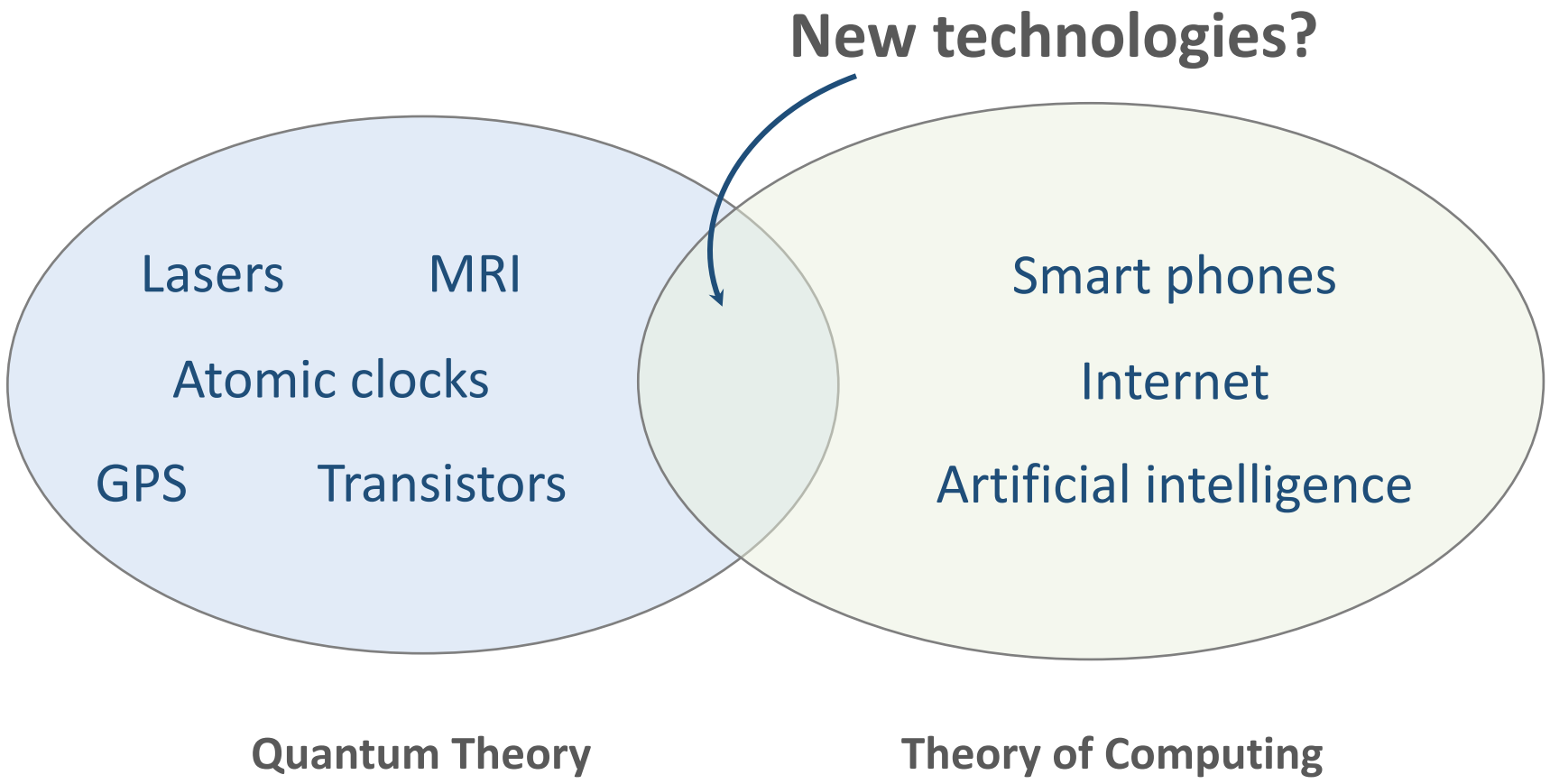
TorchQuantum Tutorial at ISCA 2023

Introduction to Quantum Computing

Yongshan Ding
Yale Quantum Institute
JUNE 2023

Quantum science meets computer science



(the quantum behavior of)

Can we control atoms to compute?

(efficiently)

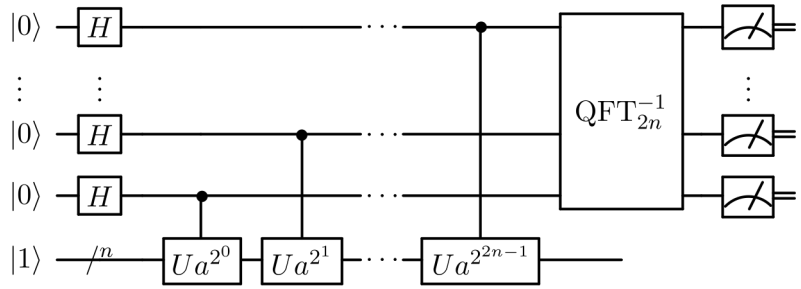
A question that would not make too much sense only a few decades ago

- Theoretical physicists: How do complex quantum systems behave at scale?
- Experimental physicists: How do we engineer a programmable Hamiltonian in the quantum systems?
- Theoretical computer scientists: What are the advantages of quantum algorithms?
- **Computer systems engineers**: How do we build scalable quantum systems that interact with classical systems?

Computational Hardness

Some problems are hard to compute, in terms of resources in space (memory) and time (steps).
But easier in a quantum world.

Prime Factorization [Shor, 1994]



1. Pick a random number $1 < a < N$.
2. Compute $K = \gcd(a, N)$, the greatest common divisor of a and N.
3. If $K \neq 1$, then K is a nontrivial factor of N, with the other factor being $\frac{N}{K}$ and we are done.
4. Otherwise, use the quantum subroutine to find the order r of a.
5. If r is odd, then go back to step 1.
6. Compute $g = \gcd(N, a^{r/2} + 1)$. If g is nontrivial, the other factor is $\frac{N}{g}$, and we're done. Otherwise, go back to step 1.

There seems to be a computational power in complex quantum systems

Source: https://en.wikipedia.org/wiki/Shor%27s_algorithm

Computational Hardness

Some problems are hard to compute, in terms of resources in space (memory) and time (steps).
But easier in a quantum world.

