DCM26: Quantum Computing 101

Infleqtion

08 Feb 2026

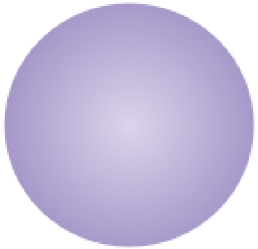
David Owusu-Antwi Peter Noell Viet Pham Ngoc Cameron Barker

Historical Context

Developments of Quantum Mechanics and a New Model of Computation

The Problem: Given an **object of interest**, along with **initial conditions** and **boundary conditions**, make a **prediction** about what will be happening in the future.

Object of Interest



Boat
Car
Box
Rock
Water droplet
Water Molecule
Hydrogen Atom**...?**

Initial & Boundary Conditions

Where is it going? ϕ

How fast is it moving? V_o

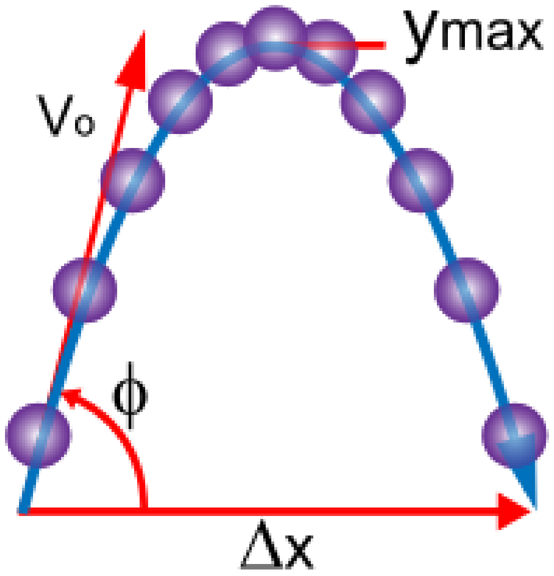
*Where *can* it go?* $y > 0$

What is ●'s future?

Where will it be at time t?

What will it be doing?
(How fast, and in what direction?)

Will the boundary conditions be different?



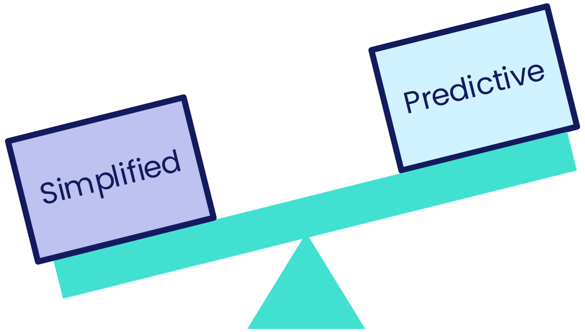
How do we solve the Problem for a given object of interest?

Historical Context

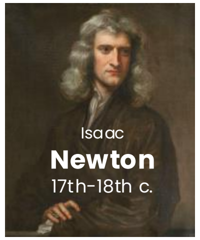
Developments of Quantum Mechanics and a New Model of Computation

We first define a **model** that predicts the behavior of a physical system (an object + its environment).

Idealised Model



Classical Physics



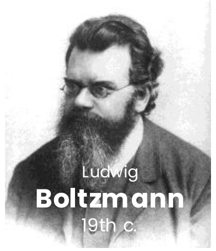
Newtonian Mechanics

$$F = ma$$

$$r(t) = r_0 + v_0 t + \frac{1}{2}at^2$$

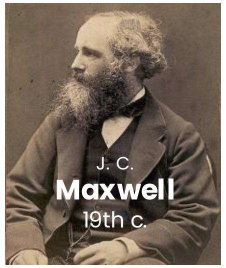
Fluid Dynamics

$$\frac{v^2}{2} + gz + \frac{p}{\rho} = C$$



Thermal Physics

$$f(E_i) = Ae^{-E_i/kT}$$



Electromagnetism

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0}$$

$$\nabla \cdot \mathbf{B} = 0$$

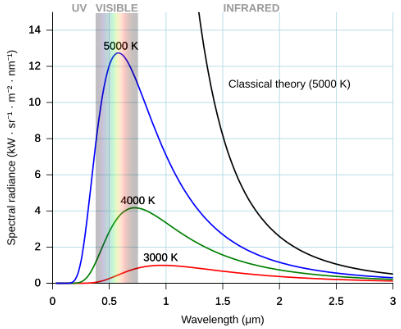
$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$

$$\nabla \times \mathbf{B} = \mu_0\left(\mathbf{J} + \varepsilon_0\frac{\partial \mathbf{E}}{\partial t}\right)$$

