

PHYS 422X/522X:  
Foundations of Quantum Computing

Prof. Thomas Iadecola  
[iadecola@iastate.edu](mailto:iadecola@iastate.edu)

IOWA STATE  
UNIVERSITY

# "THE TALK"

BY SCOTT AARONSON & ZACH WEINERSMITH

YOU'RE GROWING UP SO FAST. I... I THINK IT'S TIME YOU AND I HAD... "THE TALK."

THE QUANTUM COMPUTING TALK.

NO! IT'LL BE AWKWARD! LOOK, I HAVE INTERNET ACCESS. I KNOW ALL ABOUT WHAT PARTICLES DO WHEN NOBODY'S LOOKING!

SO YOU KNOW WHAT A QUBIT IS?

OF COURSE! IT'S A QUANTUM BIT! YOU KNOW... A CLASSICAL BIT IS EITHER 0 OR 1. ON OR OFF. BUT, WHEN A 0 AND 1 LOVE EACH OTHER VERY MUCH, SOMETIMES THEY MAKE A QUBIT, WHICH IS, LIKE, BOTH 0 AND 1 AT THE SAME TIME. TOGETHER. IN PARALLEL. "IN SUPERPOSITION." JUST LIKE SCHRÖDINGER'S CAT IS BOTH DEAD AND ALIVE.

SO, HOW WOULD THESE QUANTUM SUPERPOSITIONS HELP WITH COMPUTATION?

EASY! WITH TWO QUBITS, THERE ARE FOUR POSSIBILITIES: 00, 01, 10, 11. WITH THREE QUBITS, THERE ARE EIGHT POSSIBILITIES, AND SO ON, THE NUMBER DOUBLING WITH EACH QUBIT YOU ADD.

SO, WITH QUANTUM COMPUTERS, YOU'D JUST GET ALL THESE POSSIBILITIES WORKING ON YOUR PROBLEM IN PARALLEL, EACH ONE TRYING A DIFFERENT POTENTIAL ANSWER...

[Character looking thoughtful]

I WISH YOU WOULDN'T READ THOSE MAGAZINES. THEY'RE BAD FOR CHILDREN.

I'M NOT A CHILD!

\*sigh\*

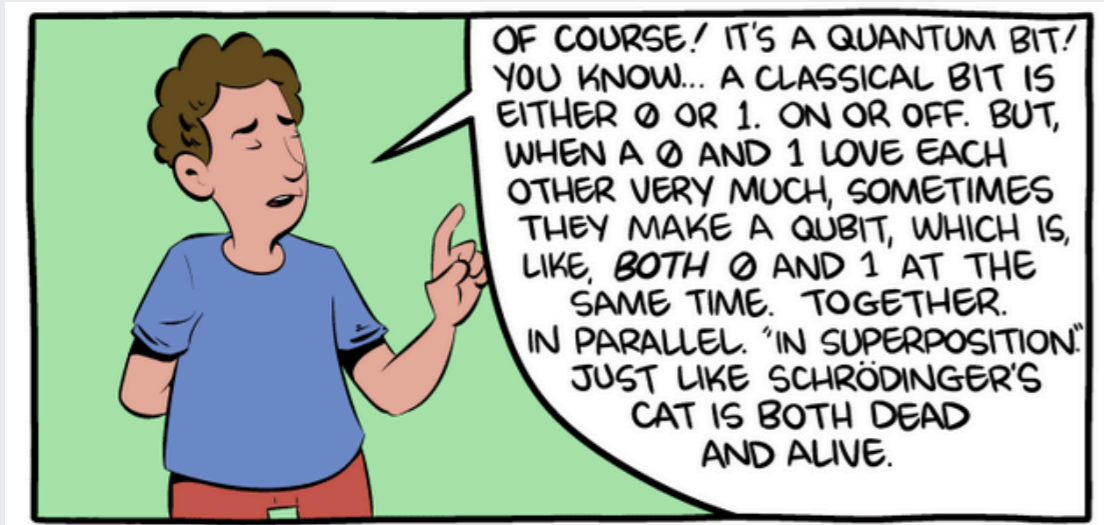
# From Bits to Qubits

Classical bit: 0, 1

Store information in **bit strings**

Ex: “quantum” =

```
01110001 01110101 01100001
01101110 01110100 01110101
01101101
```