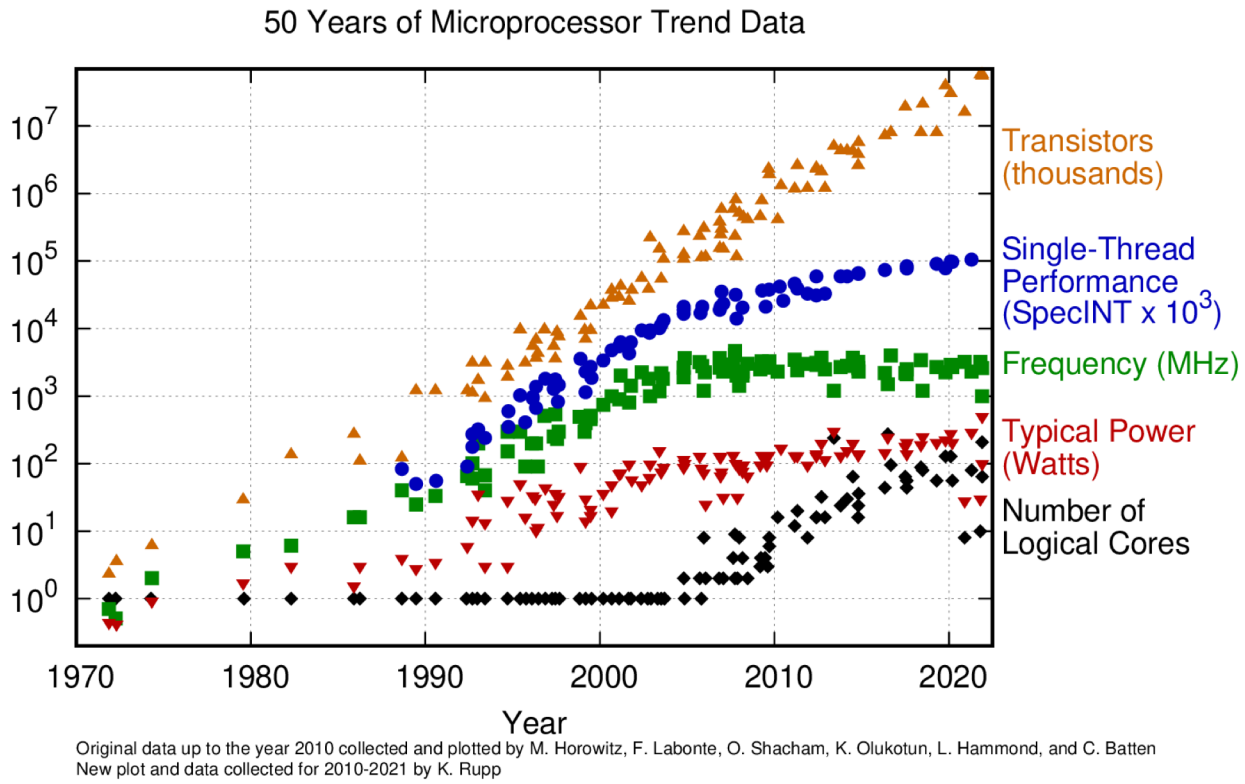
Quantum Simulation [Manin, Feynman, 1982]

> "The full description of quantum mechanics for a large system with R particles… has too many variables, it cannot be simulated with a normal computer with a number of elements proportional to R or proportional to N…
>
> And therefore, the problem is, how can we simulate the quantum mechanics? … We can give up on our rule about what the computer was, we can say:
>
> **Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws.** "

Emergence of computational problems that are inherently quantum.

Moore's law hits a wall

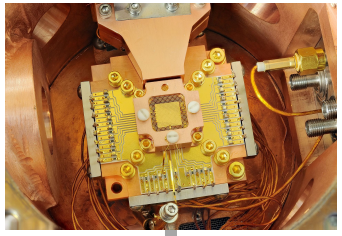
In real life, exponential growth cannot be sustained. Decades of enjoyable ride is over. [~2000]

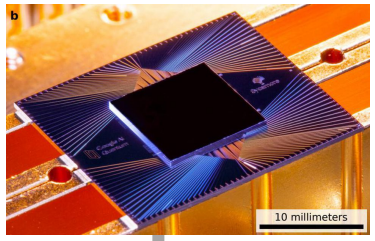


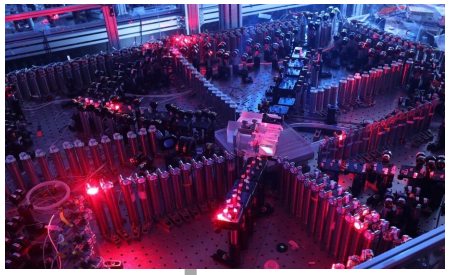
Source: https://github.com/karlrupp/microprocessor-trend-data

Emerging Quantum Computers

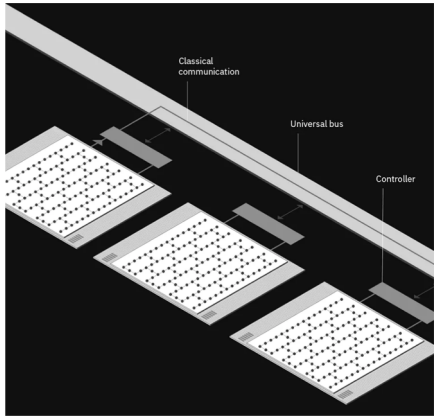
Noisy Intermediate-Scale Quantum (NISQ) Devices: 100-1000 qubits







IBM Roadmap



...

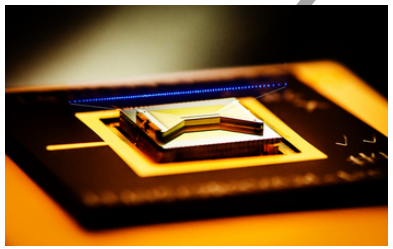
2010

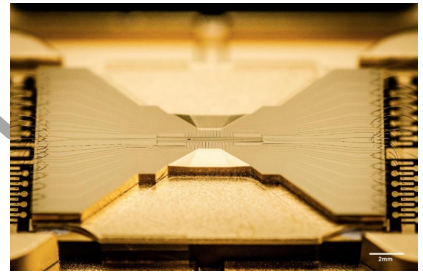
2015

2020

2025

...



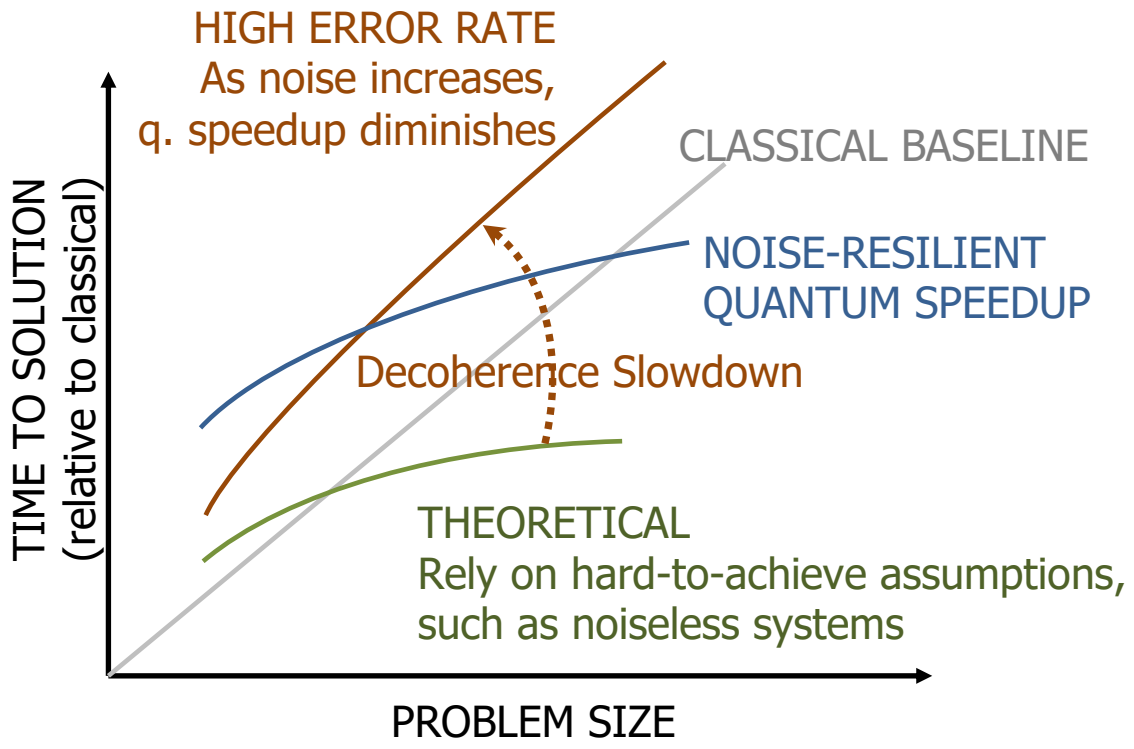


Photos from: NIST, IBM Q Graham Carlow, Google AI Quantum, Kai Hudek IonQ, E. Edwards JQI, Hansen Zhong USTC

Can we control atoms to practically achieve quantum speedup?