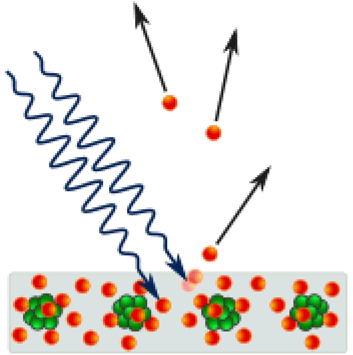
Historical Context

Developments of Quantum Mechanics and a New Model of Computation

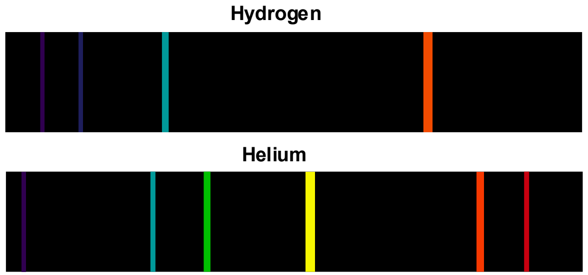
The Ultraviolet Catastrophe



The Photoelectric Effect



Atomic Spectroscopy



Object of Interest

$$\psi \sim ●$$

Initial & Boundary Conditions

Initial wavefunction ψ_0

$$\int |\psi_0|^2 = 1$$

Normalisation

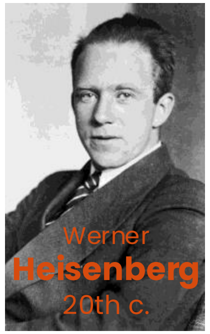
What is ●'s future?

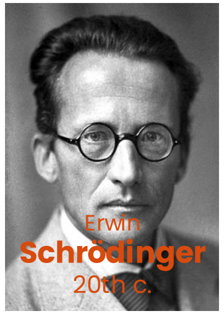
What is the wavefunction at time t*?*

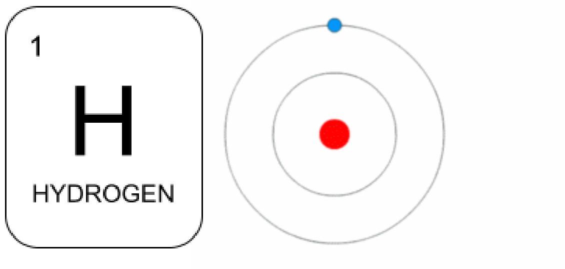
$$\Psi = \psi(t)$$

Historical Context

Developments of Quantum Mechanics and a New Model of Computation







$$i\hbar\frac{\partial}{\partial t}|\Psi\rangle = \hat{H}|\Psi\rangle$$

The **Schrödinger Equation** predicts the behavior of a **quantum** mechanical system

Object of Interest

$$\psi \sim ●$$

Initial & Boundary Conditions

Initial wavefunction ψ_0

$$\int |\psi_0|^2 = 1$$

Normalisation

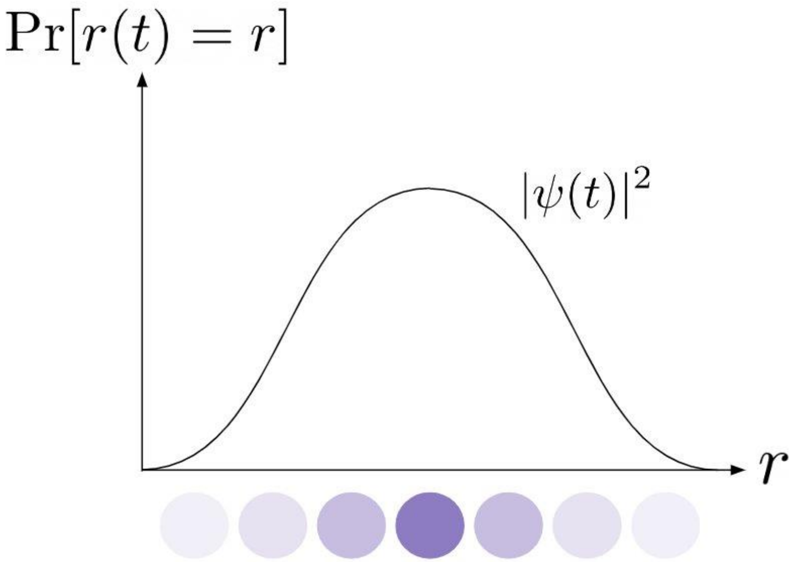
What is ●'s future?

