics, Bucknell University, Lewisburg PA

dcollins@bucknell.edu

http://www.eg.bucknell.edu/ dcollins/index.html
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 accessible to conventional classical information processing devices.
How difficult is integer multiplication?

- Two single digit integers:
  \[ 7 \times 8 = 56. \]

- Two two digit integers:
  \[
  \begin{array}{c}
  27 \\
  18 \\
  \hline
  216 \\
  \end{array}
  \quad \quad \quad
  \begin{array}{c}
  727 \\
  348 \\
  \hline
  5816 \\
  \end{array}
  \begin{array}{c}
  2908 \\
  2181 \\
  \hline
  252996 \\
  \end{array}
  \]

- Two three digit integers:

- Two \( n \) digit integers:

  Approximately \( n^2 \) single digit multiplications and additions.
**Polynomial Complexity**

- Number of basic operations as function of input size $n$.
- Assess behavior for large $n$.
- Linear, $O(n)$:
  \[ \text{Operations} = \alpha n + \ldots \]
- Quadratic, $O(n^2)$:
  \[ \text{Operations} = \alpha n^2 + \ldots \]
- Polynomial, $O(n^k)$:
  \[ \text{Operations} = \alpha n^k + \ldots \]
Integer Factorization

How difficult is integer factorization?

- Two digit integer:
  
  \[ 91 = a \times b \]
  
  \[ \Rightarrow a = 7 \quad \text{and} \quad b = 13 \]

- Three digit integer:
  
  \[ 713 = a \times b \]
  
  \[ \Rightarrow a = ? \quad \text{and} \quad b = ? \]

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

  \[ \sqrt{N} \approx \sqrt{10^n} = 10^{n/2} \quad \text{Exponential in} \ n. \]

Best known integer factorization is exponential:

\[ O\left((\exp(n^{1/3}(\log n)))^{2/3}\right) \]
Computational Complexity

- How many additional digits to double the number of steps?
- Quadratic, $O(n^2))$:
  \[ n_{\text{new}} \approx \sqrt{2} n_{\text{old}} \]
- Exponential, e.g. $O(2^n)$:
  \[ n_{\text{new}} \approx n_{\text{old}} + 1 \]

Polynomial ↔ easy.
Exponential ↔ hard.
Classical Information Representation

**Abstraction**

- Binary digit (bit):
  
  State is **one of** 0 or 1.

- Binary representation:

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

  
  $PA \equiv \begin{array} \{ \text{1001111} \end{array}$

**Realization**

- Pegs and beads

  
  $\equiv 000$

  
  $\equiv 001$

  
  $\equiv 010$
Classical Information Processing - Basic Gates

Abstraction

Example: XOR on two bits

\[
\begin{array}{c|c|c}
 a & b & a \oplus b \\
0 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\]

Realization

Example: XOR via pegs and beads

Implementation rules:
- Red and blue peg beads → green peg.
- Two beads on one peg → remove both.

1 XOR 0

1 XOR 1

Classical information is usually viewed in the abstract.
Reversible Computing

Reversible versions of basic gates exist.

- **Example:** Standard XOR:
  
  Find $a, b$ if $a \oplus b = 0$

- **Reversible XOR:**

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$a \oplus b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Vector representation for bit states:**

  
  $00 \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
  $01 \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$
  $10 \equiv \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$
  $11 \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

- **Matrix representation for gates:**

  
  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Quantum computing allows **superpositions of bit states.**
Spin $\frac{1}{2}$ Quantum Systems

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

**Stern-Gerlach** measures angular momentum via magnetic dipole moment.

- Inhomogeneous $B$ field
- Incident particles

\[ S_z = +\frac{\hbar}{2} \quad \text{State: } |0\rangle \]
\[ S_z = -\frac{\hbar}{2} \quad \text{State: } |1\rangle \]

- Examples: electron, proton, H, $^{13}\text{C}$. 

9
Quantum States and Information

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

**Energy Eigenstates**

State: $|0\rangle$

State: $|1\rangle$

**Superposition states**

State: $\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$

State: $\frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle)$

**Classical bit state.**

**Beyond classical bit states!**

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

Multiple qubit states represented via tensor products.

