Quantum computation and quantum error correction

Leonid Pryadko

UC, Riverside

June 14, 2017

Quantum computation and quantum error correction

Leonid Pryadko

UC, Riverside

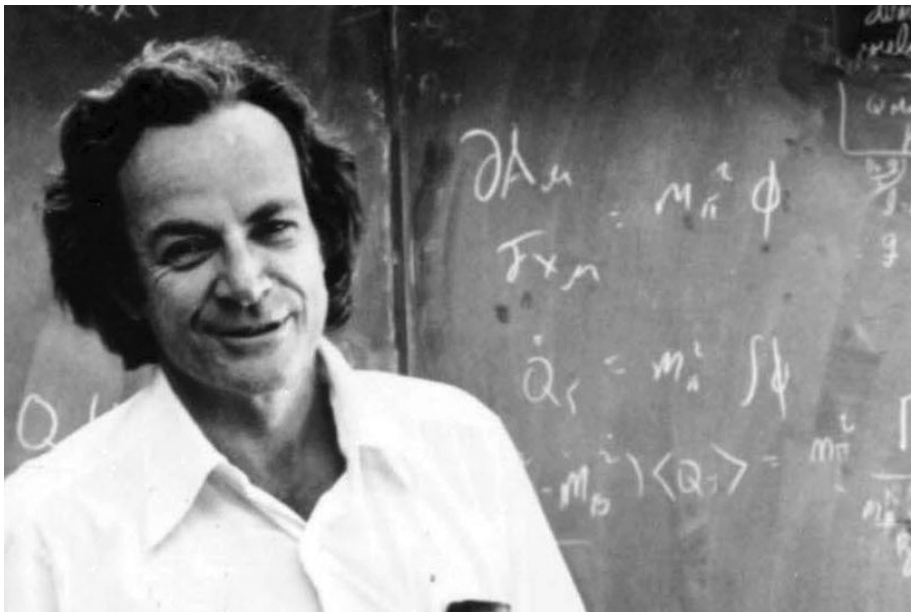
June 14, 2017

- Quantum computer: Why and How?
- Analog vs. Digital & classical error correction
- Quantum mechanics
- Simple quantum codes
- Fault-tolerance and threshold theorem
- Our results and outlook for quantum computation

Quantum computation: **WHY**

Richard Feynman (1982): if quantum many-body simulations are so hard, perhaps one could use these as a model of computation

quantum computation



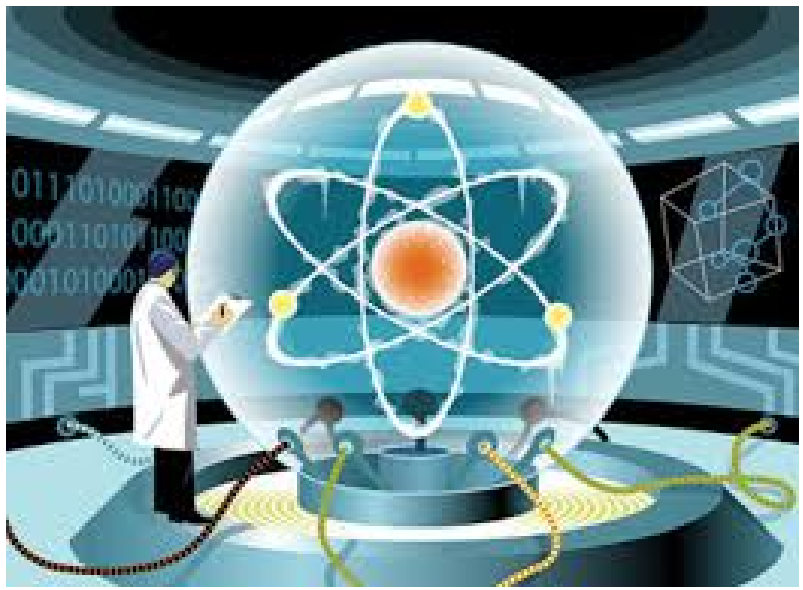
Peter Shor (1994): Polynomial complexity quantum algorithm for factoring large numbers. This would break most encription schemes used for secure communication.