What is the wavefunction at time t?

$$\Psi = \psi(t)$$

Born Rule

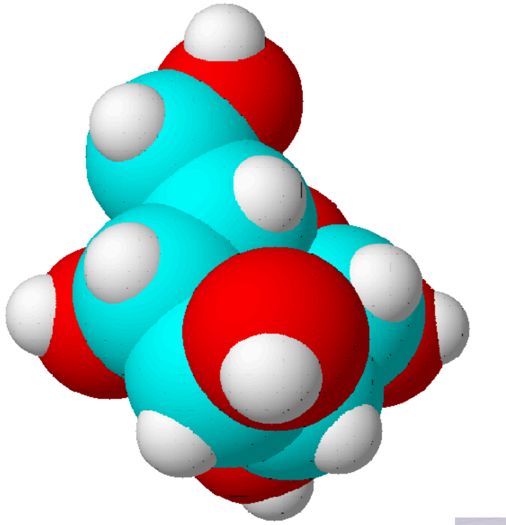
$$|\psi(t)|^2 = \Pr[r(t) = r]$$



Historical Context

Developments of Quantum Mechanics and a New Model of Computation

Problem: Predict the behavior of a quantum mechanical system, e.g., a molecule.

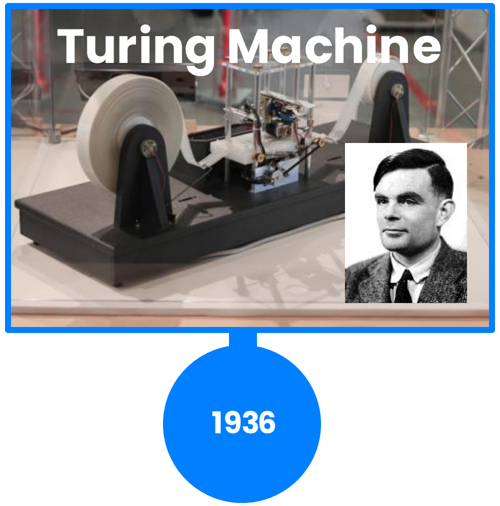


$$N \rightarrow 2^N =$$ **Storage** **(Spatial Resources)**

$$N^4 \times 2^N \times 10^3 =$$ **Time**

N = 50:

- *Storage*: ~10^{15} values
- *Time*: ~10^3steps and ~10^{22} operations/step



Exascale Computing: El Capitan
Storage: (~5PB)
Speed: > 10^{18} FLOPS

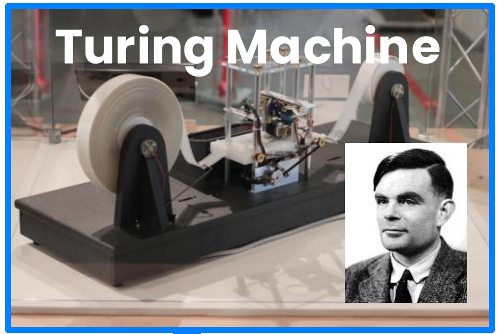
Storage: 10^{14} PB 😭

Time: 2000h ~ 3 months 😔

Inflegtion

Historical Context

Developments of Quantum Mechanics and a New Model of Computation



Turing Machine

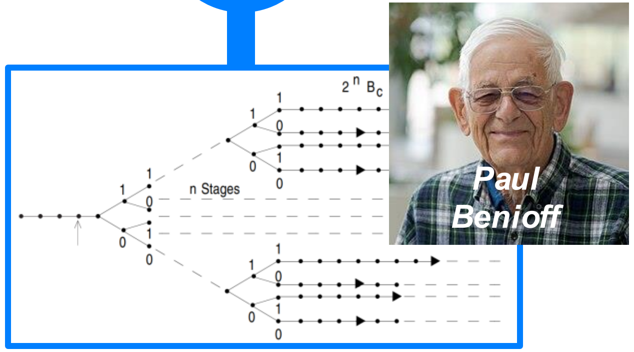
1936 . . . 1980 1981 1982 1985

КИБЕРНЕТИКА

Ю. И. МАНИН

ВЫЧИСЛИМОЕ И НЕВЫЧИСЛИМОЕ

Yuri Manin

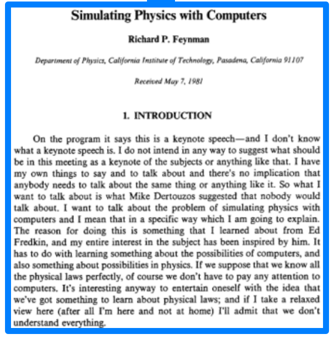


Paul Benioff

Quantum Turing Machine
[arXiv:9708054]

Richard Feynman

Physics & Computation Keynote
MIT



Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don't have to pay any attention to computers. It's interesting anyway to entertain oneself with the idea that we've got something to learn about physical laws; and if I take a relaxed view here (after all I'm here and not at home) I'll admit that we don't understand everything.

David Deutsch

Universal Quantum Computer
[arXiv:9708054]

John Preskill

Quantum Computing 40 Years Later
[arXiv:2106.10522]

Quantum Threats to Cybersecurity

What does quantum computing mean for cybersecurity?

