Promise of Quantum Computation

• Classical computers have their limitations:
  – Factoring large numbers takes exponential time.
    • No faster algorithm is known.
  – Searching an unordered list takes $O(n)$ time.
    • No faster algorithm is possible.

• Quantum computers can solve some problems more efficiently than classical computers.
  – Prime factoring: could break RSA encryption.
What Is Quantum Mechanics?

- Objects at the subatomic level behave in ways that have no analog at the macroscopic level.
- Protons, neutrons, and electrons are **not** little billiard balls. They are both *particles* and *waves* at the same time!
- Quantum mechanics describes how these objects really behave. It’s quite weird.

Examples of Quantum Weirdness

- A particle (or an atom) can:
  - Be in two different states at the same time.
  - Be in several places at the same time.
  - Move from A to B without ever occupying the space between them (tunneling).
  - Communicate information to another distant particle instantly (quantum teleportation).
Quantum Computers

• We can exploit 3 weird quantum phenomena to build a new kind of computer.

Intrinsic Angular Momentum

• Particles have a property (intrinsic angular momentum) that has two distinct values.
• Call the values “up” and “down”.
• Or $+\frac{1}{2}$ and $-\frac{1}{2}$.
• Or $|1\rangle$ and $|0\rangle$.

• Intrinsic angular momentum is called “spin” but that is misleading. Nothing is spinning.
Measurement

• We can measure a particle’s state and we will always get one of two results: $|0\rangle$ or $|1\rangle$.
  – There are no intermediate values. Spin is quantized.

• How do we measure? One way:
  – Pass the particle through a magnetic field.
  – It will go left if its state is $|0\rangle$ and right if $|1\rangle$.
  – Put a detector on each side.

Q Weirdness 1: Mixtures of States

• Before we measure, a particle’s state can be a mixture of “up” and “down”.
• Suppose it’s $\frac{3}{4}$ “up” and $\frac{1}{4}$ “down”.
• When we measure the state, we will get:
  – “Up” with probability 0.75
  – “Down” with probability 0.25
• Once we measure, the state is fixed; it’s either “up” or “down”. No more mixture.
Bits vs. Qubits

• Conventional computers use bits:
  – Value is either 0 or 1. Might be encoded by a voltage, e.g., “0” = 0 volts, “1” = +5 volts.
  – There are no mixture states. A value of +2 volts would indicate a broken computer.

• Quantum computers use qubits instead of bits. Qubits can have mixture states.

Qubits in Mixture States

• Let \(|0>\) denote the 100% “down” state and \(|1>\) the 100% “up” state. These are basis states.
• Any qubit’s state can be expressed in terms of the basis states using two coefficients \(a\) and \(b\):

\[ a|0> + b|1> \]

where \(|a|^2 + |b|^2 = 1\).
Mixture States (cont.)

• Mixture state is: \( a |0\rangle + b |1\rangle \)
• So the 100% “down” state is \( a=1, b=0 \)
  The 100% “up” state is \( a=0, b=1 \)
• Equal mixture of “up” and “down” would be:
  \[
  a = b = \frac{1}{\sqrt{2}}
  \]
  because we must have: \( a^2 + b^2 = \frac{1}{2} + \frac{1}{2} = 1 \)

Q Weird. 2: Complex Amplitudes

• “Normal” mixture coefficients: \( 0 \leq x \leq 1 \).
• Combine by simple addition: \( a + b = 1 \).
• Negative values would make no sense.
  – Can you have a dog that is \( 4/3 \) golden retriever and \( -1/3 \) german shepherd? No!
• But in quantum mechanics, the mixture coefficients are complex numbers!
• That’s why the mixture rule is \( |a|^2 + |b|^2 = 1 \).
Complex Numbers: Cartesian Form

- Define $i$ as $\sqrt{-1}$
- Complex numbers: $p = a + bi$, $q = c + di$

Complex Arithmetic

- Complex numbers: $p = a + bi$, $q = c + di$
- $p+q = (a+bi) + (c+di) = (a+c) + (b+d)i$
- $p\times q = (a+bi) \times (c+di)$
  $\quad\quad = a\times c + a\times d + b\times c + b\times d i$
  $\quad\quad = (ac-bd) + (ad+bc)i$
Complex Numbers: Polar Form

• Defined in terms of a magnitude and phase.
• Complex numbers: \( p = <r, \theta>, \ q = <s, \phi> \)

\[
\begin{align*}
  r &= \sqrt{4^2 + 5^2} \\
  \theta &= \arctan \frac{5}{4}
\end{align*}
\]

Complex Arithmetic (Polar)

• Complex numbers: \( p = <r, \theta>, \ q = <s, \phi> \)
• \( p+q = <r, \theta> + <s, \phi> = \text{something messy} \)
• \( p\times q = <r, \theta> \times <s, \phi> = <r\cdot s, \ \theta+\phi> \)
• Some common constants:
  \( 1 = <1, 0^\circ> \quad -1 = <1, 180^\circ> \)
  \( i = <1, 90^\circ> \quad -i = <1, 270^\circ> \)
  So \( i \times i = <1\cdot 1, 90^\circ+90^\circ> = <1, 180^\circ> = -1 \)
• Multiplication is just scaling plus rotation!
Complex Magnitude

• In polar form:
  \[ p = <r, \theta> \text{ so } |p| = r \]

• In rectangular form:
  \[ p = a + bi, \text{ so } |p| = \sqrt{a^2 + b^2} \]

• In quantum mechanics, probability is the square of the complex coefficient: \[ |p|^2 \]

Quantum Weirdness 2a: Phase

• Consider a photon in state \[ a|0> + b|1> \].