At this point quantum communication is just a fantasy, akin to superluminal space travel

Quantum computation: **HOW**

Peter Shor (1995): Quantum error correction and **threshold theorem**: if you can manipulate quantum bits with sufficient precision, scalable quantum computation is possible (you can build an arbitrarily large quantum computer).

A number of quantum bit (qubit) designs are now being developed…



Analog vs. Digital

Analog computers use circuit properties to integrate differential equations

- Limited for specific problems
- Accuracy limited
- Complexity limited
- Fail frequently

Example: analog cell phone

- Tend to use more power
- Noisy

Digital circuits: built-in error protection because of non-linearity of the threshold between 0 and 1.

This is not the end of the story!

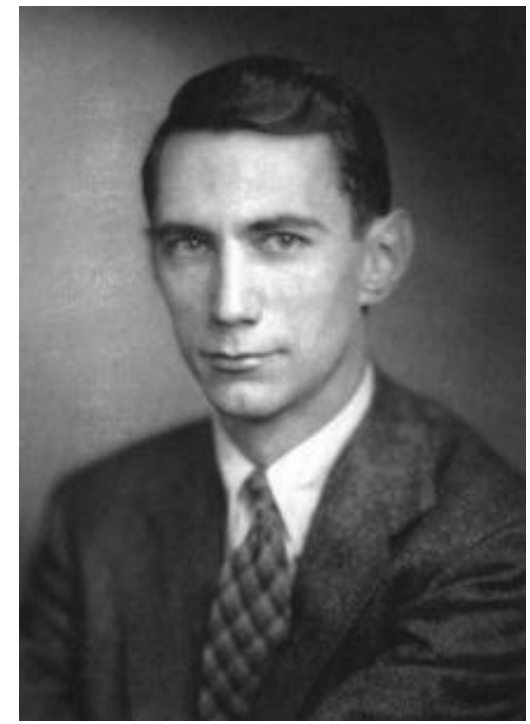
Classical error correction

Example: repetition code.

- messages: $\{0, 1\}$ ($k = 1$ bit of information)
- transmit: 00000 for 0, 11111 for 1 ($n = 5$ bits vs. $k = 1$).
- Code rate $R = k/n$.
- Decoding: majority vote.

Theorem: This can be used to transmit information reliably over a noisy channel (not very efficient, though)

Claude Shannon (1948): for any given degree of noise contamination of a communication channel, it is possible to communicate discrete data (digital information) nearly error-free up to a computable maximum rate through the channel



Classical binary linear codes

- **Repetition code** $[n, 1, n]$: $\mathbf{c}_0 = \underbrace{00\ldots0}_{n}$, $\mathbf{c}_1 = \underbrace{11\ldots1}_{n}$.
  - Code distance $d = n$ is the min Hamming weight of $\mathbf{c} \neq 0$.
  - Use majority vote to decode with up to $\lfloor d/2 \rfloor$ bit flips
  - OK for per-bit error probability $p < \dfrac{\delta}{2} \equiv \dfrac{d/n}{2}$ for $n \to \infty$.

Classical binary linear codes

- **Repetition code** $[n, 1, n]$: $\mathbf{c}_0 = \underbrace{00\ldots0}_{n}$, $\mathbf{c}_1 = \underbrace{11\ldots1}_{n}$.
  - Code distance $d = n$ is the min Hamming weight of $\mathbf{c} \neq 0$.
  - Use majority vote to decode with up to $\lfloor d/2 \rfloor$ bit flips
  - OK for per-bit error probability $p < \dfrac{\delta}{2} \equiv \dfrac{d/n}{2}$ for $n \to \infty$.