Asymmetric Encryption

RSA

Diffie-Hellman

ECC

Integer Factoring

Discrete Logarithm

Computationally (classically) hard: Number of time steps scales **exponentially** in the input size.

Naïve Search: Try every candidate factor.

$$1 \rightarrow \lfloor\sqrt{N}\rfloor = \sqrt{N}_{\text{steps}} \qquad n = \log N \rightarrow \sqrt{N} = 2^{n/2}{}_{\text{steps}}$$

General Number Field Sieve (GNFS): A sub-exponential heuristic

1. Data gathering (sieving) to find special relations among possible candidate factors.
2. Linear algebra to "recover a congruence of squares".

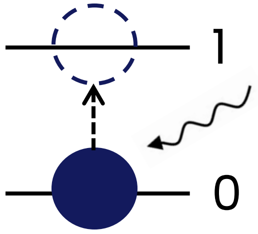
$$\exp(c \cdot \ln(N)^{1/3} \cdot (\ln \ln N)^{2/3})$$

RSA-250: 200M s ~ 7 years
RSA-2048: 1012 s ~ 31k years

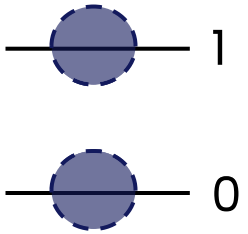
Quantum Computing Fundamentals

Building Blocks

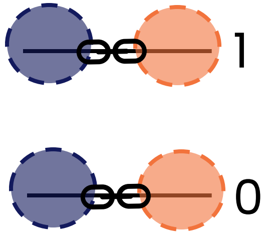
- **Quantization**: States of quantum particles are not continuous but rather exhibit discrete, or quantized, values.



- **Superposition**: Quantum particles can exist in multiple states simultaneously until they are measured.



- **Entanglement**: Measuring the state of one entangled particle instantly tells us something about the state of the other.



Fundamentals: Qubits & Superposition

- A **qubit** (quantum bit) is the quantum analogue to a classical bit; while a bit can be in two states (0 or 1), a qubit can be in a *superposition* of the *basis states* $|0\rangle$ and $|1\rangle$.

- We describe a qubit's **superposition** state by

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle$$

where the *amplitudes* c_0 and c_1 are complex numbers such that they satisfy a normalization condition:

$$|\alpha|^2 + |\beta|^2 = 1$$

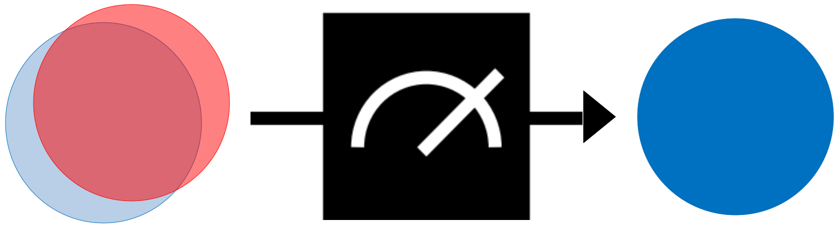
Note: the normalisation condition must hold to be a valid quantum state (i.e., satisfy the Schrödinger equation).

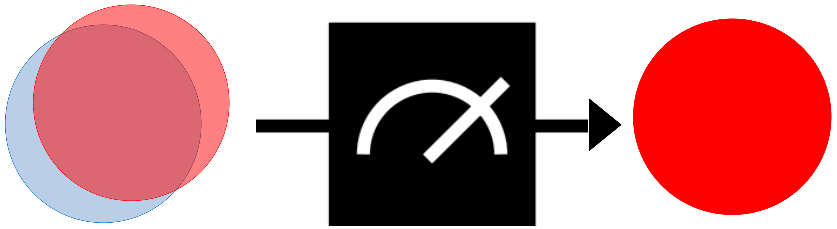
Fundamentals: Qubits & Superposition

- We cannot observe this superposition directly, and only have access to measurement outcomes that will return 0 or 1, each with some probability.

- However, the measurement outcome is correlated to the qubit's quantum state: probabilities of measuring 0 and 1 are given by the squares of the amplitudes.

