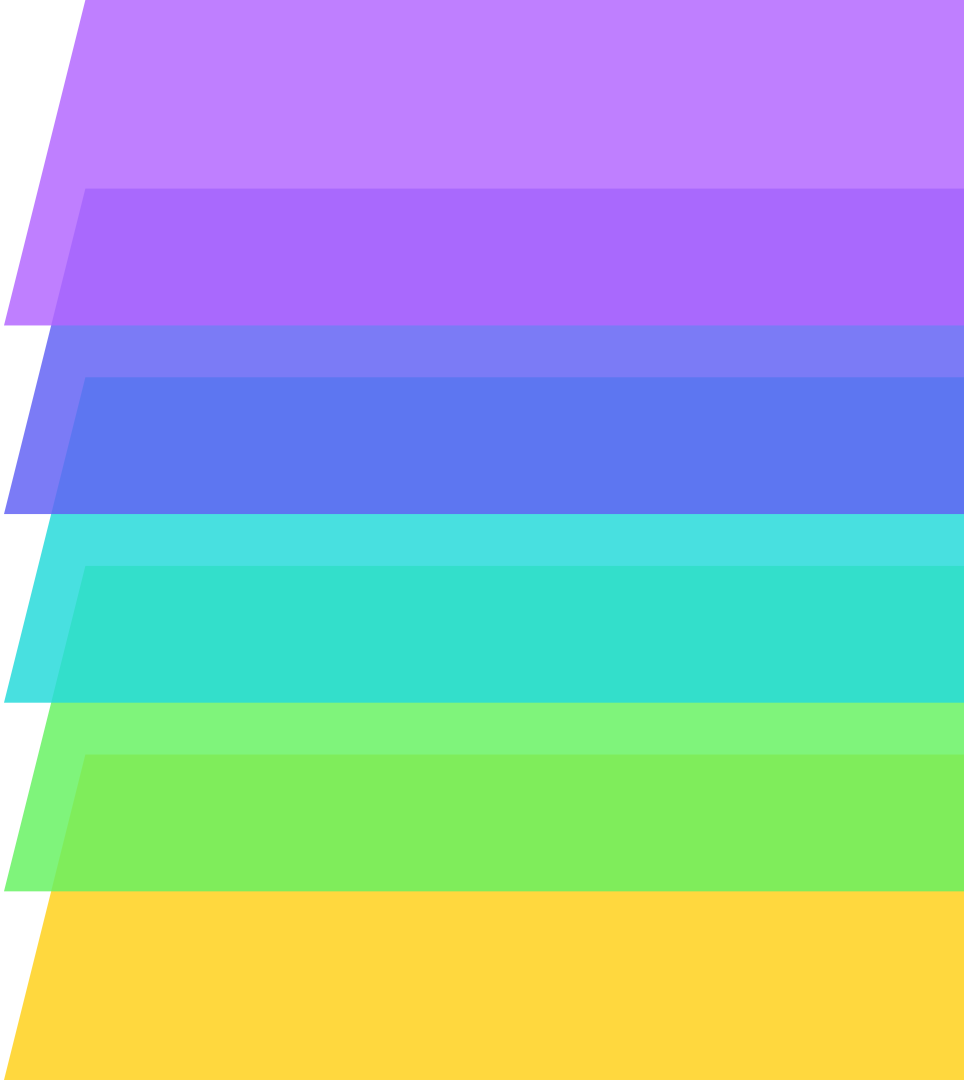
Quantum Information and Computation

Hung Nguyen



IBM: Quantum computing poses an ‘existential threat’ to data encryption

Are
The

Tim
@tim
s business
Janu eat, most
otography. We
ing insight into
ming quantum
modernize your
quantum era.

Cybersecurity Act

Share this article:

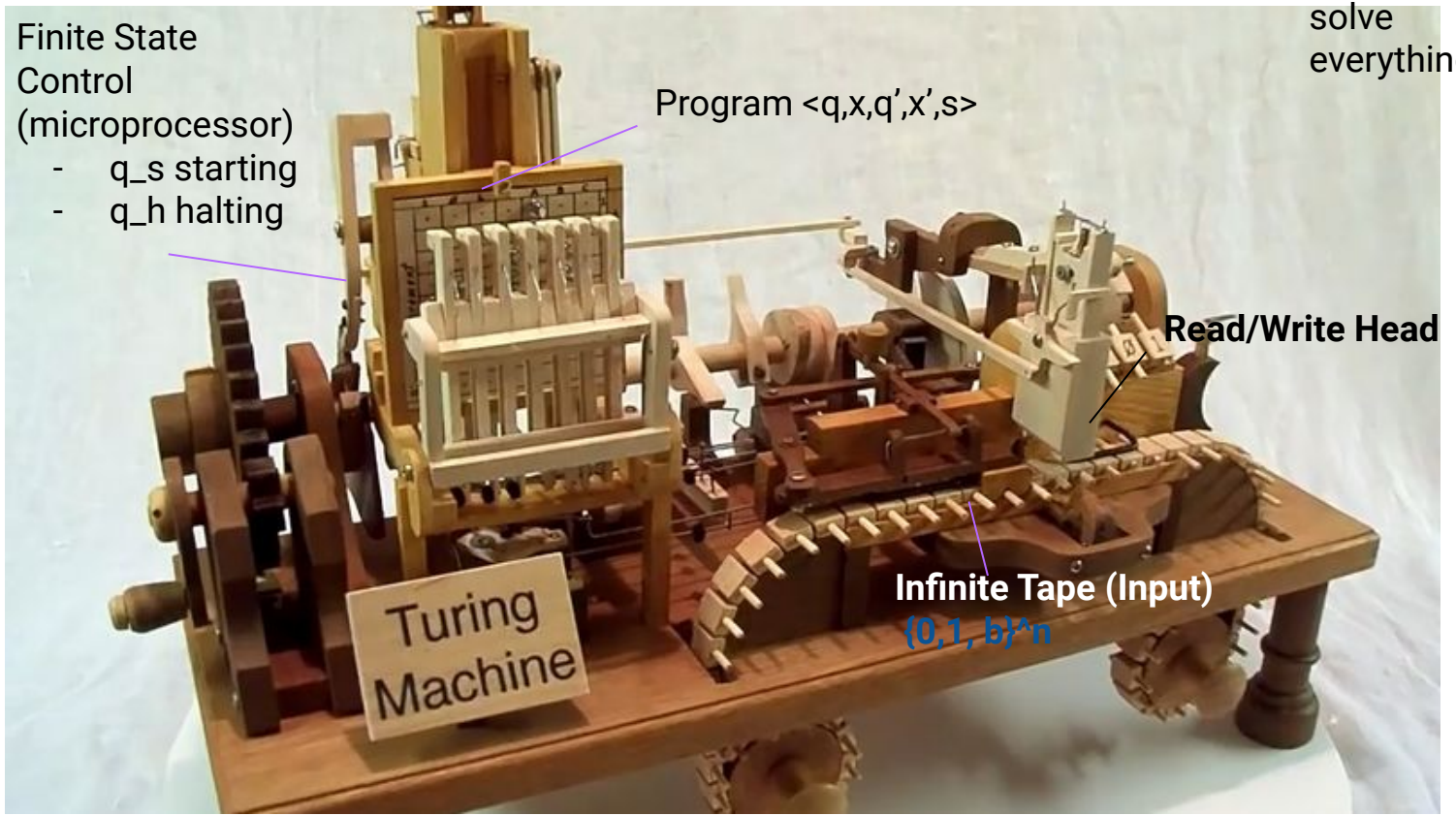
NEWS

What’s happening with quantum-safe cryptography?

Chinese researchers claim quantum technology is reaching a point where a quantum device will soon be able to crack RSA 2048 public key encryption

Model for Computation: Turing Machine

Can a Turing Machine solve everything?

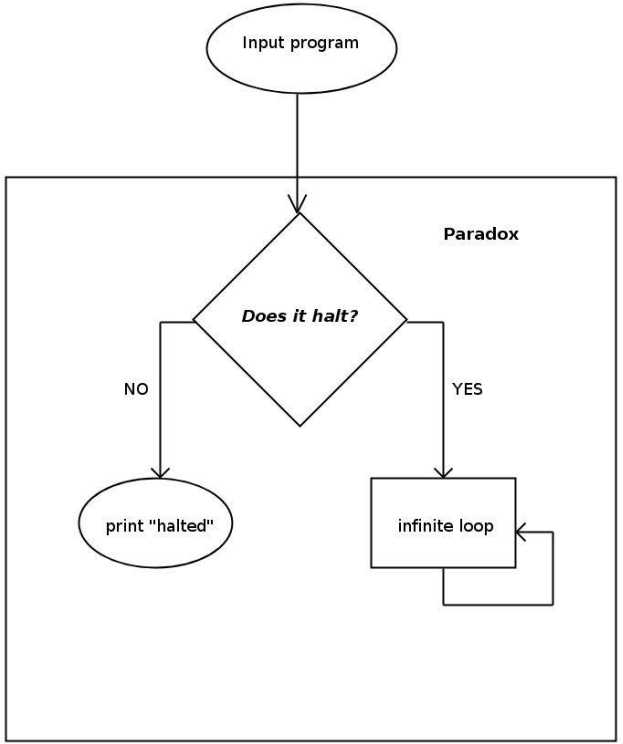


Nah!

