Quantum Computing - Next-Generation Computers

Dr. Steven R Skinner
Dr. Preethika Kumar

The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age. Paul Davies, Professor Natural Philosophy – Australian Centre for Astrobiology
Computer technology is making devices smaller and smaller. Reaching a point where classical physics is no longer a suitable model.
The orbits available to a single outermost electron in each atom can be used to represent the two bit values, logic 0 and 1.

Given quantum nature of electrons: **Qubits**
Electrons have a property that allows them to be in the two orbits (logic values) simultaneously: **Quantum Superposition**.

Allows many computations to be performed simultaneously: **Quantum Parallelism**.
Quantum Logic States

- Quantum two level system
  - $|0\rangle$ and $|1\rangle$ are states
- General state is a superposition
  - $\psi = \alpha |0\rangle + \beta |1\rangle$
- Result of measurement:
  - $|0\rangle$ with probability $|\alpha|^2$
  - $|1\rangle$ with probability $|\beta|^2$

$$|\alpha|^2 + |\beta|^2 = 1$$
Classical and Quantum Gates

**XOR (Controlled-Not)**

\[ A \quad B \quad Z \]

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>Z</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>

**Controlled-Not (CNOT)**

\[ A \quad B \quad A' \quad B' \]

Controlled-Not (CNOT) gate:

- **Controlled** (A) affects **Target** (B) only if **Control** (A) is 1.
- **Target** (B) remains unchanged if **Control** (A) is 0.

<table>
<thead>
<tr>
<th>AB</th>
<th>A'B'</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
</tr>
</tbody>
</table>

Classical and Quantum states:

- Classical state:
  - 00, 01, 10, 11
- Quantum states:
  - |00⟩, |01⟩, |10⟩, |11⟩
Quantum Computing Research

- Quantum Devices (EE and Physics)
- Quantum Circuits (EE and CE)
  - CNOT and Toffoli Gate Designs
  - Universal Gate Design
  - Shift Register (quantum wire) Design
- Quantum Architectures (CE and EE)
  - Linear (1-D) Nearest Neighbor Designs
  - 2-D NN Computing Designs
- Quantum Algorithms (CS)
Quantum algorithms are being developed that use quantum parallelism, interference, and entanglement in order to solve astronomically hard problems.

Examples:
- Simulation of quantum mechanical systems
- Grover’s Search Algorithm
  - \(N\) items in \(N^{\frac{1}{2}}\) steps (instead of \(N\))
- Shor’s Factoring Algorithm
In 1994, Peter Shor developed a quantum algorithm for factoring an $N$-digit number using only $\sim N^2$ steps.

Best known classical algorithm uses $\sim 2^{N^{1/3}}$ steps.

Can be used to break RSA (Rivest, Shamir, Adleman) public-key cryptography system.
Any Questions?