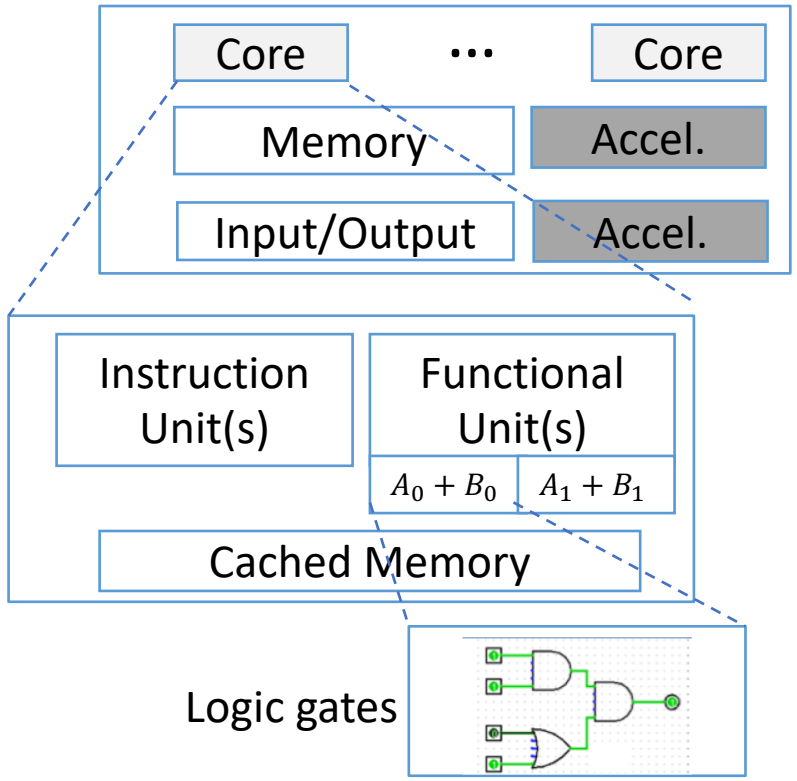
- Emergence of quantum problems
- Computational power of complex quantum systems
- End of Moore's law
- Ability to control quantum systems at the individual atom level

A convergence of many factors

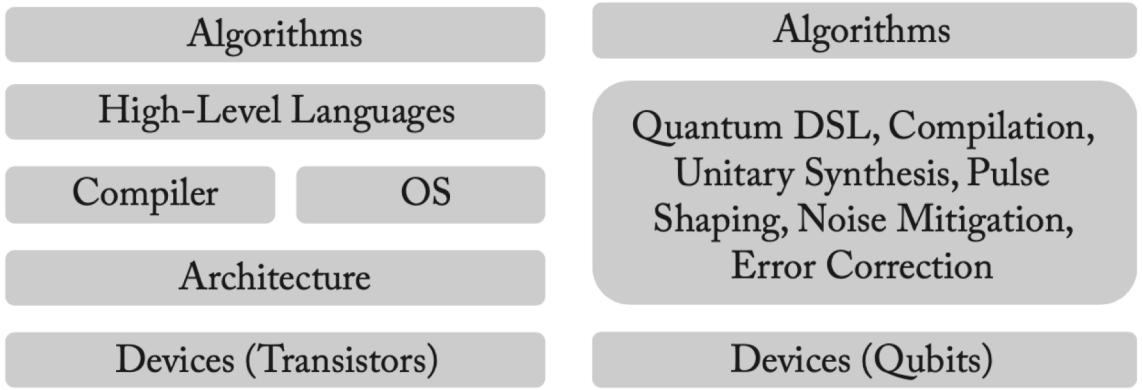


Computer Architecture
hardware-software interface

(Classical) Hardware Organization



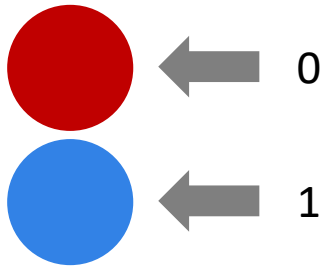
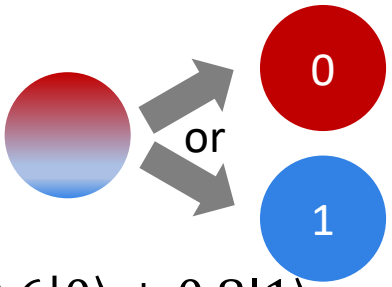
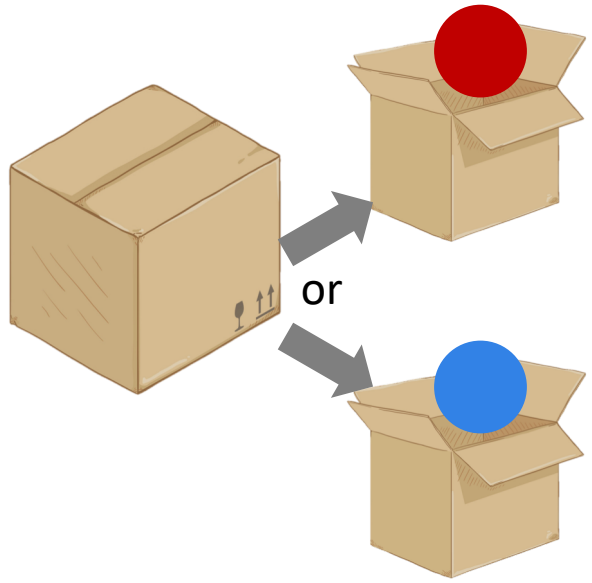
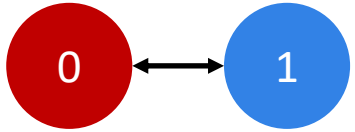
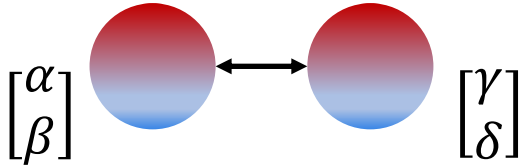
Software Stack



