Microsoft

Microsoft Research Faculty Summit 2013

Microsoft

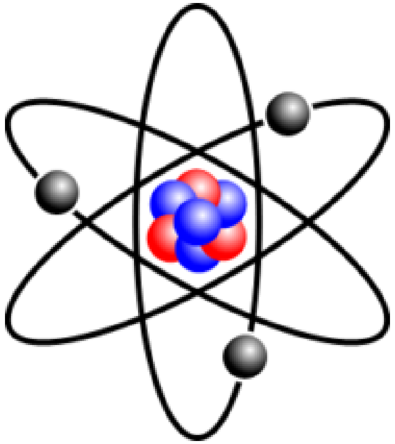
Quantum Mechanics: What's It Good For?

Scott Aaronson
Associate Professor, EECS
MIT

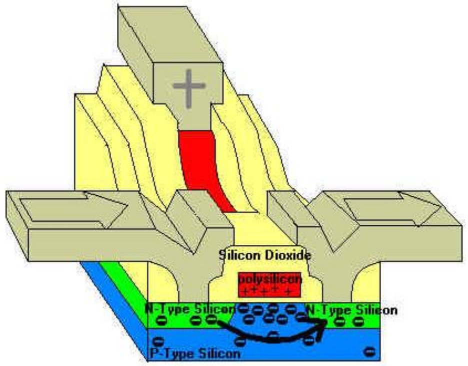
Microsoft Research
Faculty Summit

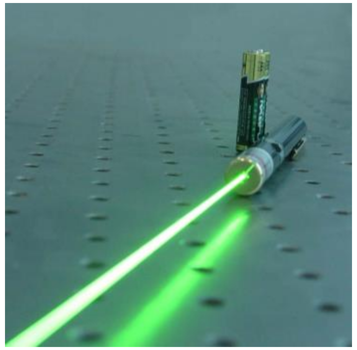
Some “Obvious” Things QM Is Good For

Keeping atoms from disintegrating

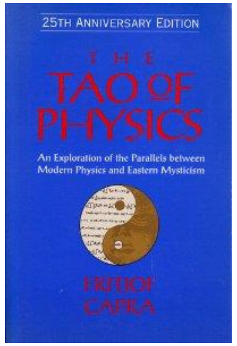


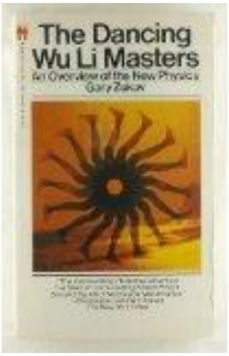
Allowing transistors and lasers to work



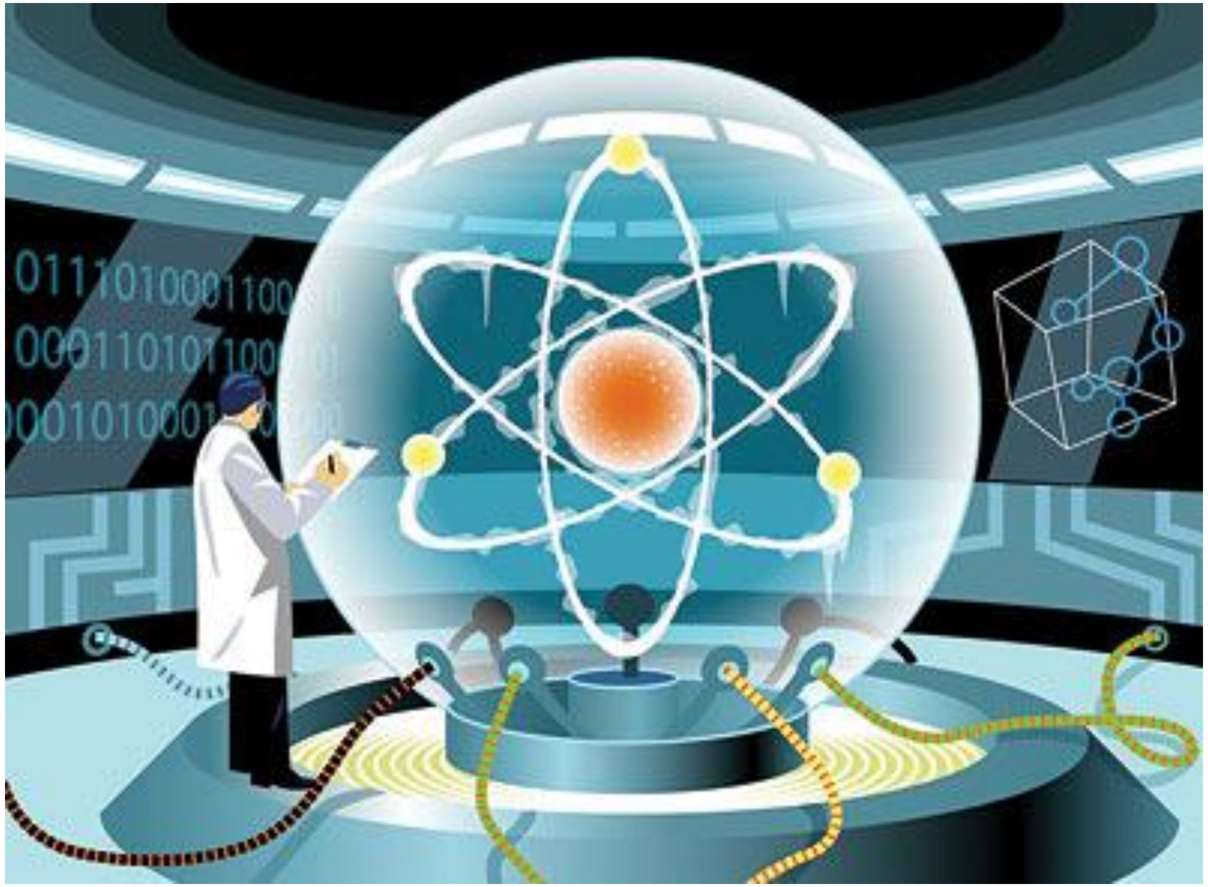


Helping to sell New Age books


25TH ANNIVERSARY EDITION
THE
TAO OF
PHYSICS
An Exploration of the Parallels between
Modern Physics and Eastern Mysticism
FRITJOF
CAPRA



OK, but you're here to hear about quantum computing



First, what **is** quantum mechanics?

APPLICATION LAYER	Electrodynamics	Nuclear Forces	Gravity
OS LAYER	Quantum Mechanics $\lvert\alpha_1\rvert^2+\cdots+\lvert\alpha_n\rvert^2=1,\ \alpha_i\in C$		
HARDWARE LAYER	Mathematics		

Main Quantum Algorithms Known

Shor’s algorithm and variants

Factoring / discrete log / breaking RSA / other problems in group theory and number theory

Grover’s algorithm and variants

Can search an N-element list or evaluate a size-N game tree in ~√N steps, and get subquadratic improvements for many other problems

Quantum simulation

Potentially useful for: chemistry, protein folding, nanomaterials, high-energy physics