- Two-qubit unentangled state (e.g. two spins along the $x$ axis):

\[
(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle
\]

where

\[|ab\rangle \equiv |a\rangle |b\rangle := |a\rangle \otimes |b\rangle.\]

- Quantum mechanics allows any (often entangled) superposition:

\[
|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \sim \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}
\]

where

\[|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1.\]
Quantum Measurements and Information Extraction

Information is extracted via quantum measurements.

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

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

- Measurement induces “collapse” of state:

<table>
<thead>
<tr>
<th>$S_z$</th>
<th>Bit value</th>
<th>State collapse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+\hbar/2$</td>
<td>0</td>
<td>$\alpha</td>
</tr>
<tr>
<td>$-\hbar/2$</td>
<td>1</td>
<td>$\alpha</td>
</tr>
</tbody>
</table>
Quantum Dynamics and Information Processing

Information is processed via **unitary transformations** ("gates").

- **Linear time evolution**

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

- **Example:** Single qubit quantum NOT

  \[ \hat{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ transforms } \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \]

  and generalizes classical NOT

  \[ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \]
Quantum Gates

Reduction to one and two qubit unitary operations.

Single qubit rotations

- **Example:** Single bit rotation

\[
|\psi\rangle \xrightarrow{R_y(\theta)} R_y(\theta)|\psi\rangle
\]

\[
R_y(\theta) = \begin{pmatrix}
\cos(\theta/2) & -\sin(\theta/2) \\
\sin(\theta/2) & \cos(\theta/2)
\end{pmatrix}
\]

- On “classical” \(|0\rangle\) (for \(\theta = \pi/2\)):

\[
\begin{pmatrix}1 \\ 0\end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix}1 \\ 1\end{pmatrix} \begin{pmatrix}1 \\ 1\end{pmatrix}
\]

\[
= \frac{1}{\sqrt{2}} \begin{pmatrix}1 \\ 1\end{pmatrix}
\]

Two-qubit gates

- **Example:** Controlled-NOT

\[
\hat{U}_{\text{CN}} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

on \(\begin{pmatrix}\alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3\end{pmatrix}\)
Dynamics: Gate Construction

Gate construction via evolution under the system Hamiltonian.

- **Schrödinger equation:**
\[
    i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle
\]
gives **unitary evolution**
\[
    |\psi(t)\rangle = \hat{U}(t, t_0) |\psi(t_0)\rangle
\]

- For time independent \(\hat{H}\):
\[
    \hat{U}(t, t_0) = e^{-i\hat{H}(t-t_0)/\hbar}.
\]

- **Example:** Magnetic field along \(\hat{y}\):
\[
    \hat{H} = \hbar \gamma B_1 \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}
\]
applied for \(t - t_0 = \frac{\theta}{2B_1\gamma}\)
Quantum Computing Scheme

- Uses distinguishable qubits.

\[ |\psi_i\rangle \rightarrow \hat{U}_M \cdots \hat{U}_1 |\psi_i\rangle \rightarrow |\psi_f\rangle \]

- Artful construction of evolution steps uses:
  - superpositions,
  - entangled states.

Quantum algorithms provide speedups (fewer computational steps).
Quantum Algorithms

▶ “Toy” algorithms:
  - Global properties of binary functions.
  - Exponential speedup.
  - Deutsch-Jozsa, Bernstein-Vazirani and Simon’s algorithms.

▶ Searching (Grover):
  - Search unstructured database.
  - Quadratic speedup in terms of oracle queries.

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

<table>
<thead>
<tr>
<th>Decimal digits</th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>$\sim 10^{13}$</td>
<td>$\sim 10^7$</td>
</tr>
<tr>
<td>200</td>
<td>$\sim 10^{17}$</td>
<td>$\sim 10^9$</td>
</tr>
<tr>
<td>300</td>
<td>$\sim 10^{20}$</td>
<td>$\sim 10^{10}$</td>
</tr>
<tr>
<td>400</td>
<td>$\sim 10^{23}$</td>
<td>$\sim 10^{10}$</td>
</tr>
</tbody>
</table>

- Age of universe $\sim 10^{17}$s.
- Can break RSA code.
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:**
  \[
  0 \oplus 0 := 0 \quad 0 \oplus 1 := 1 \\
  1 \oplus 0 := 1 \quad 1 \oplus 1 := 0
  \]

- **Task:** Find \(a\).