• The complex coefficients (“amplitudes”) \( a \) and \( b \) have both magnitude and phase.

• Photons have polarization determined by the relative phases of \( a \) and \( b \).
  – Vertically polarized, horizontally polarized, left or right circularly polarized, elliptically polarized, etc.

• Polarized sunglasses filter out photons based on phase to reduce glare.
Logic Gates

Conventional Boolean logic gates:
1-input: the NOT gate
2-input: AND, OR, NAND, NOR, XOR, EQV, ...

Quantum Gates

- 1-input quantum gates change the magnitudes and/or phases of \( a \) and \( b \). Assume state is: \( a|0\rangle + b|1\rangle \).
- Pauli-X gate: \( (a,b) \rightarrow (b,a) \) quantum NOT
- Pauli-Y gate: \( (a,b) \rightarrow (bi,-ai) \)
- Pauli-Z gate: \( (a,b) \rightarrow (a,-b) \) phase flip
- Hadamard: \( (a,b) \rightarrow (a+b,a-b)/\sqrt{2} \)
Quantum Gates

- 2- and 3-input quantum gates perform operations on one qubit based on the values of one or two other qubits.
- Controlled-NOT gate performs NOT on second qubit when first qubit is |1>.

• More gates: Toffoli, Fredkin, etc.

How to Make a Quantum Gate

- Use trapped ions for qubits.
  - Trap them in a vacuum using magnetic fields.
- Zap the ions with:
  - Magnetic fields
  - Lasers
  - Radio waves
QW3: Entanglement (Big Payoff)

• Suppose we have two independent qubits:
  \[ q_1 = a_1 |0\rangle + b_1 |1\rangle \]
  \[ q_2 = a_2 |0\rangle + b_2 |1\rangle \]

• If we measure them, we find that:
  \( q_1 \) is “down” with probability \( |a_1|^2 \)
  \( q_2 \) is “down” with probability \( |a_2|^2 \)

• For \( n \) qubits, we have \( 2^n \) amplitudes.

• But qubits don’t have to be independent…
Entanglement

• We can “hook up” two qubits so that their states are bound together, or “entangled”.
• Now they have a joint state space:

\[ a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \]

where \(a, b, c, d\) can all vary freely, subject to  \[ |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1. \]
• If \(a=d=0\) then \(q_1\) and \(q_2\) have opposite states.

Implications of Entanglement

• If we entangle \(n\) entangled qubits, the resulting system has \(2^n\) independent coefficients.
• You can operate on all \(2^n\) coefficients in parallel by applying quantum gates.
• 50 entangled qubits give \(2^{50} = 10^{15}\) coefficients: more memory than in any computer!
Quantum Algorithms

• Shor’s algorithm can factor numbers.
  – Runs in time polynomial in # of digits.
  – Exponentially faster than conventional computer.
  – Might break RSA encryption.

• In 2001 IBM demonstrated factorization of 15 into 3 and 5 using a 7-qubit quantum computer.

• Another group has factored 21 into 3 and 7.

Quantum Algorithms

• Grover’s algorithm for searching unordered lists (or inverting a function).
  – Runs in time $O(\sqrt{N})$ where $N =$ # of items
  – Conventional computer requires $O(N)$ time.

• Works by exploiting the fact that coefficients have phases that can amplify (if in phase) or attenuate (if out of phase) when added.

• Google wants to use quantum algorithms for fast, sophisticated searching.
Obstacles to Quantum Computers

• Qubits don’t last very long (decoherence).
  – Must keep them isolated to preserve their states.
  – Atoms cooled to almost absolute zero.
  – Any collision is a “measurement” that will “collapse the wave function”: no more mixture.

• Entanglement is tricky to achieve.
  – Gets harder as the number of qubits goes up.

D-Wave Systems “demonstrated” a 28-qubit quantum computer in November 2007 at a SC07 (a supercomputing conference).
What’s Next?

• Will we eventually prove that P = NP or P \neq NP?
• Will the computers for the next generation be made up of quantum particles rather than silicon?
  – Star Trek computers already use qubits!
• Will humans become more and more robotic as they evolve?
  – Smartphones today; Google glasses tomorrow; cyborgs in 50 years?
• Will robots eventually replace humans as the dominant race due to their superior intelligence?