Classical Systems

Quantum Systems

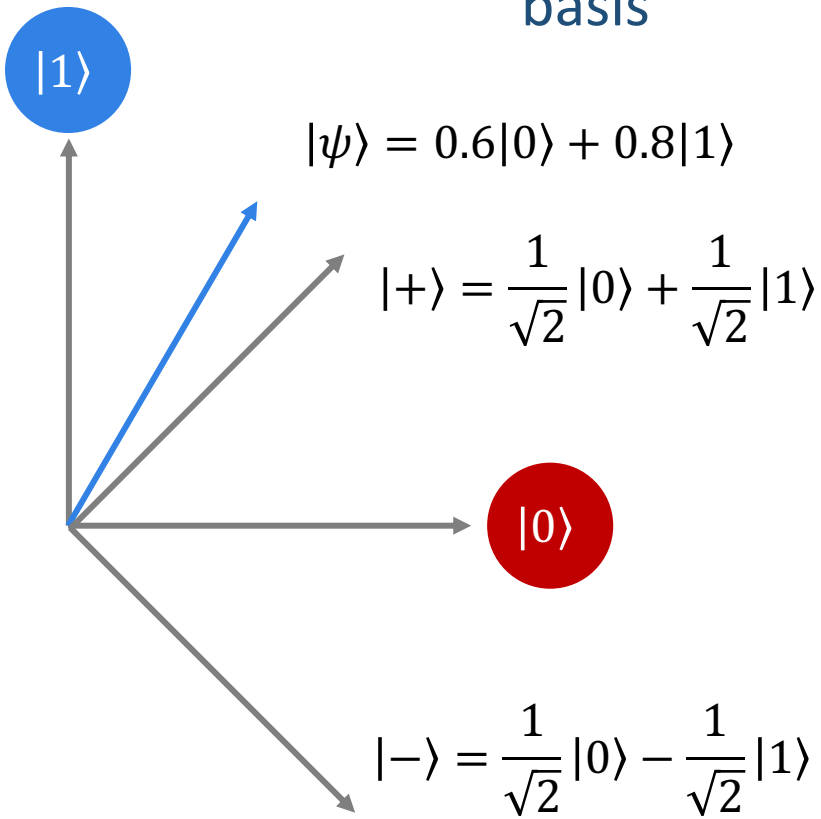
Classical v.s. Quantum Information

	Classical Bit	Quantum Bit	Random Bit
Read and Write		 $p = 0.36$ $p = 0.64$ $\|\psi\rangle \propto 0.6\|0\rangle + 0.8\|1\rangle$	
Logic		 $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ $\begin{bmatrix}\gamma\\ \delta\end{bmatrix}$	
	Boolean algebra	Linear algebra	

Quantum State

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$$

basis



$$|\psi\rangle = 0.6|0\rangle + 0.8|1\rangle$$

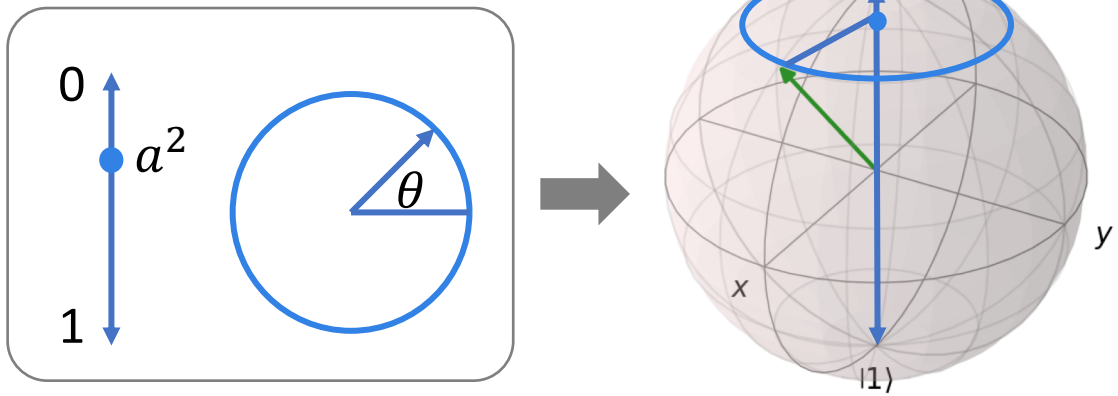
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

- Normalized: $|\alpha|^2 + |\beta|^2 = 1$
- Global phase does not matter:
  $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ not distinguishable

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \sim \begin{bmatrix}a\\ e^{i\theta}b\end{bmatrix} \sim \begin{bmatrix}a\\ e^{i\theta}\sqrt{1-a^2}\end{bmatrix}$$: two real numbers

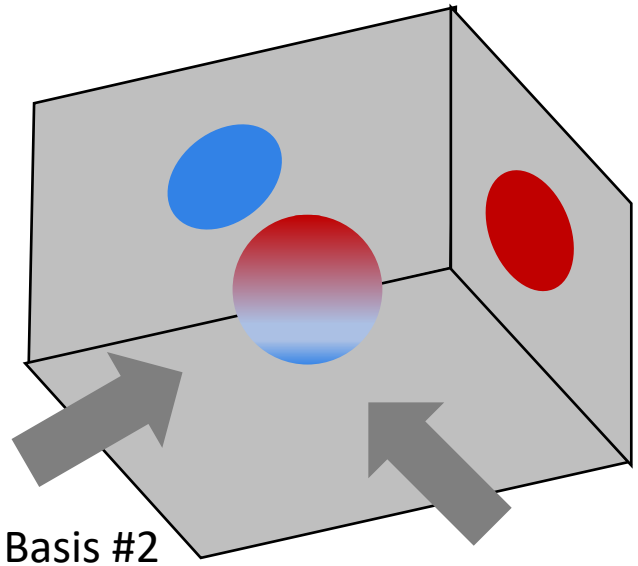
$$0 \le a \le 1, 0 \le \theta < 2\pi$$



Quantum Measurement

Projection to subspaces H of $\mathbb{C}^{2^n}$.

Orthonormal decomposition $\mathbb{C}^{2^n} = H_1 \oplus H_2 \oplus \cdots \oplus H_m$



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha'|+\rangle + \beta'|-\rangle$$

Randomness:

The measurement event is inherently random, even given full description of the qubits.

Irreversibility:

The measurement operation collapses the quantum state to the associated subspace. This process cannot be reversed.

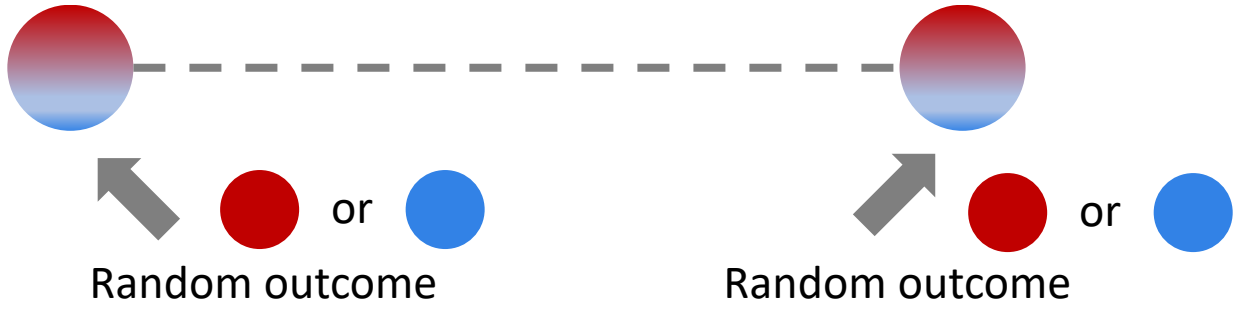
Non-commutativity:

When A and B do not commute, measuring operator A influences the outcome of the subsequent measurement B.