**Function Evaluation**

- **Use unitary function evaluation:**
  \[
  |x\rangle \xrightarrow{\hat{U}_f} |x\rangle \\
  |y\rangle \xrightarrow{\hat{U}_f} |f(x) \oplus y\rangle
  \]
  for \(x, y \in \{0, 1\}\).

- **“Classical” approach requires two function evaluations:**
  \[
  |0\rangle |0\rangle \rightarrow |0\rangle |b\rangle \\
  |1\rangle |0\rangle \rightarrow |1\rangle |a \oplus b\rangle
  \]
Deutsch-Jozsa Algorithm

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

- **Use quantum superpositions.**

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

\[
\hat{U}_f \quad \hat{H}
\]

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

- **Upper qubit state before Hadamard:**

  If \( a = 0 \):

  \[
  \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}
  \]

  If \( a = 1 \):

  \[
  \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}
  \]

- **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 \( a \).
**Nuclear Magnetic Resonance**

**Nuclear Spin Spectroscopy**

- Spin $\frac{1}{2}$ nuclei in strong magnetic field, $\vec{B}_0$.
- Selective manipulation by tuning frequencies of external 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**

- Distinct nuclear spins provide qubits.
- **Example:** The $^{13}$C nuclei of alanine give three qubits.

**Issues**

- Readily available technology.
- Weak interactions with environment ⇒ many gates before information is degraded.
- Algorithm implementation:
  - Shor factorization - 7 qubits.
  - Grover search - 3 qubits.
- **Ensemble initialization and readout.**

- Single qubit gates: spin selective external magnetic fields.
- Two qubit gates: evolution under spin-spin coupling.
Ensemble Quantum Computing

Ensemble of Identical Computers
- NMR sample with $\approx 10^{20}$ identical molecules.
- Rapid molecular motion $\Rightarrow$ no intermolecular interactions.

Statistically Mixed States
- Quantum state varies through ensemble, e.g. thermal equilibrium:
  - $|0\rangle$ with prob $\approx \frac{1}{2} \left( 1 + \frac{\hbar \omega}{2k_B T} \right)$
  - $|1\rangle$ with prob $\approx \frac{1}{2} \left( 1 - \frac{\hbar \omega}{2k_B T} \right)$

$\omega = \text{precession frequency about } \vec{B}_0$.
- 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 prepares pseudo-pure state.

  Thermal eq. state
  \[ \downarrow \]
  Completely random + pure state

- Poor scaling common:

  \[ \text{Signal strength } \sim n/2^n \]

  where \( n \) = number of qubits.

**Readout**

- Sample averages over ensemble with \( M \) members.

  \[ z_1 = 0, \quad z_2 = 1, \quad z_3 = 0, \quad z_4 = 0, \quad z_5 = 1 \]

  \[ z = \sum z_i/M \]

- Majority vote decisions: \( z > 1/2 \).

- 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.

Initialization

- Use noisy thermal equilibrium input states?

  - Bernstein-Vazirani algorithm:
    - Standard thermal equilibrium state plus unmodified algorithm plus expectation values satisfactory.

  - Deutsch-Jozsa algorithm:
    - Existing “one pure qubit plus maximally mixed state” approach unsatisfactory.


  - Grover, Shor: - ?

Single Bit Output: Statistics

**Framework**

- Pure state quantum algorithm:

  $$|\psi_i\rangle \rightarrow |\phi_z\rangle |z\rangle$$

  where $z = 0, 1 \sim$ algorithm output.

- Mixed state algorithm initial state:

  $$\rho_i = \frac{1 - \varepsilon}{2^n} \mathbb{1}^\otimes n + \varepsilon |\psi_i\rangle \langle \psi_i|$$

- Polarization $\varepsilon \sim$ fraction of molecules in pure state gives:

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

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

**Classical vs Quantum Ensemble**

- For given ensemble size, $M$:

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

- Deutsch-Jozsa

  ![](image)

# 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
Future Directions

Ensemble QC

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

General

- Quantum mechanics provides a new information processing paradigm.
- Information is stored and manipulated in ways fundamentally different from those for classical information processing.
- The laws of physics dictate information processing possibilities and limitations.