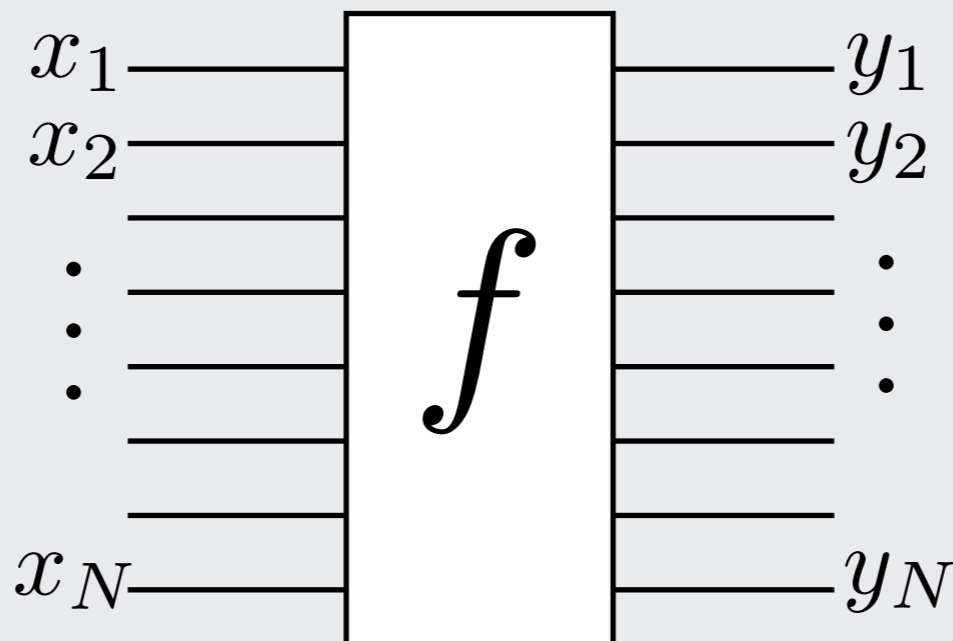


Computation: Transform one bit string into another using a predefined function (a “computer program”) represented in terms of **logic gates**)

Ex: An  $N$ -bit function  $f$

$$x = (x_1, x_2, \dots, x_N)$$

$2^N$  possible inputs



$$y = (y_1, y_2, \dots, y_N)$$

$2^N$  possible outputs

# From Bits to Qubits

“A qubit... is, like, both 0 and 1 at the same time...”

Qubit (=quantum bit): A physical system with two “states”  $|0\rangle$ ,  $|1\rangle$  that is described by **quantum mechanics**



“Dirac notation”

Can form **superposition** states

$$|\psi\rangle = a |0\rangle + b |1\rangle \quad a, b \in \mathbb{C}$$
$$|a|^2 + |b|^2 = 1$$

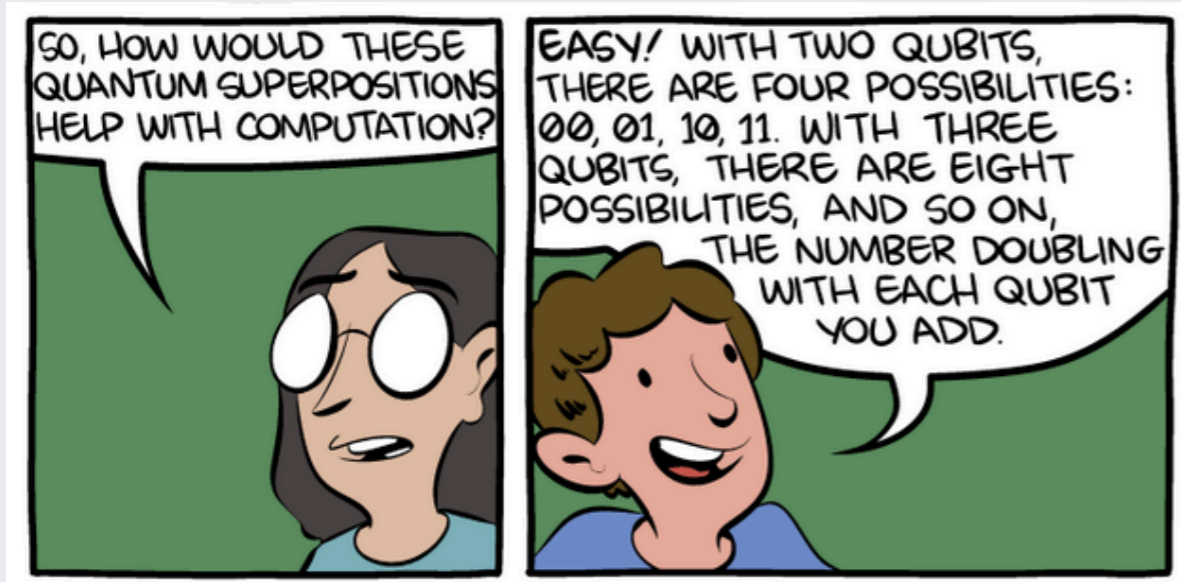
**Probabilistic** objects:  $|a|^2 =$  probability of being a 0 bit