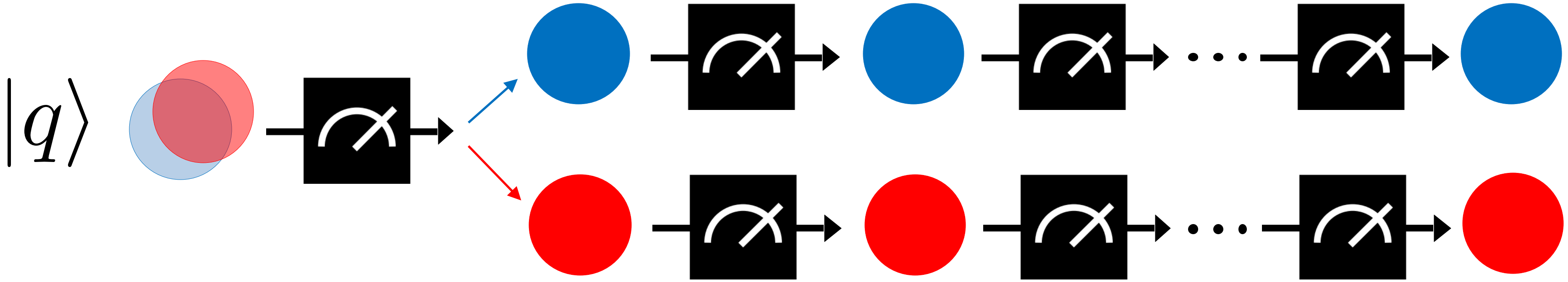
- Following measurement, a qubit's superposition state collapses to the measured state.





Fundamentals: Qubits & Superposition

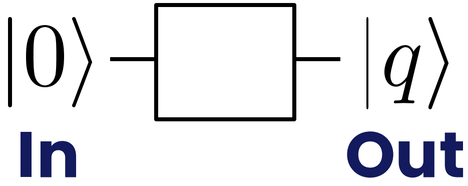
- Immediately after the initial measurement, that state collapses and all subsequent measurements will obtain the same result. E.g., if 0 is measured then every subsequent measurement will yield 0.



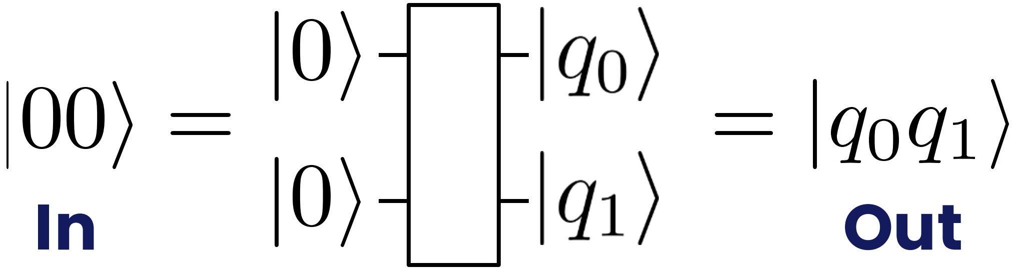
Quantum Logic Gates & Circuits

- Qubits are typically initialised in the ground state |0⟩; we generate superposition states and entanglement using **quantum logic gates**.

One-qubit Gates

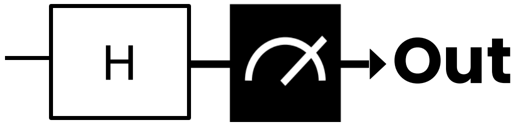


Two-qubit Gates

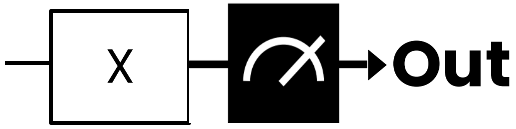


Quantum Logic Gates & Circuits

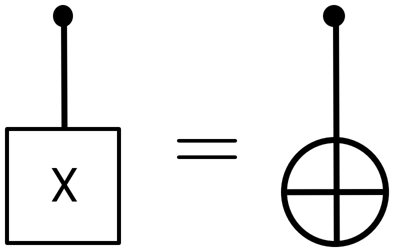
- Typical quantum logic gates:



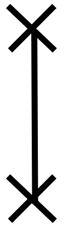
In	Out	Pr
0	0	50%
0	1	50%



In	Out
0	1
1	0



In	Out
00	00
01	01
10	11
11	10

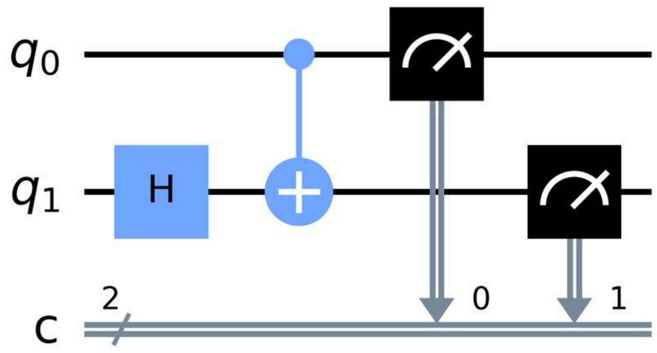


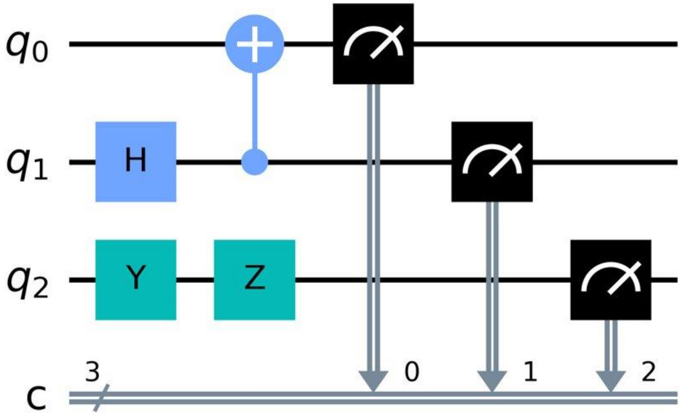
In	Out
00	00
01	10
10	01
11	11

Infleqtion

Quantum Logic Gates & Circuits

- **Quantum circuits**, are sequences of quantum logic gates acting on qubits. They are the quantum analogue to classical (Boolean) logic circuits.
  - We represent qubits with wires and gates with blocks placed over the wires corresponding to the qubits they operate on.
  - Measurements are represented with meter symbols, and a double wire represents classical bit in which a measurement result is stored.





Inflegtion

Quantum Algorithms

- **Quantum algorithms** use quantum circuits to solve a problem more efficiently than classical systems allow.
  - Variational quantum algorithms (e.g., QAOA, VQE)
  - Quantum machine learning (QML)
  - Grover's algorithm (database search)
  - Shor's algorithm (prime factorisation)
    - Deutsch-Josza algorithm
    - Bernstein-Vazirani algorithm
    - Quantum Phase Estimation (QPE)
    - Quantum Fourier Transform (QFT)

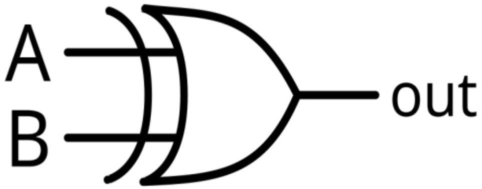
Quantum Error Correction

Why powerful quantum computers .

- Classical computing uses error correction to protect against (typically rare) events that corrupt computations or stored data.
  - An **error-correcting code** is a protocol that uses a reversible transformation of data to protect against error, typically by adding some form of redundancy.
  - E.g., CDs and QR codes use Reed-Solomon codes; 3G/4G networks use turbo code; 5G networks use low-density parity-check (LDPC) codes
- Quantum states are fragile; large quantum computers require continuous error correction during computation to prevent faulty computation.
  - Surface code, hypercube codes, quantum LDPC codes, etc.

Quantum Error Correction

- How can we detect and correct errors on quantum state **without disturbing it**?
- Consider the classical XOR gate:



A	B	Out
0	0	0
0	1	1
1	0	1
1	1	0

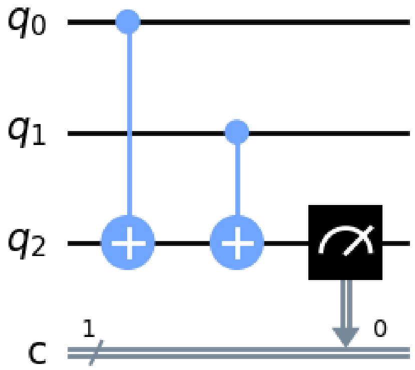
E.g., if we know that during our computation A and B should be equal, when the XOR outputs a 1 then we know an error has occurred.

That is, given the output bit, we can determine how the input bits A and B relate to each other ***without knowing the values of the bits***.

A similar principle is applied in quantum error detection/correction using *quantum stabilizer* measurements.

Quantum Error Correction

- Quantum error correction implements parity checks using **quantum stabilizers**, sets of measurements that detect parity violations using ancillary qubits.
- Quantum error-correcting codes are specified by their stabilizers, identically to specifying a (linear) classical code by its parity checks.