Entanglement – non-local information

A new notion of shared state.. $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}|+\,+\rangle + \frac{1}{\sqrt{2}}|-\,-\rangle$

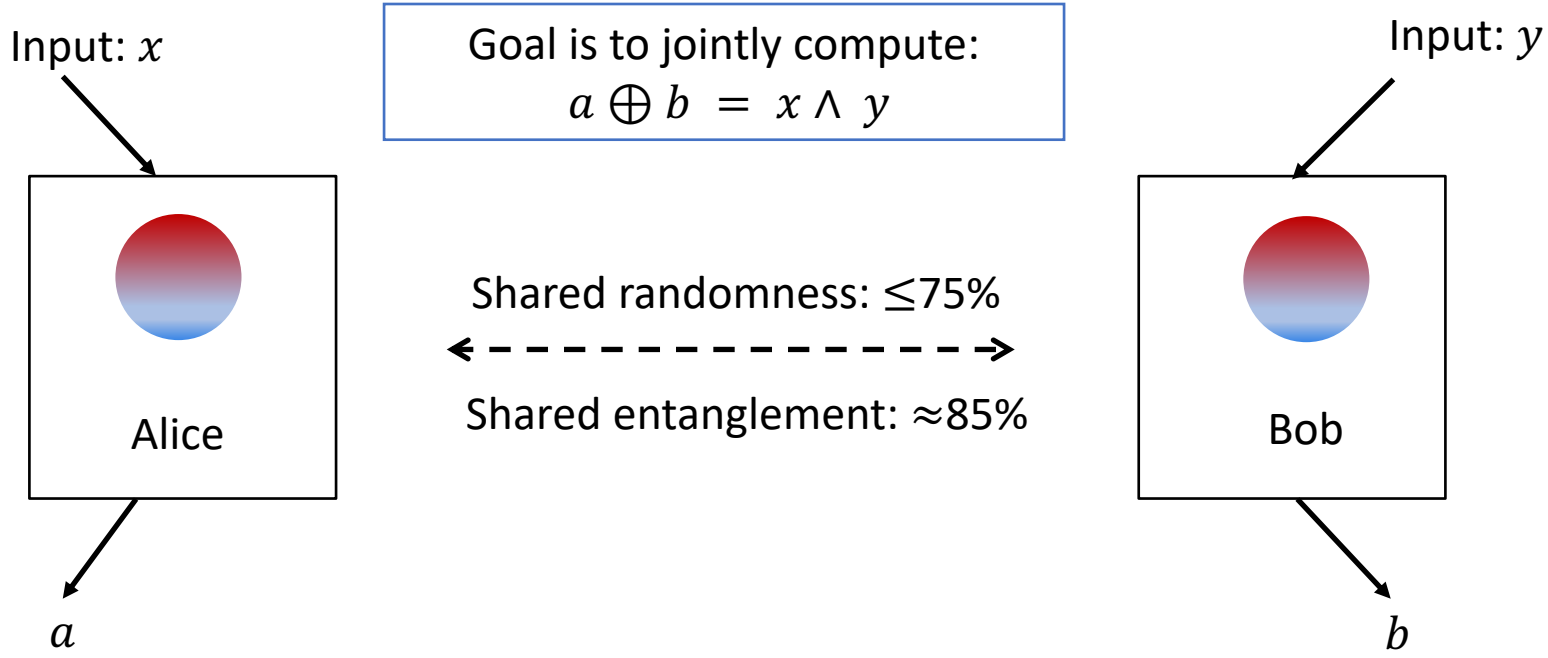
Information is not stored in any subsystems, but as correlations in the entire system.



But if measure in an agreed basis, their outcome will always be the same.

Entanglement is stronger than classical correlation

Clauser–Horne–Shimony–Holt (CHSH) Game



Theory: J. Bell (1964)
Experiment: A. Aspect et al., early ’80s

Entanglement can be used as a resource.
More example: generating certifiable randomness.

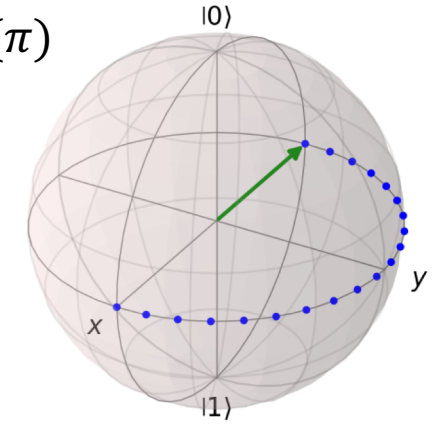
Unitary Transformation

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \longleftrightarrow \begin{bmatrix}\gamma\\ \delta\end{bmatrix}$$

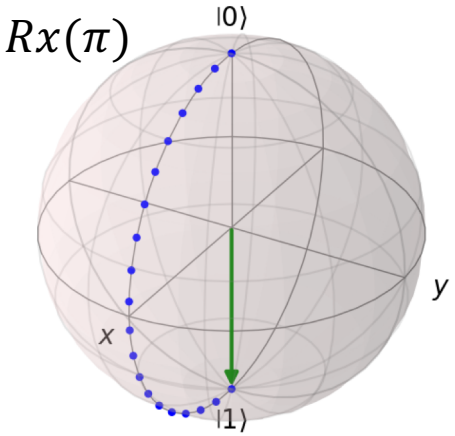
Linear algebra: unitary matrices $U^{-1} = U^{\dagger}$ (Prove it!)

Computational universality:
A subset of operations can implement arbitrary transformations.
Claim: Any single-qubit transformation can be implemented by Rx and Rz gates.

$Rz(\pi)$



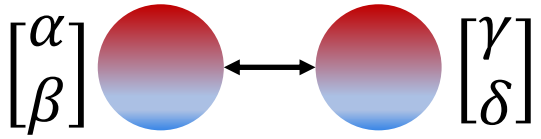
$Rx(\pi)$



Exercise:

Implement an arbitrary angle, arbitrary axis rotation by three Rx and Rz rotations.

Circuit Synthesis and Quantum Compiling

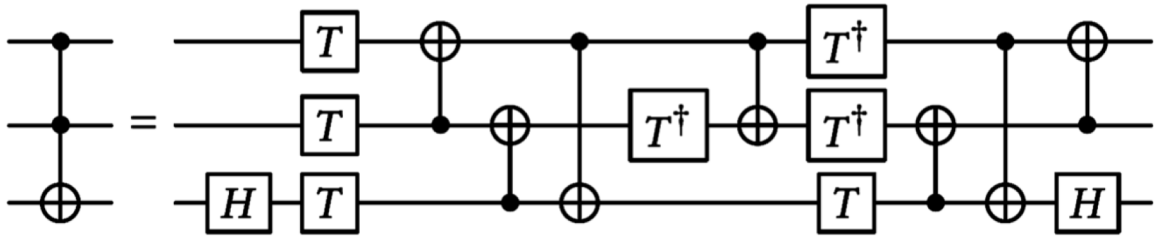


Linear algebra: unitary matrices $U^{-1} = U^{\dagger}$ (Prove it!)

In fact, **Hadamard and $Rz(\pi/4)$ gates** can implement any single-qubit transformations.
Two-qubit gates can implement arbitrary transformation on any number of qubits.

In practice, having a **redundantly universal** instruction set can be helpful: more efficient circuit.