- **Decoding threshold** p_c: Consider an infinite family of error correcting codes. With probability p for independent errors per (qu)bit, at $p < p_c$, a large enough code can correct all errors with success probability $P \to 1$, but not at $p > p_c$

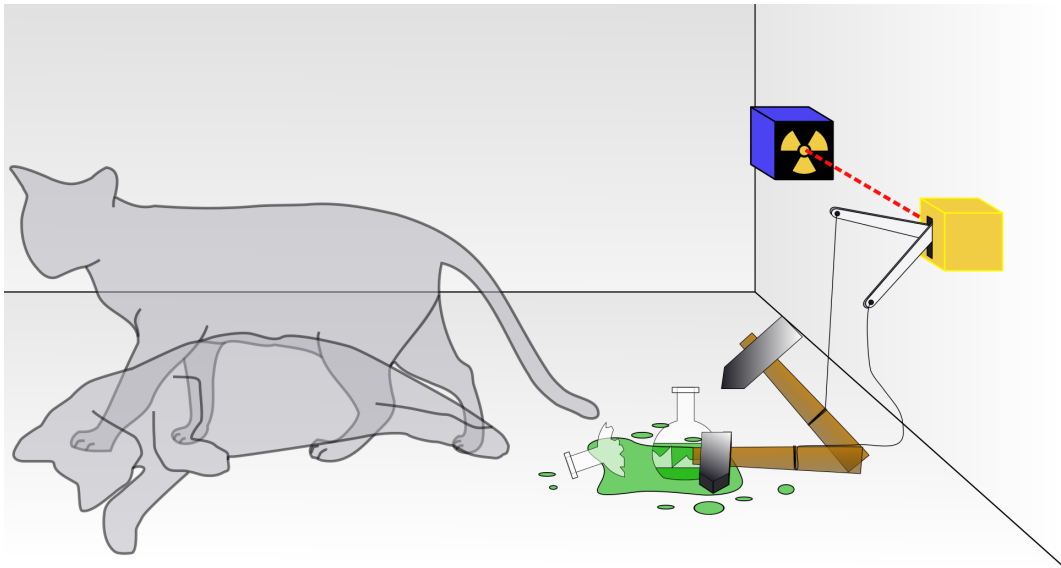
- **Example:** code family with **finite relative distance** $\delta = d/n$. A code can detect any error involving $w < d$ (qu)bits, and distinguish between any two errors involving $w < d/2$ qubits each. For such a family, $p_c \geq \delta/2$.

Error correction in your life

- Audio CD: two levels of encoding using Reed-Solomon codes – can correct errors of up to 3500 bits (2.4mm missing). Make sure all scratches are across the tracks!
- DVD: similar code, but larger data blocks.
- Hard disk and DRAM of your computer
- Local networks and internet
- Cellular communications
- Satellite communications
- Deep space missions

Quantum mechanics

- Quantum objects naturally exist in superposition states $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.
- When you look (measure), the outcomes come with probabilities $P_0 = |\alpha|^2, \quad P_1 = |\beta|^2$
- The coherence is usually lost quickly due to interaction with the environment



Quantum computer operates with many-body superposition states

$$|\psi\rangle = \alpha_0\,|000\rangle + \alpha_1\,|001\rangle + \ldots + \alpha_7\,|111\rangle$$

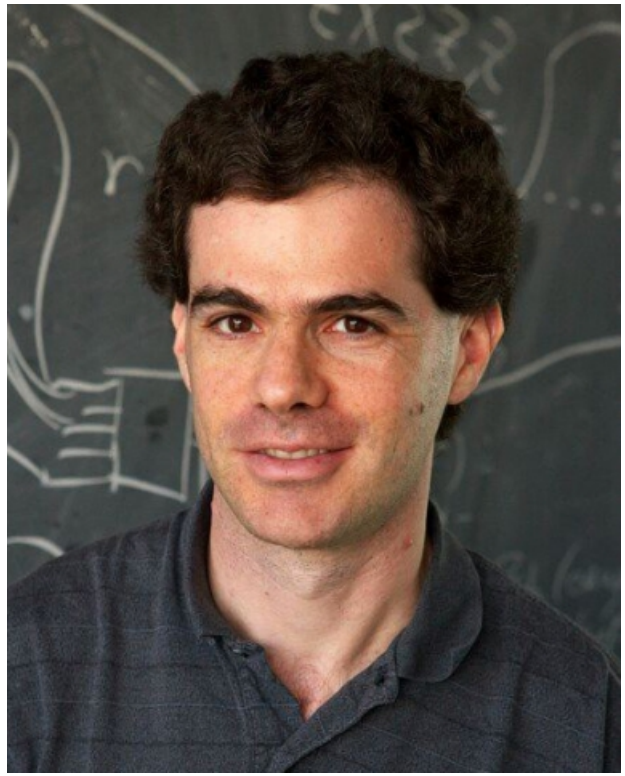
Measuring a single qubit projects onto one of the two states:

$$\psi_0 = e^{i\phi_0}\left[\alpha_0\,|000\rangle + \alpha_1\,|001\rangle + \alpha_2\,|010\rangle + \alpha_3\,|011\rangle\right]$$

$$\psi_1 = e^{i\phi_1}\left[\alpha_4\,|100\rangle + \alpha_5\,|101\rangle + \alpha_6\,|110\rangle + \alpha_7\,|111\rangle\right]$$

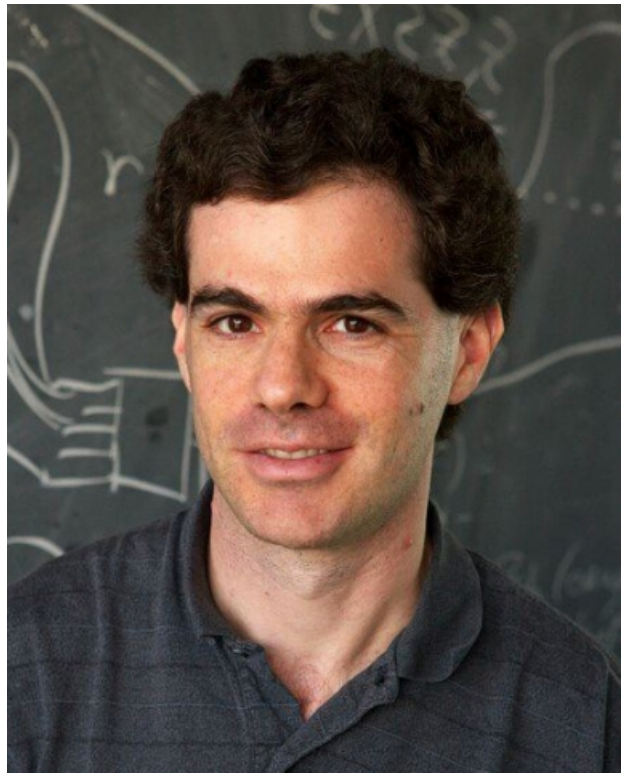
Quantum error correction codes

- Main issue: have to protect an unknown quantum superposition state without doing any measurements that would destroy the superposition
- Most important class of such codes are *stabilizer codes* invented by Daniel Gottesman (1997 Caltech thesis)



Quantum error correction codes

- Main issue: have to protect an unknown quantum superposition state without doing any measurements that would destroy the superposition
- Most important class of such codes are *stabilizer codes* invented by Daniel Gottesman (1997 Caltech thesis)

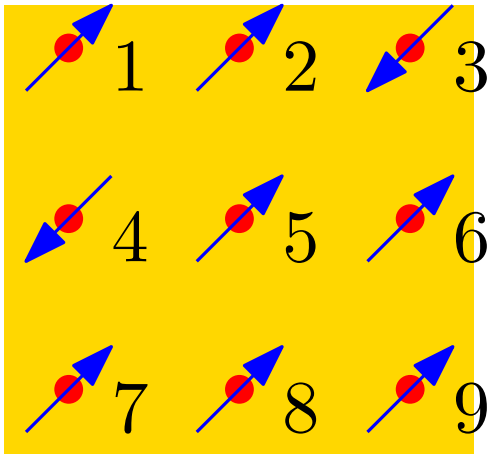


Toy example: version of the repetition code
Original state: $\psi = \alpha\,|0\rangle + \beta\,|1\rangle$
Encoded: $\psi = \alpha\,|000\rangle + \beta\,|111\rangle$

Measure the parity of neighboring qubits $Z_1 Z_2 = 1$, $Z_2 Z_3 = 1$, in both states of superposition, change sign when one of the qubits is flipped — no protection against phase errors!

