Putting Weirdness to Work: Quantum Information Science

John Preskill, Caltech Biedenharn Lecture
6 September 2005
Information is encoded in the state of a *physical* system.
Information is encoded in the state of a quantum system.
Put

Weirdness
to work!
Theoretical Quantum Information Science

is driven by ...

Three Great Ideas:

1) Quantum Cryptography
2) Quantum Computation
3) Quantum Error Correction

Though quantum theory is over 100 years old, these ideas have begun to draw substantial attention in just the past few years.
Classical Bit
Classical Bit
Classical Bit

What went in, comes out.
Quantum Bit ("Qubit")

The two doors are two different ways to prepare or measure the quantum state of an atom or photon (but never mind).
Quantum Bit ("Qubit")

If you open the *same* door that you closed, you can recover the bit from the box.
Quantum Bit ("Qubit")
Quantum Bit ("Qubit")

If you open a different door than you closed, the color is random (red 50% of the time and green 50% of the time).
Quantum Bit ("Qubit")
Quantum Bit ("Qubit")

If you open the *same* door that you closed, you can recover the bit from the box.
Quantum Bit ("Qubit")
Quantum Bit ("Qubit")

If you open a different door than you closed, the color is random (red 50% of the time and green 50% of the time).
Quantum Copier
No cloning!
Put Weirdness to work!
No tapping a quantum telephone!!
Unbreakable code: if Alice and Bob share a random key (string of bits) that is not known to Eve.
Message: HI BOB
01001000 01001001 00100000 01000010 01001111 01000010
01110100 10111001 00000101 10101001 01011100 01110100
00111100 11110001 00100101 11101011 00010011 00110110
Message: HI BOB

Alice

Eve

Bob

HI BOB
Message: HI BOB

Alice and Bob can communicate privately if they share a random key that Eve doesn’t know.

HI BOB
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice Announces Doors She Used!!


<table>
<thead>
<tr>
<th>Lorem Ipsum</th>
<th>Lorem Ipsum dolor</th>
<th>Lorem Ipsum dolor</th>
<th>Lorem Ipsum dolor</th>
<th>Lorem Ipsum dolor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

Alice

Quantum News

January 15, 1997 Volume 1, Issue 1

“Spooky action at a distance”
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Alice can use quantum information (qubits) to send a random key to Bob.
Quantum key distribution, augmented by classical protocols that correct errors and amplify privacy, is *provably* secure against *arbitrary* eavesdropping attacks.

Alice can use quantum information (qubits) to send a random key to Bob.
QKD for sale!

Security is based on the principle that copying of quantum signals can be detected, a property not shared by classical information.

Experiments have demonstrated the feasibility of quantum key distribution (QKD) protocols in which single-photon pulses are sent through (150 km) telecom fibers.

Furthermore, quantum key distribution is now commercially available. You can order one over the (classical) Internet.

Bennett-Brassard ‘84
Open either door in Pasadena, and the color of the ball is *random*. Same thing in Andromeda.
Quantum Correlations

But if we both open the same door, we always find the same color.
Quantum Correlations

Quantum information can be *nonlocal*, shared equally by a box in Pasadena and a box in Andromeda.

This phenomenon, called *quantum entanglement*, is a crucial feature that distinguishes quantum information from classical information.
Classical Correlations
Classical Correlations
Classical Correlations

Quantum Correlations

Aren’t boxes like soxes?
Einstein's boldly original 1905 paper on the light quantum hypothesis had helped to launch quantum theory. His 1935 paper, with Podolsky and Rosen (EPR), launched the theory of quantum entanglement. Arguably, it is the last paper of Einstein's career that still reverberates loudly today.

To Einstein and his collaborators, quantum entanglement was so unsettling as to indicate that something is missing from our current understanding of the quantum description of Nature.
“Another way of expressing the peculiar situation is: the best possible knowledge of a whole does not necessarily include the best possible knowledge of its parts … I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives [quantum states] have become entangled.”

“It is rather discomforting that the theory should allow a system to be steered or piloted into one or the other type of state at the experimenter’s mercy in spite of his having no access to it.”

Quantum Entanglement

Bell ‘64

Pasadena

Andromeda
Quantum information can be *nonlocal*; quantum correlations are a stronger resource than classical correlations.

Bell ‘64
Quantum entanglement

Alice and Bob are cooperating, but distantly separated, players on the same team, playing a game. They cannot communicate, but in order to win the game, they must make correlated moves.