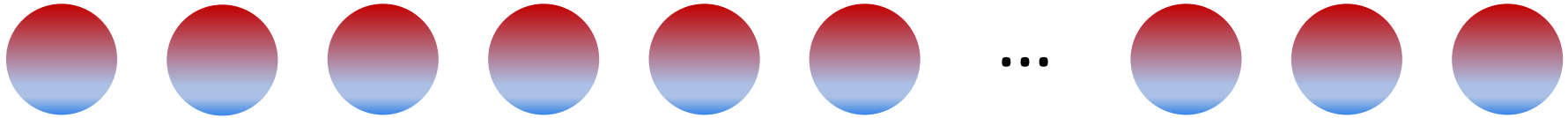
A **quantum circuit/program** specifies a sequence of quantum gates and measurements.



Source: Amy et al, https://arxiv.org/abs/1206.0758

Superposition and Interference

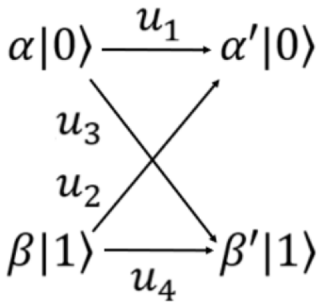
The massive quantum parallelism



$$\mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$$

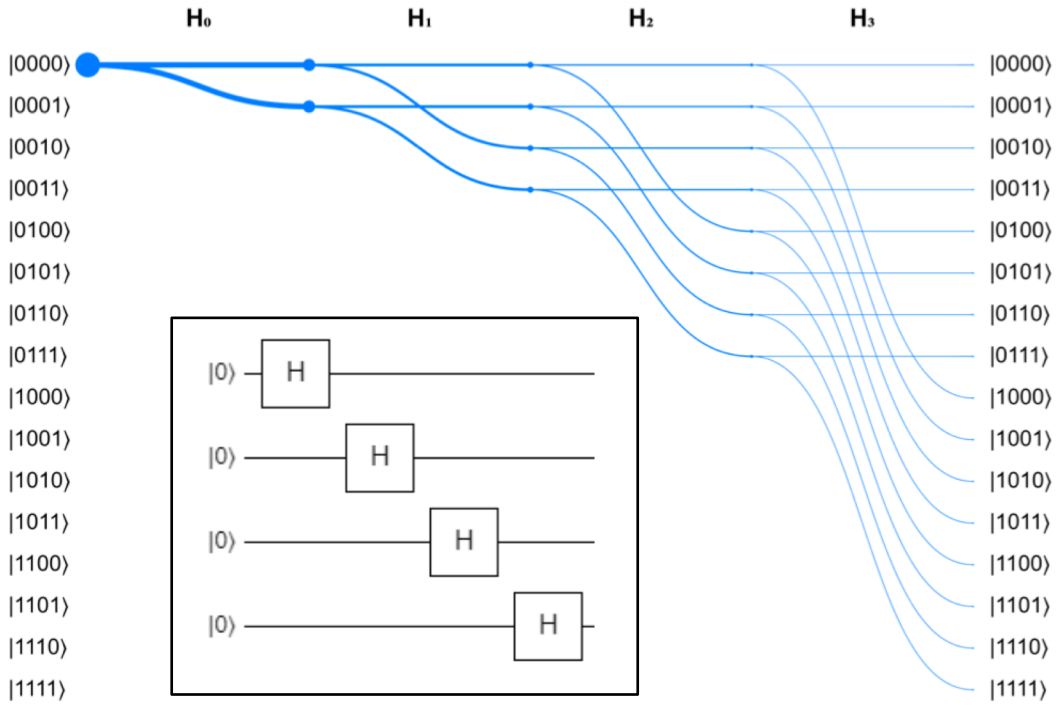
Feynman paths:
describe the transitions between superposition of states.