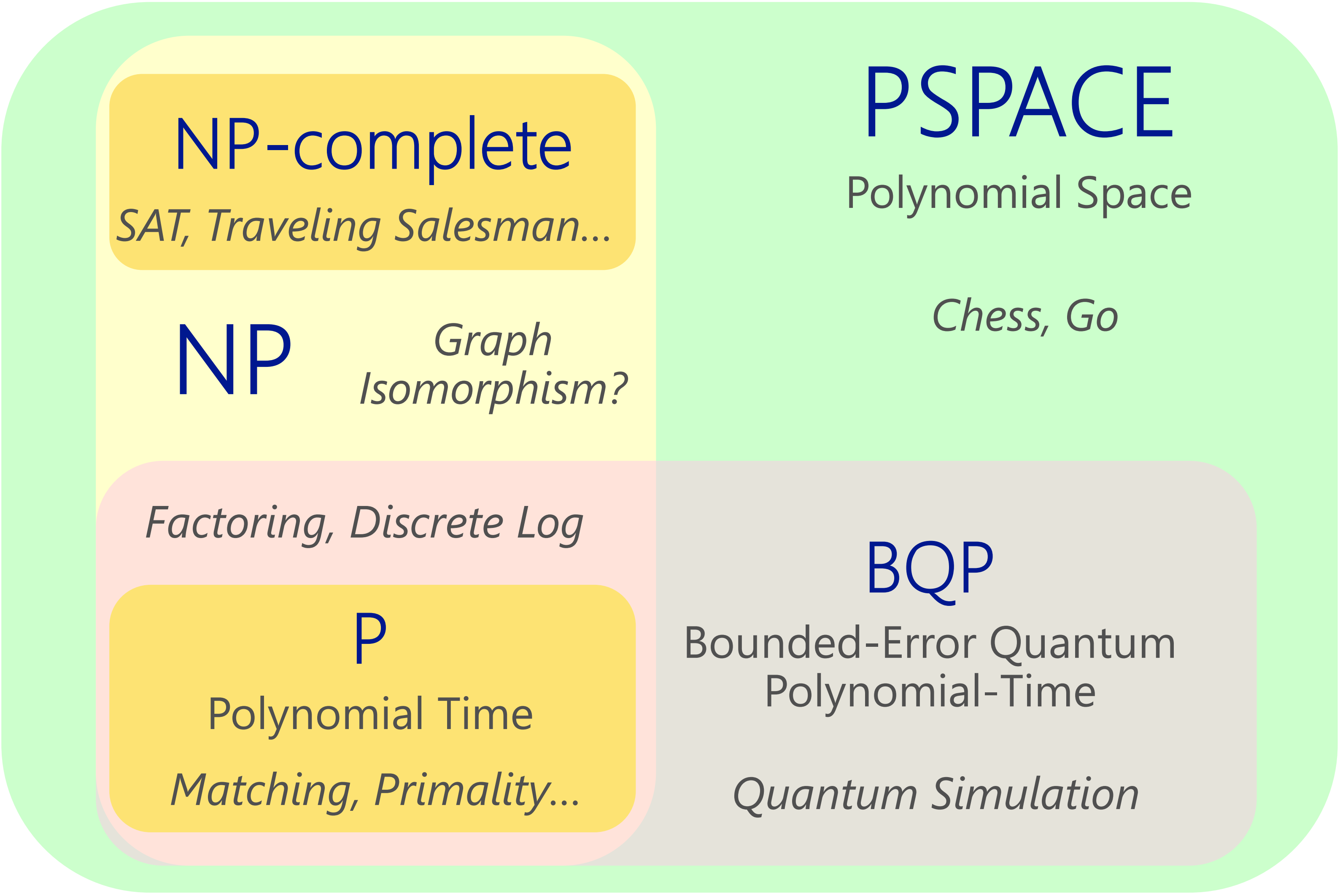
Quantum adiabatic algorithm

“Quantum-enhanced” version of simulated annealing. Performance on practical optimization problems remains a major open question

Other quantum algorithms

Learning properties of a linear system, with possible machine learning applications [Lloyd et al. 2008-2013]; verifying that two functions are close to each other’s Fourier transform [A. 2010]…

Quantum Complexity Theory



NP-complete

SAT, Traveling Salesman…

NP

Graph Isomorphism?

PSPACE

Polynomial Space

Chess, Go

Factoring, Discrete Log

BQP

Bounded-Error Quantum Polynomial-Time

Quantum Simulation

P

Polynomial Time

Matching, Primality…

How good is the evidence for P≠BQP?

Well, if you think Factoring∉P then you have to believe that!

A.-Arkhipov 2011 gave arguably stronger evidence that QCs can solve classically hard sampling problems

OK, what about putting quantum weirdness to work for things other than computation?