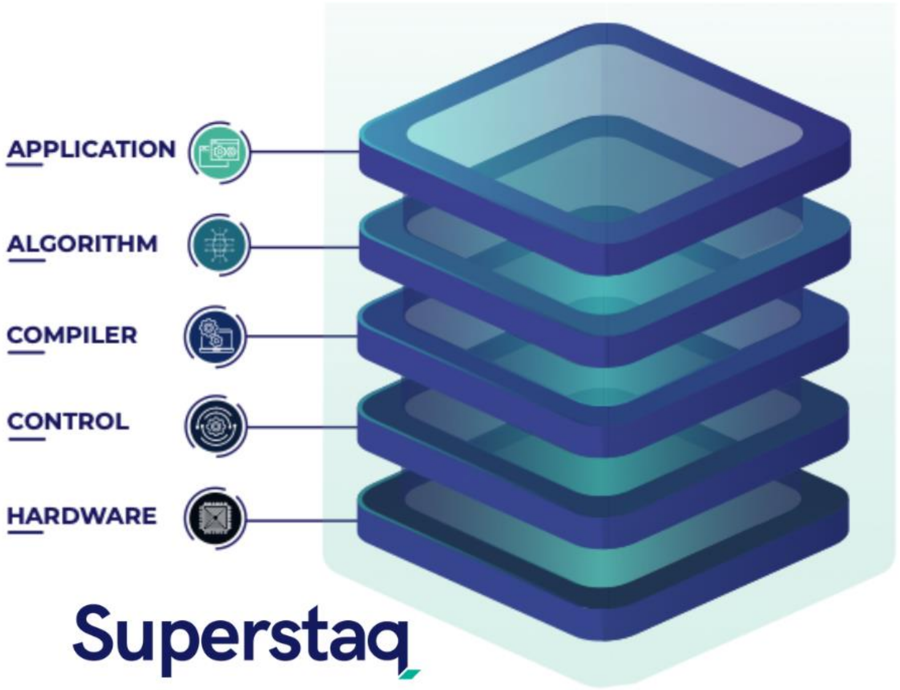
E.g., a circuit for performing a ZZ parity-check on qubits q_0 and q_1, storing the measurement result in an ancillary qubit q_2.

q_0	q_1	Out [Meas(q_2)]
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Truth table for the ZZ parity-check on input (pure-state) qubits q_0 and q_1, with measuring an ancillary qubit q_2 as output.

Quantum Software: Compilation

- For near-term quantum computing experiments, running a quantum program requires integration across the full quantum computation stack.



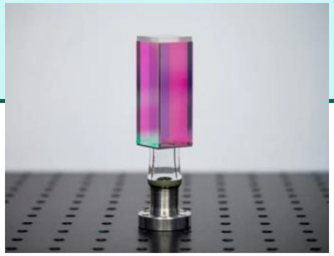
- **Quantum compilation**: Converting a user-defined program into an instruction sequence executable on a quantum computer.
    - Integration with classical workflow (Python, C/C++, etc.)
    - Quantum circuit optimization
    - Quantum software libraries (Qiskit, Cirq)
    - Low-level quantum instruction sets (QASM, analog pulse waveforms)

Quantum Hardware

Building a Quantum Computer

Cold (Neutral) Atoms

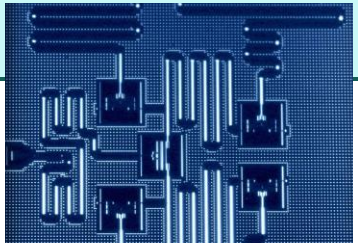
Infleqtion QuEra



Infleqtion vacuum cell.

Superconducting Transmons

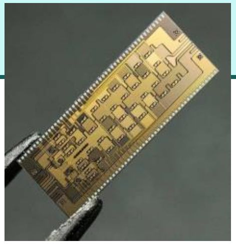
IBM Quantum Google AI Quantum



Early IBM 7-qubit chip.

Photons

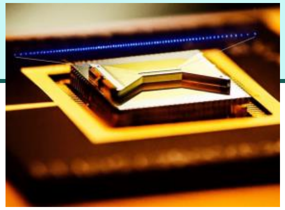
XANADU PsiQuantum



Xanadu X8 chip.

Trapped Ions

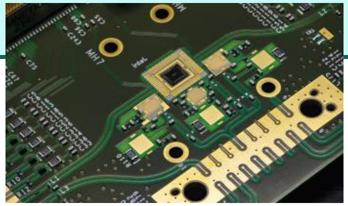
IONQ QUANTINUUM



IonQ 1-d array chip, with ion image overlay in blue.

Semiconductor Spin Systems

intel diraq



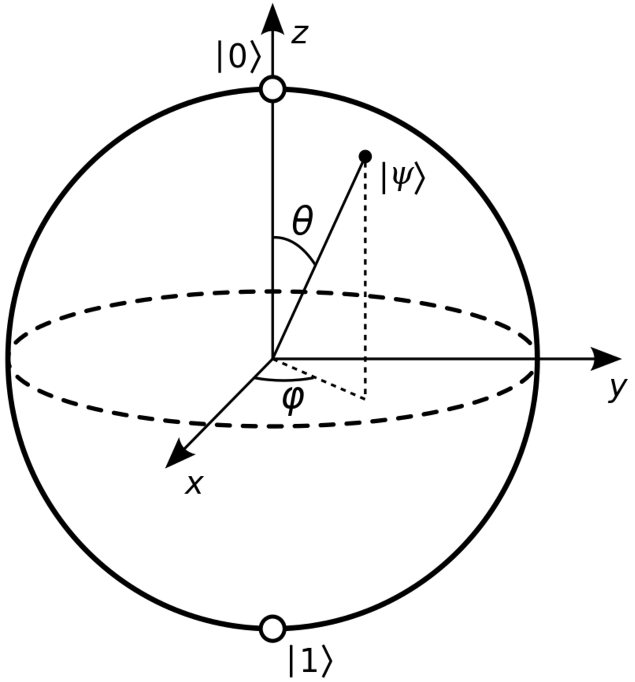
Intel Tunnel Falls 12-dot chip.