- Church-Turing thesis states that if a problem is solvable using an algorithm, then it is also possible to solve with a Turing machine!

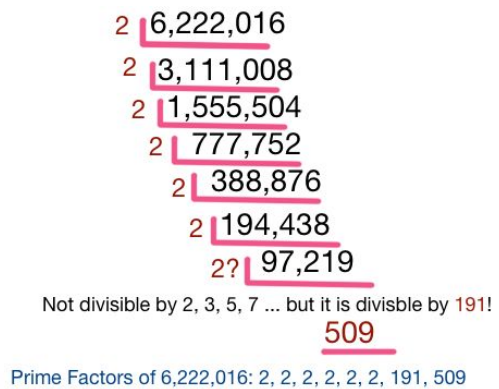
There was a guy who asked whether it is possible to solve every problem using algorithms?

- The Undecidability problem proves that it is not possible to have an algorithm for every problem.



Information Complexity Theory

P: could be solved easily on a classical computer.
NP: have solutions that could be checked on a classical computer easily (factoring-there exists no fast way to perform this, but it can easily check the answer).
P -> subset of NP.
NP-complete: very hard to solve on a classical computer.
There are other classes like PSPACE (takes a long time).
And BPP can be solved in a polynomial time in a region of error.



Introduction

What is quantum information?

It is not proven, but widely accepted to solve NP problems faster than a classical computer (factoring).
You deal with information the quantum way! (qubits)
Transferring information using quantum teleportation.
Deciphering crypto using quantum algorithms (search algorithms/factoring).
Closed systems are described with unitary operators.
Open systems are described with density operators.

What is quantum computation/computer?

You build a computer the quantum way! (qubits)
Come up with quantum algorithms to work with a quantum computer.
The most prominent algorithm is quantum error correction because quantum computers deal with a lot of noise.
Quantum computers use a circuit model instead of Turing machine model.
The two models are proven to be equivalent in solving algorithms.

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

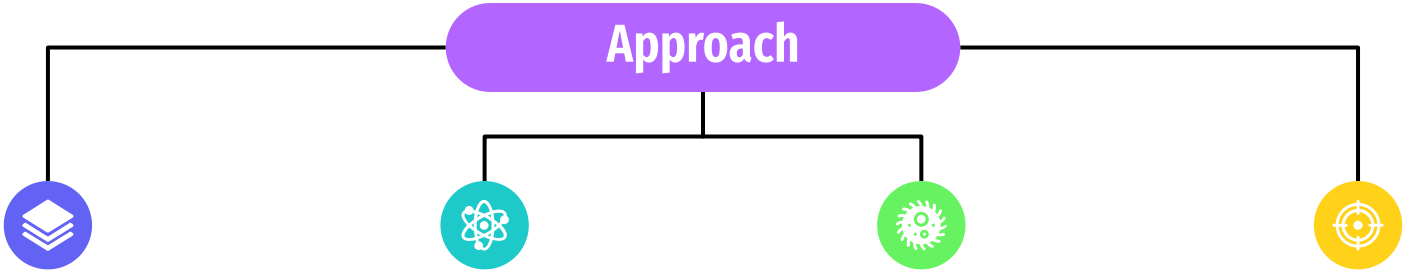
Misinformation

With some pre-knowledge equipped:

- Quantum computers do not mean faster computers. They are new tools to explore new areas of mathematical solutions.
- They are not proven to solve problems (P for example) faster than classical computers.
- They are not sci-fi computers, but they are real and achievable computers

Beautiful analogy by Cleo Abram. (Submarine to explore area like cryptography, searching, ???)

Quantum Computer Models



Trapped Ion

- Companies: Quantinuum, IonQ
- Use solid state models to trap ions.

Superconductor

- Companies: Google, IBM
- Use superconductors to build virtual qubits.

Photonics

- Companies: Xanadu Quantum Technologies, PsiQuantum
- Use photons as qubits.

NMR(:))/Others

- Many other methods exist outside of the main three.