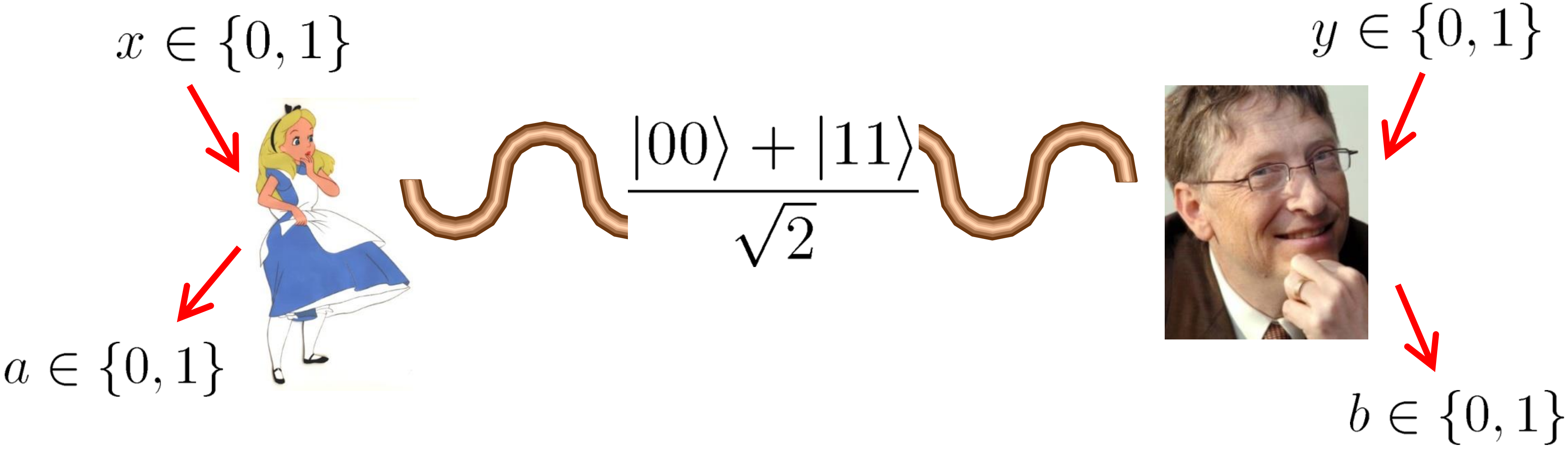
Quantum Random Number Generation

```
1 1 0 0 1 0 0 0 1 0
1 0 0 1 1 1 0 0 1 1
1 1 1 1 1 1 0 1 0 0
1 0 0 1 1 0 1 0 1 1
0 0 0 1 1 1 0 1 0 1
1 1 1 0 1 1 1 0 1 1
1 0 1 0 0 1 1 0 1 1
0 1 0 0 1 0 0 0 0 1
0 0 1 1 1 0 1 1 0 0
1 1 1 1 0 1 1 0 1 1
```

Commercially available

But why should anyone **trust** such a device's output as truly random? Surprisingly, we now know how to solve that problem, using Bell inequality violations! [Colbeck 2009, Pironio et al. 2010, Vazirani and Vidick 2011]

Aside: The Bell Inequality



$x \in \{0, 1\}$

$y \in \{0, 1\}$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$a \in \{0, 1\}$

$b \in \{0, 1\}$

$$\boxed{\Pr[a \oplus b = xy] \approx 0.85 > 3/4}$$

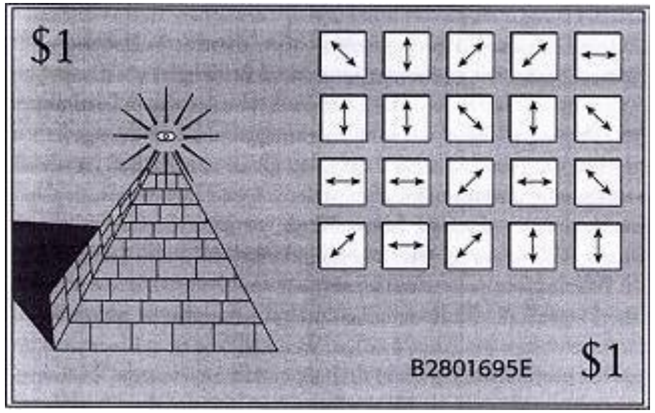
Quantum Cryptography

Again, is already commercial. And again, we now understand (in principle) how to verify untrusted devices using the Bell inequality

[Mayers-Yao 1998 … Vazirani-Vidick 2012]

But requires special hardware, and existing public-key crypto is quite good. Ironically, it might take quantum computers to create the market for quantum crypto!

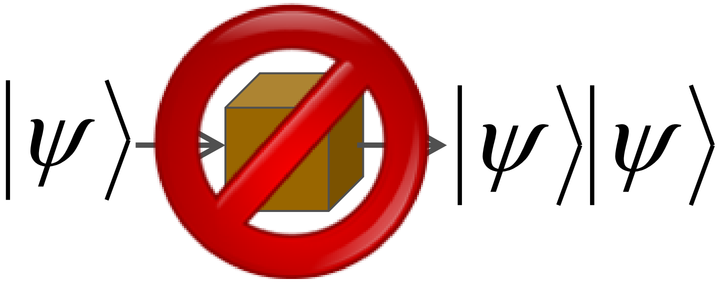
Quantum Money



Proposed by Wiesner circa 1970. In addition to a serial number, each bill would contain qubits in one of the four states |0〉,|1〉,|+〉,|-〉.