$$\begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$$



$$\alpha' = u_1\alpha + u_2\beta$$

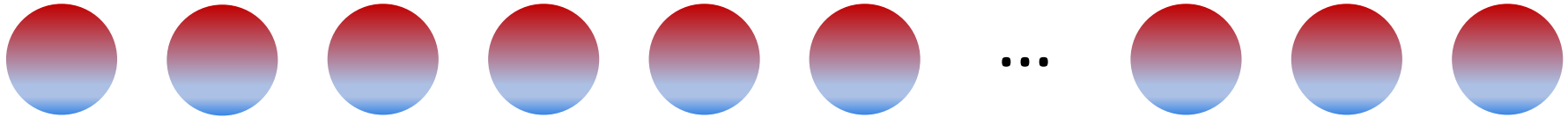
$$\beta' = u_3\alpha + u_4\beta$$

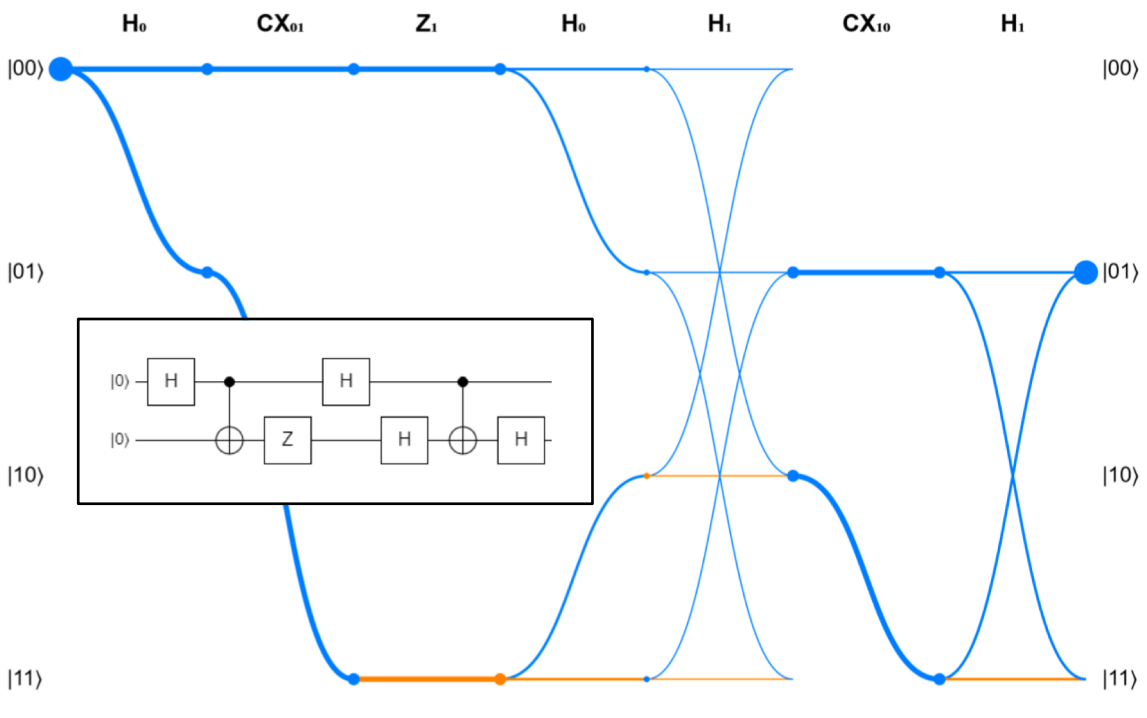


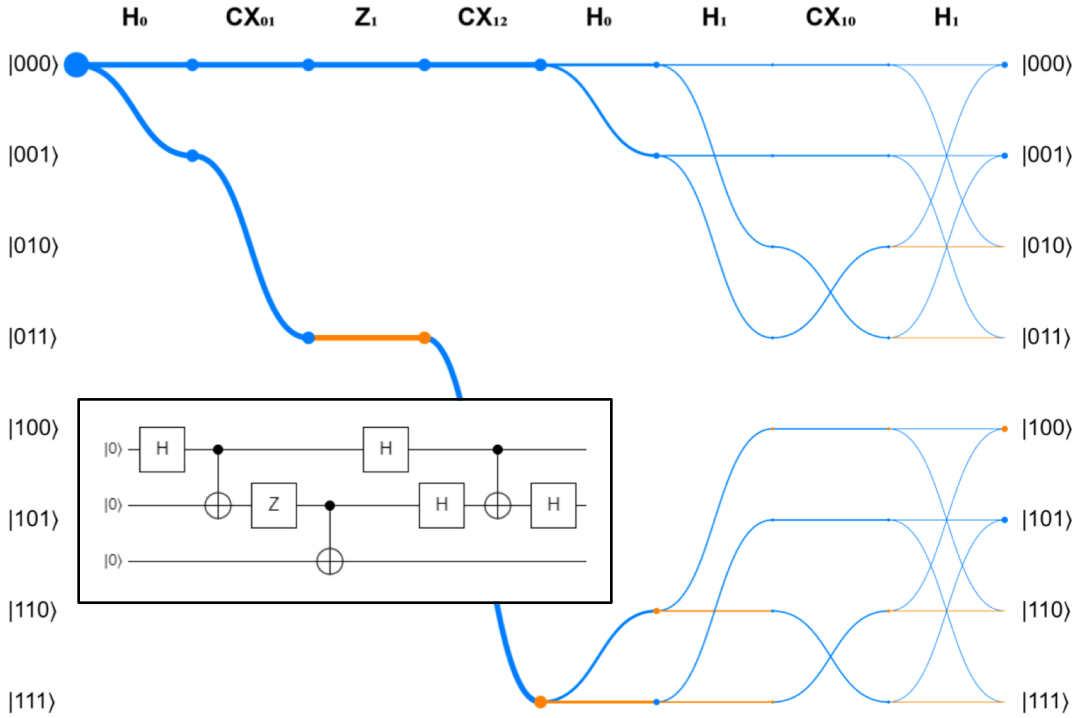
https://github.com/Yale-QCS/feynman-path-visualizer

Superposition and Interference

The massive quantum parallelism



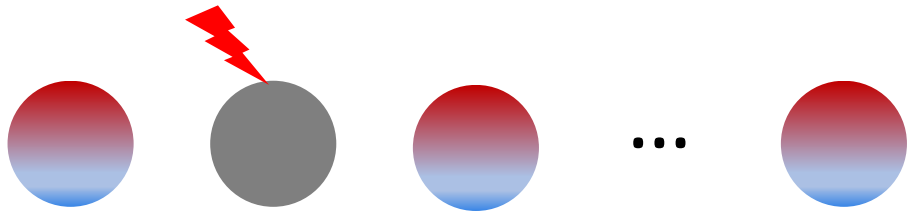




Feynman-path visualization: https://github.com/Yale-QCS/feynman-path-visualizer

Quantum errors

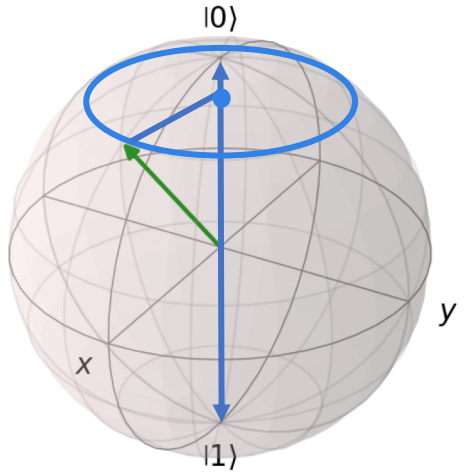
Decoherence: loss of information to the environment (e.g., bit-type errors, phase-type errors).



$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \sim \begin{bmatrix}a\\ e^{i\theta}b\end{bmatrix} \sim \begin{bmatrix}a\\ e^{i\theta}\sqrt{1-a^2}\end{bmatrix}$$: two real numbers

$$0 \le a \le 1, 0 \le \theta < 2\pi$$

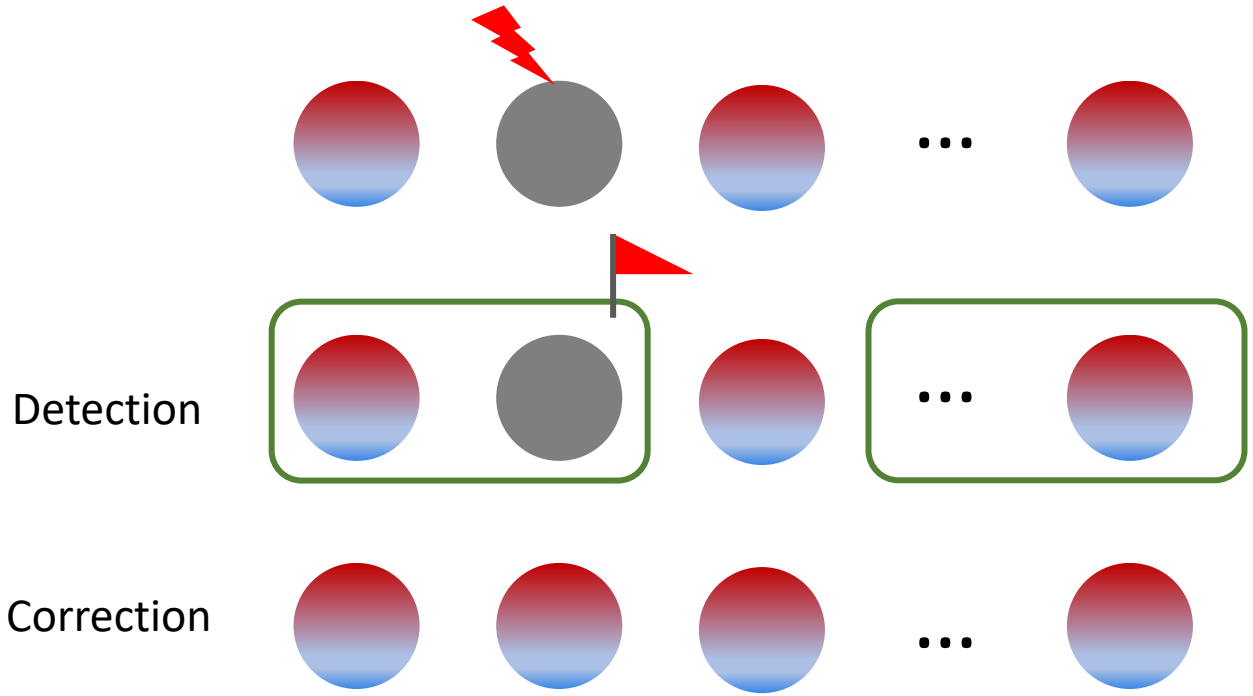
- Bit-type errors: random disturbance to a.
  - Amplitude damping: spontaneous decay from $|0\rangle$ to $|1\rangle$ at a random time.
- Phase-type errors: random disturbance to θ.
  - Dephasing: spontaneous loss of phase information



Quantum errors and how to catch them

Protecting information against decoherence:

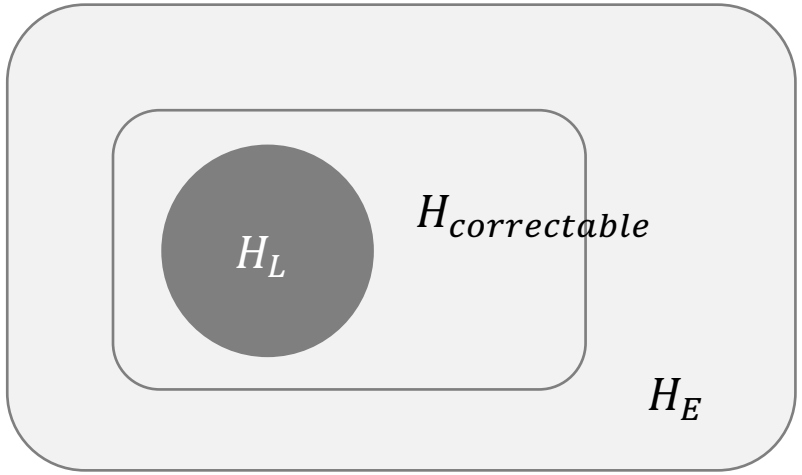
- Redundancy: encode information non-locally.
- Error detection/correction: frequent checks to restore information



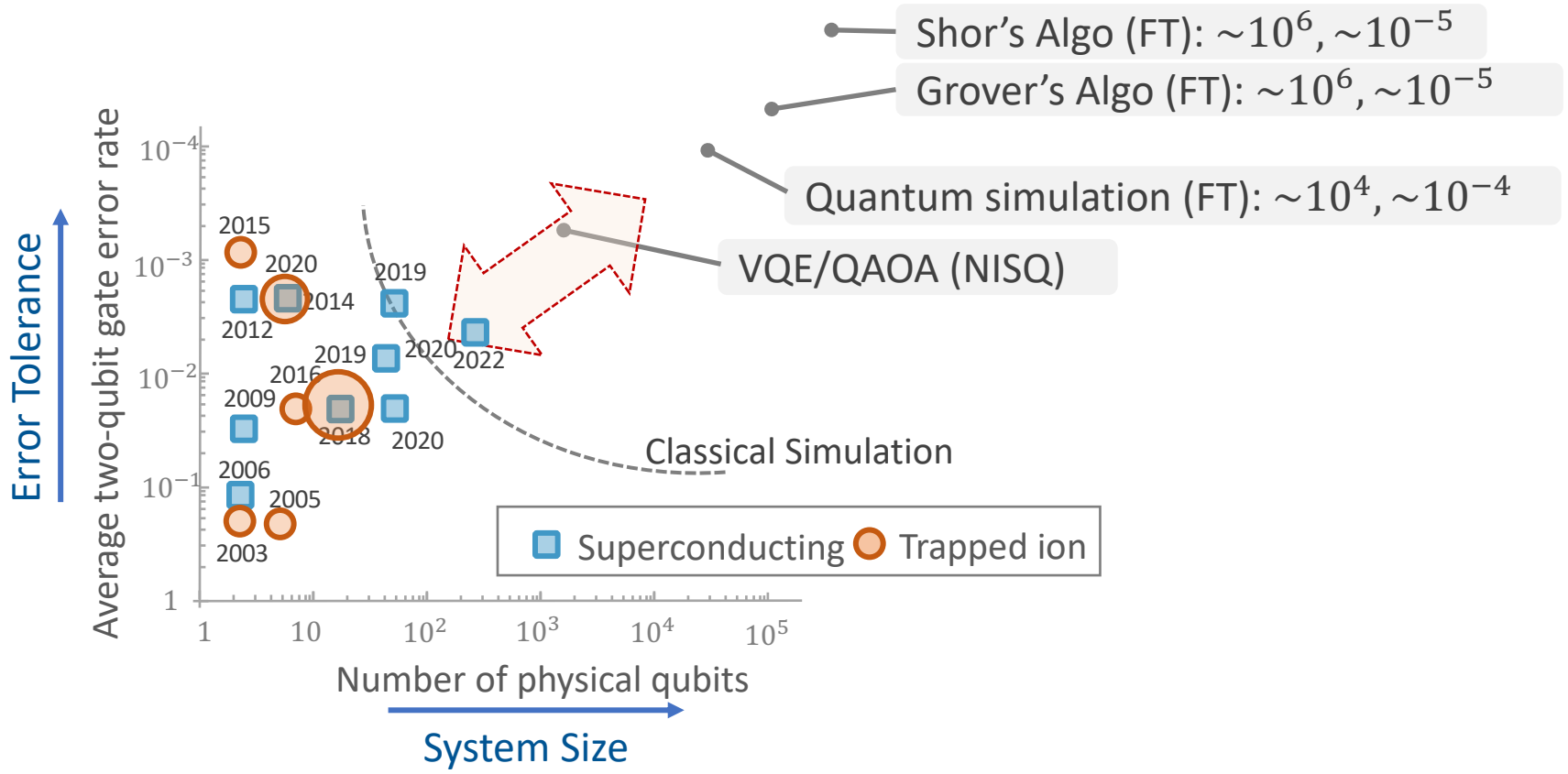
$$\mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$$

$$= H_1 \oplus H_2 \oplus H_3 \oplus H_4 \oplus \cdots \oplus H_m$$

Logical subspace H_L | Error subspace H_E



From Algorithms to Hardware

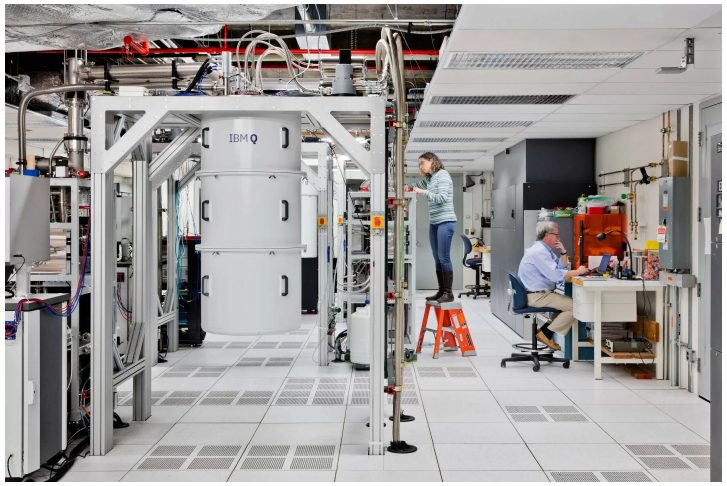


*Size of data point indicates connectivity; larger means denser connectivity.

Data: Ding & Chong (2020)

From Vacuum Tubes to Modern Computers

IBM System/360 at NASA (1960s)



IBM Q (2019)

How do we build practical quantum computers sooner?
The answer has to do with leveraging digital computers and experience of building digital computers.

Photo from: en.wikipedia.org, www.techspot.com

Emerging Applications

Computational tasks that are considered potentially easy on quantum computers:

TCS	Numerical Analysis	Simulation	Machine Learning
• Post-Quantum Cryptography • Distributed/blind computation • Secure Communication	• Optimizations • Adiabatic algorithms • Quantum Linear Algebra	• Quantum chemistry • Learning quantum systems	• Quantum Neural Networks • Quantum Learning Theory

...