Goal: \[ a \oplus b = x \land y \]

Bell’s theorem (1964): If Alice and Bob share classically correlated bits (which were prepared before the game began), they can win the game with probability no higher than 75% (averaged over all possible inputs), but if they share quantumly correlated qubits (quantum entanglement), they can win the game with probability 85.4%.

This example illustrates that quantum correlations are a stronger resource than classical correlations, enabling us to perform tasks that would otherwise be impossible.
Quantum entanglement

Bell’s theorem (1964): Alice and Bob have a higher probability of winning the game if they share quantumly correlated qubits (quantum entanglement) than if they shared classically correlated bits.

In experimental tests, physicists have played the game (e.g. with entangled photons – Aspect, 1982) and have won with a probability that exceeds what is possible classically (though there are still loopholes to these tests!).

Quantum information can be \textit{nonlocal}; quantum correlations are a stronger resource than classical correlations.

* Spooky action at a distance!!
Quantum entanglement

Bell’s theorem (1964): Alice and Bob have a higher probability of winning the game if they share quantumly correlated qubits (quantum entanglement) than if they shared classically correlated bits.

In experimental tests, physicists have played the game (e.g. with entangled photons – Aspect, 1982) and have won with a probability that exceeds what is possible classically (though there are still loopholes to these tests!).

* Spooky action at a distance!!
Classical Correlations

Quantum Correlations

Aren’t boxes like soxes?
Always: an even number of red socks.
an odd number of green socks.
Always: an even number of red socks. an odd number of green socks.
Always: an even number of red socks. an odd number of green socks.
Always: an even number of red socks.
an odd number of green socks.
We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.
We open door number 1 of two of the boxes, and open door number 2 of the other box. We *always* find an even number of red balls and an odd number of green balls.
We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.
We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.
We open door number 1 of two of the boxes, and open door number 2 of the other box.

We always find an even number of red balls and an odd number of green balls.

By opening doors of the first two boxes, we can determine what will happen if we open either door 1 or door 2 in the third box.
We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.

By opening doors of the first two boxes, we can determine what will happen if we open *either* door 1 or door 2 in the third box.
If we open door number 1 of two boxes, and open door number 2 of the other box, we *always* find an even number of red balls and an odd number of green balls.

But... what will happen if we open door number 2 of all three boxes?
If we open door number 1 of two boxes, and open door number 2 of the other box, we *always* find an even number of red balls and an odd number of green balls.

If . . . 

then . . .
If we open door number 2 of all three boxes, we expect that the number of red balls will always be even, and the number of green balls will always be odd.
But, in fact, when we open door number 2 on all three boxes, we find an odd number of red balls and an even number of green balls!
But, in fact, when we open door number 2 on all three boxes, we find an odd number of red balls and an even number of green balls!
But, in fact, when we open door number 2 on all three boxes, we *always* find an odd number of red balls and an even number of green balls!
Boxes are *not* like soxes!

When the three quantum boxes are entangled, opening two of the boxes seems to "influence" what will happen when we open the third box! (But in a subtle way that does not allow us to send a message from one box to another.)

We must not reason based on what might have happened but did not in fact happen (e.g., “what if we had opened door number 1 instead of door number 2?”).
Put Weirdness to work!
10 classical bits.
10 classical bits.
1,000 numbers to describe 10 qubits
1,000 numbers to describe 10 qubits
1,000 numbers to describe 10 qubits
1,000 numbers to describe 10 qubits
1,000,000 numbers to describe 20 qubits
1,000,000 numbers to describe 20 qubits
1,000,000 numbers to describe 20 qubits
1,000,000,000 numbers to describe 30 qubits
1,000,000,000 numbers to describe 30 qubits
1,000,000,000 numbers to describe 30 qubits
To describe 300 qubits, we would need more numbers than the number of atoms in the visible universe!
We can’t even hope to describe the state of a few hundred qubits in terms of classical bits.

Might a computer that operates on qubits rather than bits (a quantum computer) be able to perform tasks that are beyond the capability of any conceivable classical computer?
Prime Numbers

Finding Prime Factors

15 = 3 × 5
Finding Prime Factors

$91 = 7 \times 13$
Finding Prime Factors

2537 = ? × ? ?
Finding Prime Factors

\[2537 = 43 \times 59\]
Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

= ? × ?

MISSION: IMPOSSIBLE
Finding Prime Factors

\[
\begin{array}{c}
1807082088687 \\
4048059516561 \\
6440590556627 \\
8102516769401 \\
3491701270214 \\
5005666254024 \\
4048387341127 \\
5908123033717 \\
8188796656318 \\
2013214880557
\end{array}
\times
\begin{array}{c}
3968599945959 \\
7454290161126 \\
1628837860675 \\
7644911281006 \\
4832555157243
\end{array}
= 
\begin{array}{c}
4553449864673 \\
5972188403686 \\
8972744088643 \\
5630126320506 \\
9600999044599
\end{array}
\times
\]
We can’t even hope to describe the state of a few hundred qubits in terms of classical bits.