Bank remembers states on each bill, so can verify them by measuring

But counterfeiters would be physically unable to copy bills, because of the **No-Cloning Theorem**



$$|\psi\rangle \rightarrow \quad \rightarrow |\psi\rangle|\psi\rangle$$

Problem: Only entity able to verify bills as genuine is the bank that printed them

Publicly-Verifiable Quantum Money

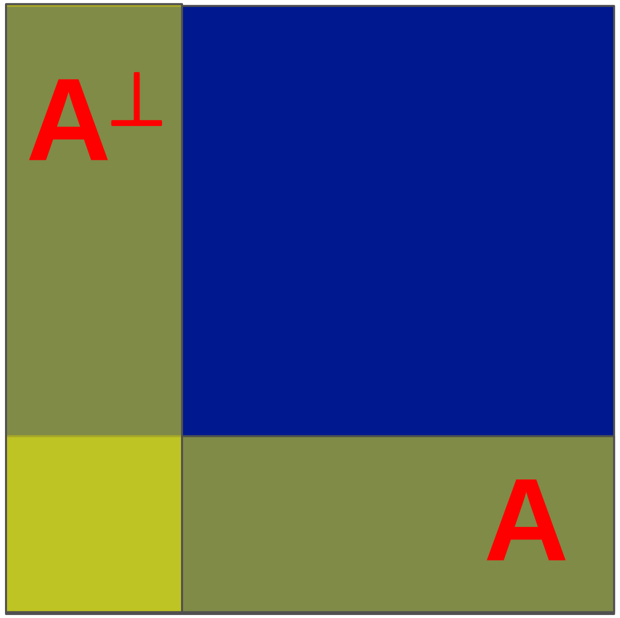
We'd like quantum money states that can't be copied, but that **anyone** can verify as legitimate—not just the bank that printed them

Will certainly require computational assumptions, in addition to quantum mechanics (why?)

Farhi et al. paradigm:

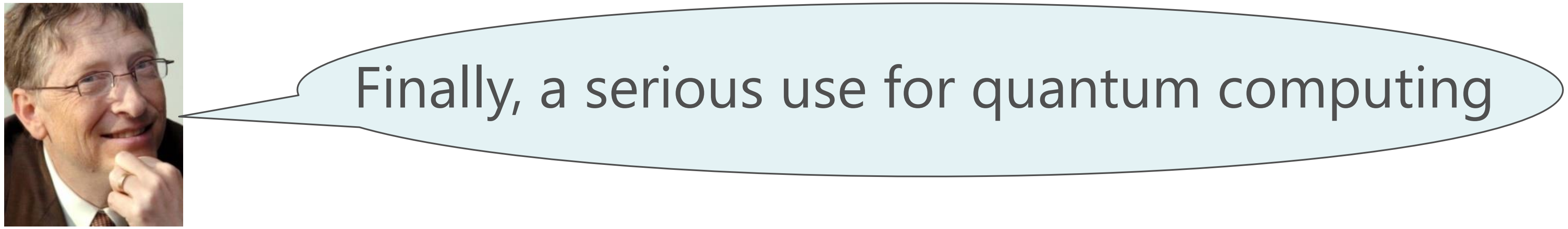
$$|s\rangle|sig_s\rangle|\psi_s\rangle$$

They used knot theory to construct $|\psi_s\rangle$; no formal security argument



A.-Christiano 2012: Publicly-verifiable quantum money based on hidden subspaces, which is secure under a plausible assumption about multivariate polynomial cryptography

Quantum Copy-Protected Software



Goal: Quantum state $|\psi_f\rangle$ that lets you compute an unknown function f, but **doesn't** let you efficiently create more states with which f can be computed

Easy to achieve if f is a point function!

A.-Christiano, work in progress: Proposed scheme to quantumly copy-protect arbitrary functions f. So far, don't know how to argue security (though can prove security of a black-box variant)

Conclusions

Quantum weirdness can indeed be “put to work” in surprising ways

How important will these applications be in real life? And how long until the most dramatic ones become practical? Unfortunately, we don’t know

If we’re intellectually honest, always need to ask: can a classical approach also do this? Why not? (Often the hardest part of a QC project!)

In my opinion, asking what quantum mechanics can do for us has given unprecedented insight into the theory itself—which, for me, is more than enough reason to continue studying this field

Most important application of quantum computing, in my view:
Disproving the people who said it was impossible!