$|b|^2 =$  probability of being a 1 bit

Ex:

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \quad 50/50 \text{ mixture of 0 and 1}$$

# From Bits to Qubits



2 bits:  $4=2^2$  possibilities

00, 01, 10, 11

3 bits:  $8=2^3$  possibilities

000, 001, ..., 110, ..., 111

For qubits, any superposition is allowed!

Ex: 2 qubits

$$a, b, c, d \in \mathbb{C}$$

$$|\psi\rangle = a |00\rangle + b |01\rangle + c |10\rangle + d |11\rangle$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

Ex:  $N$  qubits

$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} |x\rangle$$

Notation: Integer  $x$  corresponds to a bit string of length  $N$

$$|x=0\rangle = |0\dots 00\rangle$$

$$|x=1\rangle = |0\dots 01\rangle$$

$$|x=2\rangle = |0\dots 10\rangle$$

$$|x=3\rangle = |0\dots 11\rangle$$

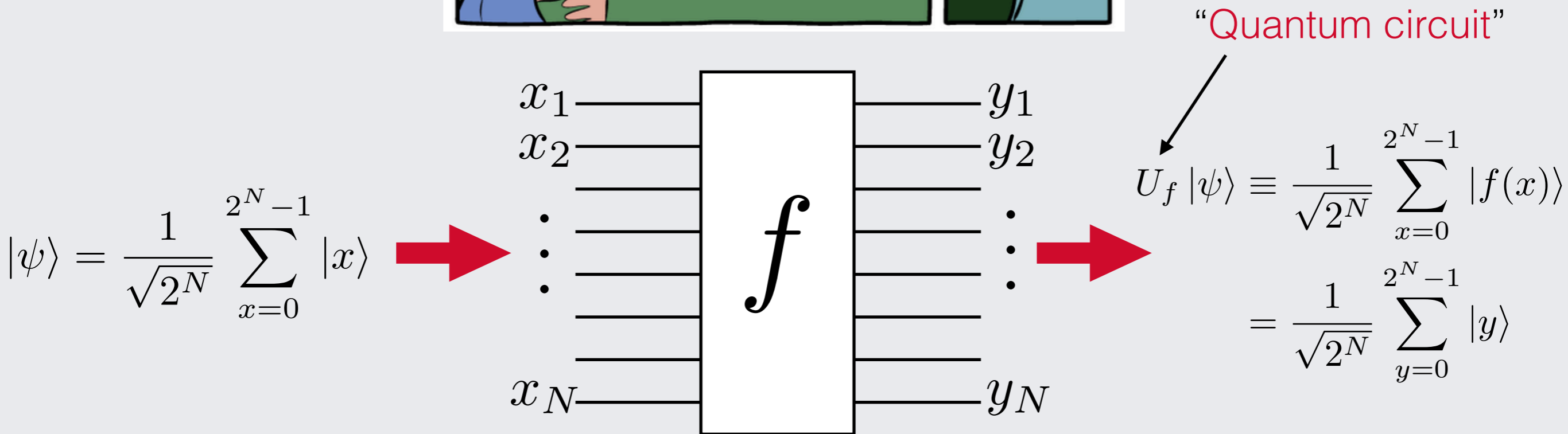
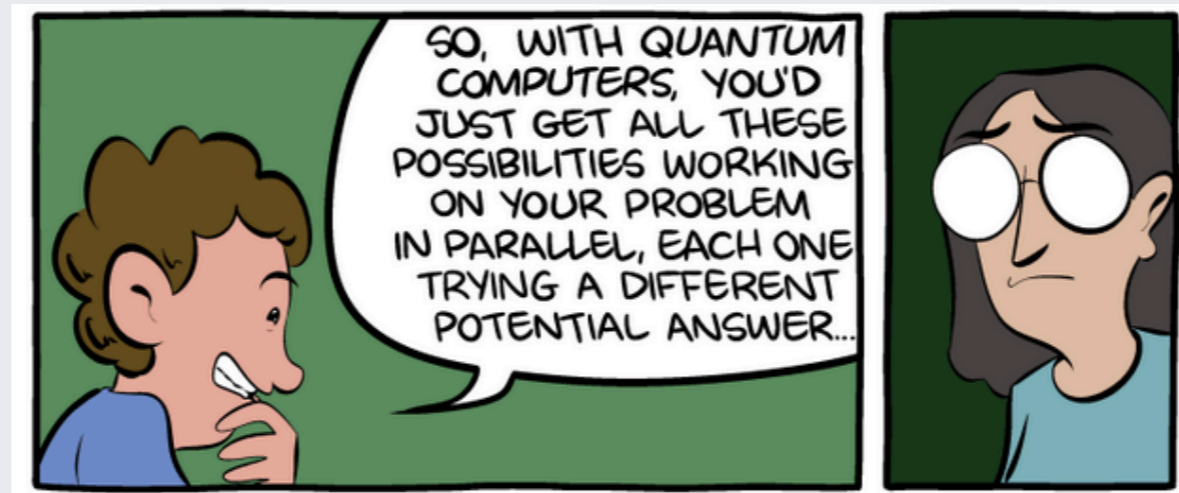
...