Might a computer that operates on qubits rather than bits (a quantum computer) be able to perform tasks that are beyond the capability of any conceivable classical computer?
Try every key, until one fits the lock.
Try all the keys at once!

Massive Parallelism
<table>
<thead>
<tr>
<th>Classical Computer</th>
<th>Quantum Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Classical Computer Icon]</td>
<td>![Quantum Computer Icon]</td>
</tr>
<tr>
<td>Factor 130 digits in 1 month.</td>
<td>Factor 130 digits in 1 second.</td>
</tr>
<tr>
<td>Factor 400 digits in 10 billion years.</td>
<td>Factor 400 digits in 30 seconds.</td>
</tr>
</tbody>
</table>

**IMPOSSIBLE:**

Peter Shor (1994)
Finding Prime Factors

\[
\begin{align*}
1807082088687 &= \, ? \times \, ? \\
4048059516561 &= \, ? \times \, ? \\
6440590556627 &= \, ? \times \, ? \\
8102516769401 &= \, ? \times \, ? \\
3491701270214 &= \, ? \times \, ? \\
5005666254024 &= \, ? \times \, ? \\
4048387341127 &= \, ? \times \, ? \\
5908123033717 &= \, ? \times \, ? \\
8188796656318 &= \, ? \times \, ? \\
2013214880557 &= \, ? \times \, ? \\
\end{align*}
\]
Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

= Shor ‘94

3968599945959
7454290161126
1628837860675
7644911281006
4832555157243

4553449864673
5972188403686
8972744088643
5630126320506
9600999044599
Decoherence

\[ \frac{1}{\sqrt{2}} \left( \begin{array}{c} \text{Environment} \\ \end{array} \right) \]
How can we protect a quantum computer from decoherence and other sources of error?
What about errors?
What about errors?
What about errors?

Error!
What about errors?
What about errors?
What about errors?
What about errors?

Redundancy protects against errors.
Quantum Copier

No cloning!
What about *quantum* errors?
What about *quantum* errors?
What about *quantum* errors?

Error!
What about *quantum* errors?
What about *quantum* errors?
What about *quantum* errors?

To fix the errors, must we know what door the dragon opened?
A quantum code

Errors are local --- encode information nonlocally:

Even number of 2 = Even number of 2

Even number of 2 = Even number of 2
A quantum code

Odd number of Error

- Four such measurements diagnose the error.
- Measure *only* the parity, or else the quantum information will be damaged.
What about *quantum* errors?
What about quantum errors?

Error!
What about *quantum* errors?
What about *quantum* errors?

Redundancy protects against *quantum* errors!
Ion Trap Quantum Computer
Ion Trap Quantum Computer

Two $^9$Be$^+$ ions in an ion trap at the National Institute of Standards and Technology (NIST) in Boulder, CO.
Ion Trap Quantum Computer
Ion Trap Quantum Computer
Ion Trap Quantum Computer
Ion Trap Quantum Computer
Ion Trap Quantum Computer
Ion Trap Quantum Computer

Cirac  Zoller  Blatt  Wineland
Quantum Achievements

- **Algorithms**: Spectacular speedups relative to classical algorithms for certain problems (like factoring).

- **Cryptography**: Secure quantum key distribution founded on principles of quantum physics.

- **Error correction**: Schemes for protecting quantum information from damage and processing it reliably.

- **Hardware**: Working prototypes for quantum key distribution; coherent quantum gates in small-scale devices.
Quantum Challenges

- **Algorithms**: How can quantum computers be used?

- **Cryptography**: What applications for a “quantum Internet?”

- **Error correction**: How can protection against decoherence and other errors be realized in actual quantum devices?

- **Hardware**: What quantum hardware is potentially scalable to large systems?

And … what are the implications of these ideas for basic physics?
Einstein saw, sooner and more clearly than others, the essential weirdness at the core of quantum theory, what Schrödinger called “quantum entanglement.”

To Einstein, this “spooky action at a distance” presaged the emergence of a deeper theory that would supersede quantum mechanics. In the 70 years since 1935, that has not happened.

But EPR’s insight that quantum entanglement signifies an especially profound (weird) departure from the classical description of Nature has been amply vindicated. And now we face the exciting challenge of putting the weirdness to work.