Simple quantum error correction codes

Shor code: encode 1 qubit in 9, correct any one-qubit error



Measure: $Z_1 Z_2$, $Z_2 Z_3$ – horizontal pairs as in repetition code against bit flip errors

$\begin{pmatrix} X_1 X_2 X_3 \\ X_4 X_5 X_6 \end{pmatrix}$, $\begin{pmatrix} X_4 X_5 X_6 \\ X_7 X_8 X_9 \end{pmatrix}$ – against phase errors.

Here $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$, $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ are 2×2 single-qubit Pauli matrices, $XZ = -ZX$.

$Z_1|01\rangle = |01\rangle$, $Z_2|01\rangle = -|01\rangle$, etc.

5-qubit code: measure $Z_1 X_2 X_3 Z_4$, $Z_2 X_3 X_4 Z_5$, $Z_1 Z_3 X_4 X_5$, $X_1 Z_2 Z_4 X_5$. Total of 16 different outcomes uniquely corresponds to any one-qubit error (or no error).

Fault-tolerance

Big difference compared to classical "channel" setting: quantum operations are prone to errors.

A measured values may be wrong, or doing the measurement can affect the quantum state...

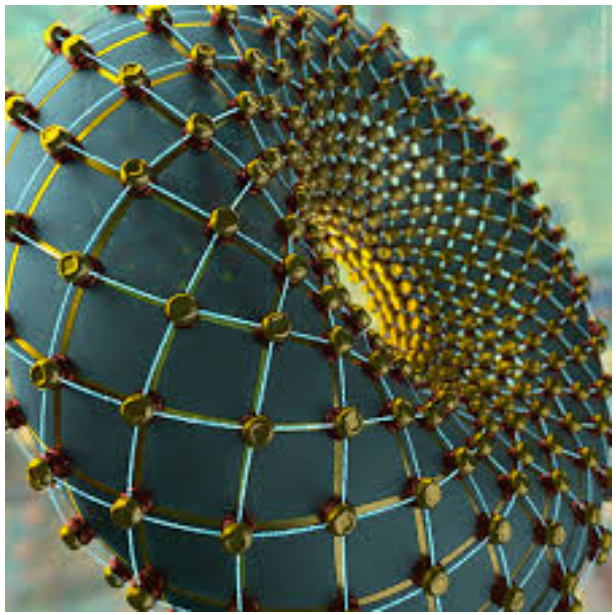
Original Shor prescription: **concatenation**.
Encode one qubit into 5, each of those into 5 (1 into 25), each of those into 5 again (1 into 125), etc.

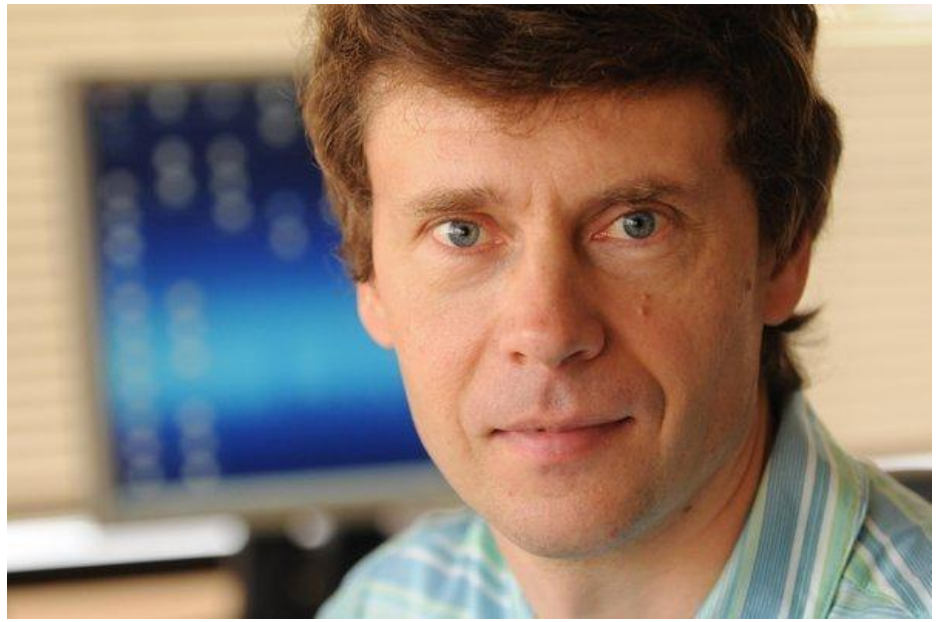
Threshold theorem: if each operation is done with fault probability below certain threshold, an arbitrary long quantum computation can be done.