$$|x=2^N-1\rangle = |1\dots 1\rangle$$

Equal probability of all classical  $N$ -bit strings

# “Quantum Parallelism”

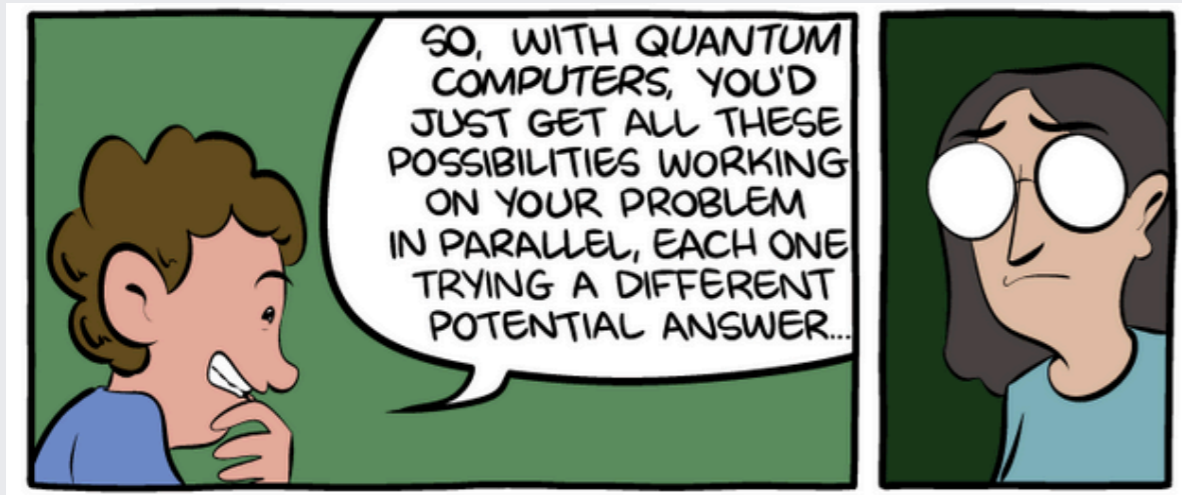
Or, “How quantum computers **don't** work”



A quantum computer with  $N$  qubits is like having  $2^N$  classical computers running in parallel!

# “Quantum Parallelism”

Or, “How quantum computers **don’t** work”



A quantum computer with  $N$  qubits is like having  $2^N$  classical computers running in parallel!