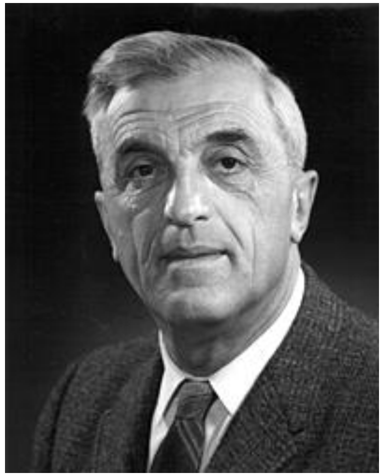
Q&A

Appendix

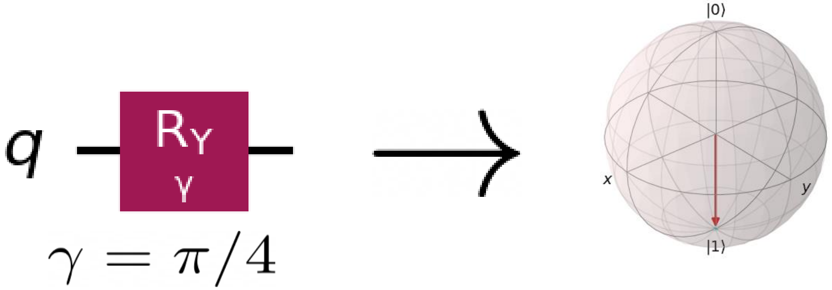
Visualizing a Quantum State

- The **Bloch Sphere**
  - A geometric representation of a quantum superposition state.





Felix Bloch



E.g., a Y-axis Rotation Gate (R_Y)

Appendix

Visualizing a Quantum State

- Deriving the **Bloch sphere**: $|c_0|^2 + |c_1|^2 = 1$ can be re-expressed using *polar coordinates*

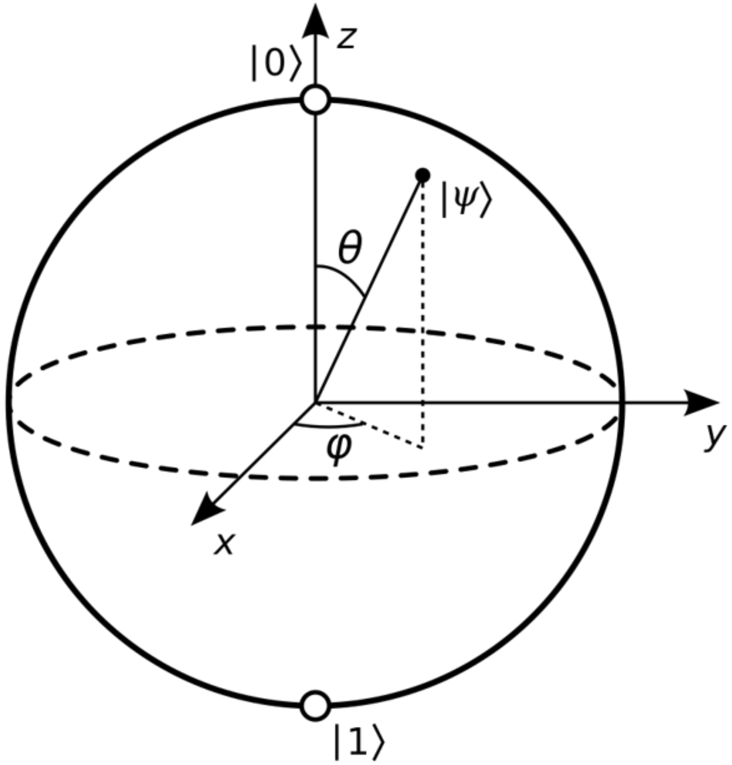
$$c_1=\sin(\theta/2)e^{i\varphi}$$

$$c_2=\cos(\theta/2)$$

where $0 \leq \theta \leq \pi$ and $0 \leq \varphi \leq 2\pi$, and so we rewrite the single-qubit state $|\psi\rangle$ as

$$|\psi\rangle=\cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\varphi}|1\rangle$$

Thus, the state $|\psi\rangle$ corresponds to a point on the surface of a sphere where the north pole is $|0\rangle$ and the south pole is $|1\rangle$ with (θ,φ) as coordinates (colatitude and longitude).



z
$|0\rangle$
$|\psi\rangle$
θ
φ
y
x
$|1\rangle$