- Threshold values are small ($\sim 10^{-4}$ error probability)
- This requires a lot of qubits (bad code rate)

Better codes

Alexey Kitaev (2001): topological (surface) codes





Achievable threshold much better: $\sim 10^{-2}$ error probability/gate

Yet, these codes have poor rate: big block encodes only one or two qubit

Tillich and Zemor (2009): Practical quantum codes with finite rate k/n.

Our results (with Alexey Kovalev & others)

- Demonstrated that finite-rate codes designed by Tillich and Zemor have finite threshold in fault-tolerant setting
- With optimal decoding, the threshold point correspond to a phase transition in some (rather compex) Ising model
- Estimated the position of the threshold – it is comparable to that of Kitaev's codes (within a factor of two).

Open problems

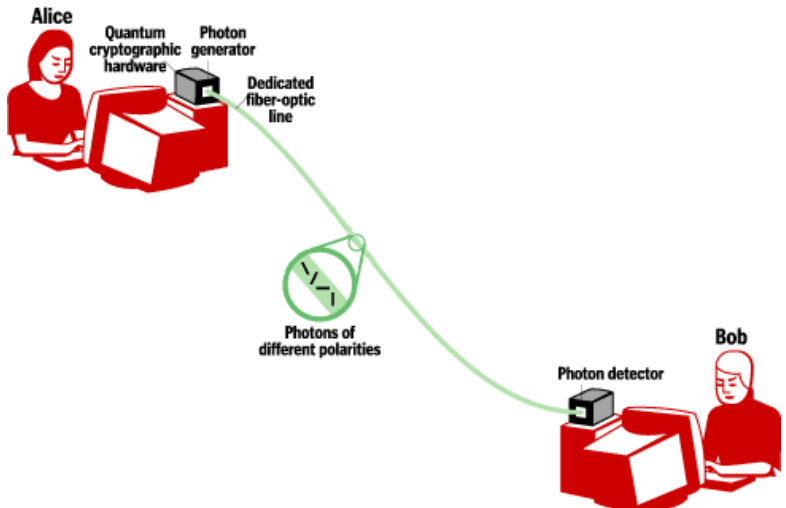
- **Decoding:** There are many known near-optimal decoders for Kitaev's codes, but none for more general finite-rate codes
- Engineering the qubit layout and actual operations
- Making it all work in a lab and scaling the number of qubits...

Commercial quantum computers

D-wave systems (commercial quantum computers used to solve hard optimization problems)

Microsoft, Google, Intel, Honeywell, Lockheed Martin, Nokia Bell Labs, . . . + a growing number of start-up companies: R&D in quantum computing

Large effort in secure quantum communication (**IBM, HP, Mitsubishi, NEC, Toshiba** . . .)