This is super exciting! Suppose we had  $N=300$  qubits:

$$2^{300} \approx 10^{90}$$

# of atoms in the known universe  $\approx 10^{80}$

There aren't enough atoms in the universe to build a classical computer that can handle all  $2^{300}$  inputs simultaneously!

# “Quantum Parallelism”



Unfortunately, quantum computing is not that simple!

$$\begin{aligned} U_f |\psi\rangle &\equiv \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} |f(x)\rangle \\ &= \frac{1}{\sqrt{2^N}} \sum_{y=0}^{2^N-1} |y\rangle \end{aligned}$$

A quantum computer can *make* this state, but we still have to extract the answer from it.

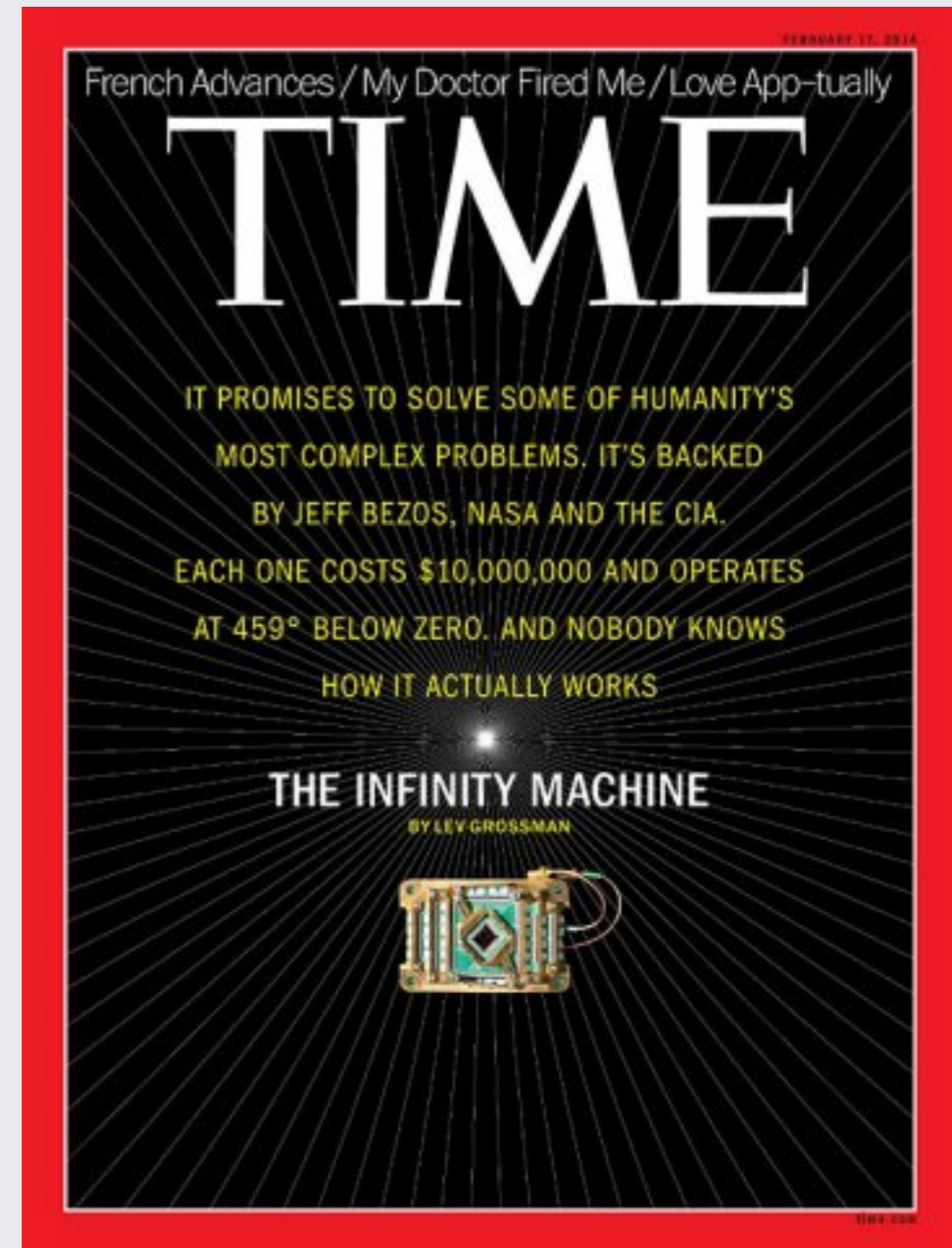
This turns out to be hard!