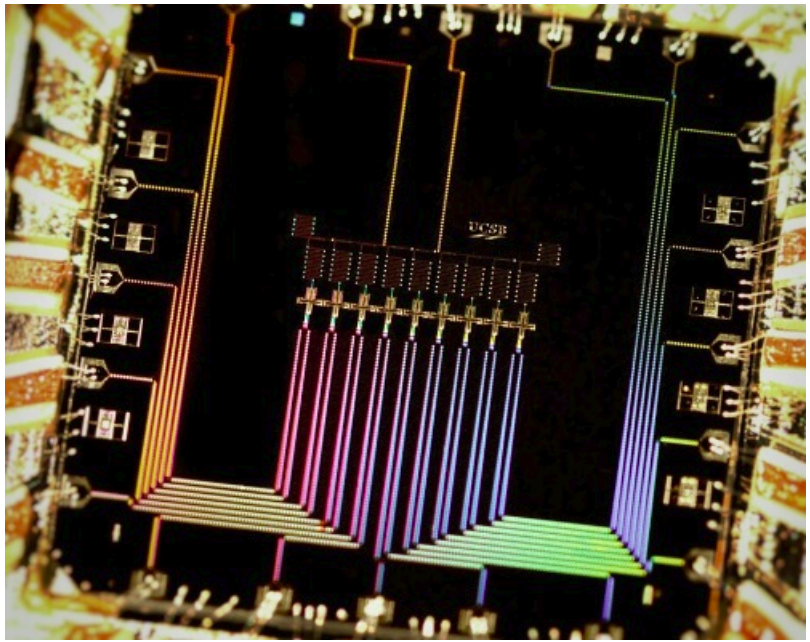


QC effort at Google

John Martinis is the world leading expert in designing superconducting qubits

Currently has a working chip integrating $n = 9$ superconducting qubits

Scaling the technology is the next step—within a year expect to have a working chip integrating around $n = 100$ qubits (10×10 square)



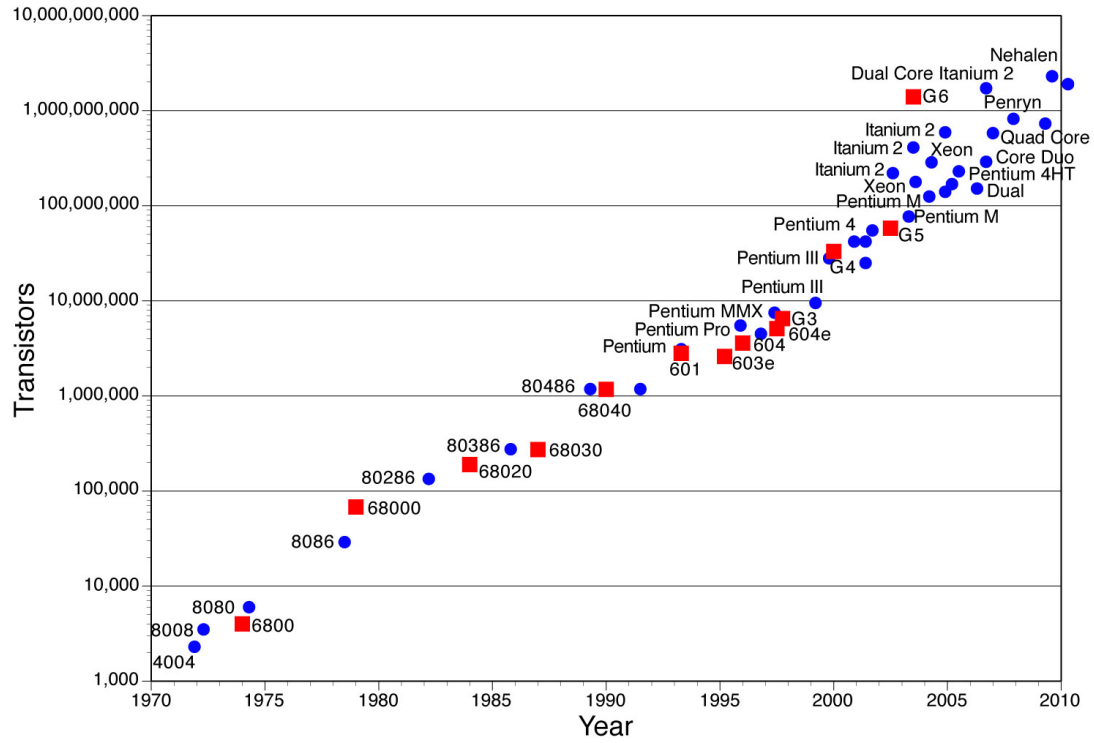
This is sufficient to demonstrate the SUPREMACY of quantum computers over quantum.

Potential applications: quantum chemistry, classically hard computer science problems, many-body quantum mechanics, etc

Intention: commercialize QC technology in 5 years

Know a good quantum mechanic?

For fifty years classical computers enjoyed exponential growth of performance (Moore's law)



This cannot continue indefinitely since feature size is getting close to the quantum tunneling limit

Many in the industry believe that quantum computers will be able to save Moore's law

It is possible that in 10 or 20 years quantum information will be conventional technology

Yet very few engineering schools offer many-body quantum mechanics as part of their curriculum…