Huge interdisciplinary research activity in academia and industry is devoted to finding problems where quantum parallelism can be harnessed effectively

# Applications/Hype

## Long-term

- Shor's algorithm for **factoring** large numbers: Breaks RSA encryption!
- Shor's algorithm for **discrete logarithms**: Breaks Diffie-Hellman encryption!
- Grover's **search** algorithm for unstructured databases
- Solving systems of **linear equations**: Possible implications for many fields, including **machine learning**



## Near-term

- **Simulating quantum mechanics**: Advancing basic science (e.g. small-scale quantum chemistry, condensed matter physics)
  - Possible first steps toward larger-scale advances in chemistry, drug design, etc.

## Goals of this course are to understand:

- **How** quantum systems can be used to store and process information; **why** quantum computers can provide a “**quantum advantage**” over classical ones
- (to some extent) **What** physical systems could make good quantum computers; **what** kinds of computational problems they could solve in the near term

## And, most importantly:

Give you the background you need to learn more in the future!

# Course Content Plan (Subject to Change!)

Unit 1: Linear Algebra Review

Unit 2: Introduction to Quantum Mechanics

Unit 3: Introduction to Classical Computation

Unit 4: Quantum Circuits

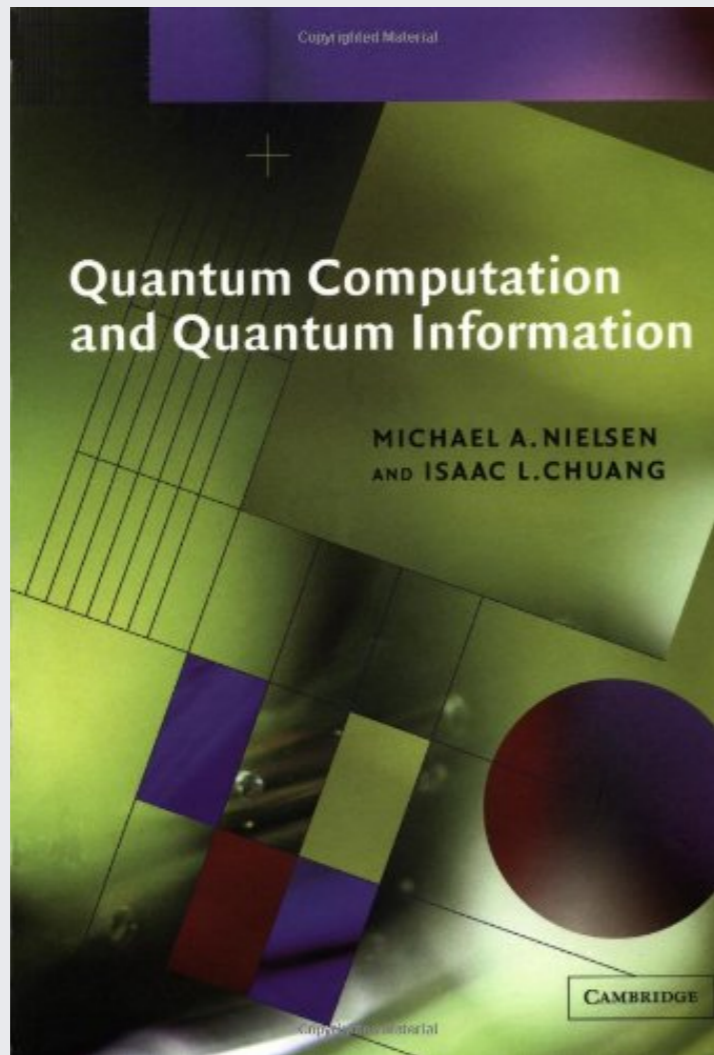
Unit 5: Physical Realizations

Time permitting!



Unit 6: Near-Term Quantum Algorithms

Textbook: Nielsen and Chuang, *Quantum Computation and Quantum Information* (N&C)



The gold standard QC textbook!