Prerequisites for a Quantum Computer

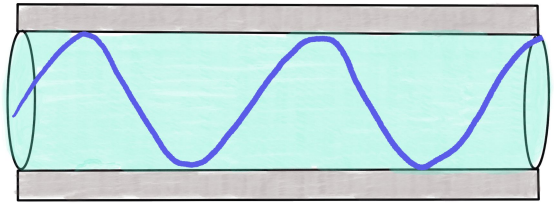
In 2000, Di Vincenzo's paper set the prerequisites needed to build a working/scalable quantum computer. The five requirements are:

1. The quantum model needs to have a well defined qubit and it is possible to scale qubits to a desired number.
2. It is possible to initialize a quantum state in a known state since quantum states are unknown unless measured.
3. Quantum states usually become classic quickly after interacting with the environment. It is required to keep the coherence as long as possible to be able to perform as many quantum gates as needed. Quantum error correction shows it is possible to reduce the noise with enough qubits.
4. Universal set of gates: similar to a classical computer, we want to be able to define gates that are universal like NAND and NOR. These gates could help us perform any task like a classical computer.
5. Even though we want the system to be as separate from the environment as possible, we still want to control the system when needed. Therefore, a good quantum computer model should have a way to measure the final outcome.

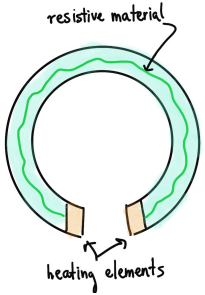
Photonic Quantum Computer

Use photons as qubits based on its polarization.
Photons do not interact with one another, but we want them to interact so how can we do that?
We can do this by using linear material as a mediator. Together, they will provide gaussian states. We could use photodetector to find out the state of output photons.
The two observables are position and momentum (note that they are not commute). And, we need infinite of basis to build this Gaussian state. (Gaussian state of in vacuum)

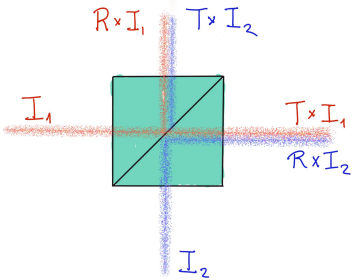
Tools



Fiber optics to transmit photons



Create a phase shift difference



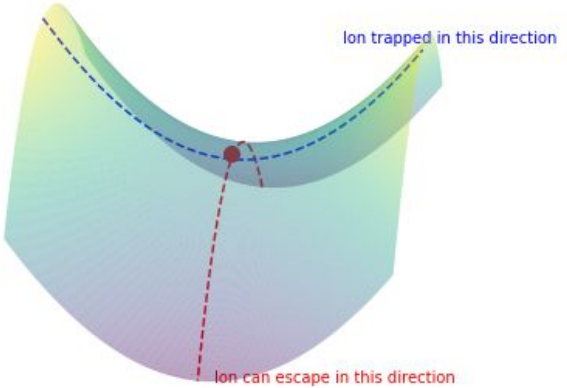
Split photons to create entangled states

Disadvantages/Advantages

Advantages: devices to work with photons are well studied and built. Photons could be scalable faster than other approaches.

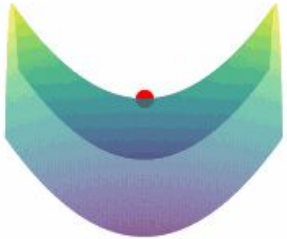
Disadvantages: The non-interactive of photons are both a bless and a curse because we want photons to interact with each other, but not the environment.
The preparation of state is hard because the gaussian state appears to be random.

Ion Trapped Quantum Computer



We can use electric field to trap ions within a potential. However, static electric field does not create a “bowl” configuration to trap the ion. One way to handle this is to alternate the field. Therefore, the chance for electron to escape is much lower (though not never).

These ions act like huge qubits

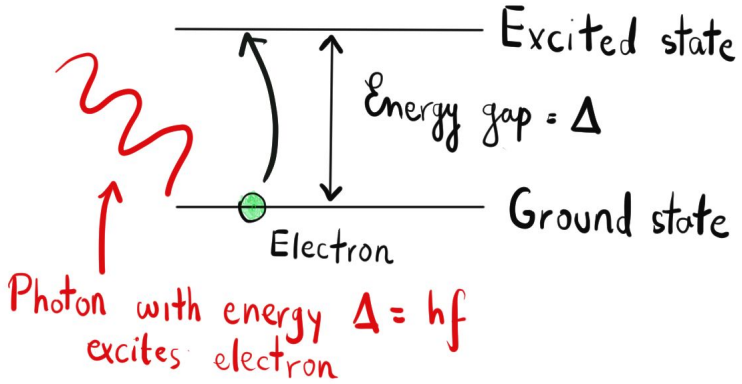


Interaction between ions

We want interactions of qubits, but putting them too close together will result in too much interaction and too far results in no interaction.

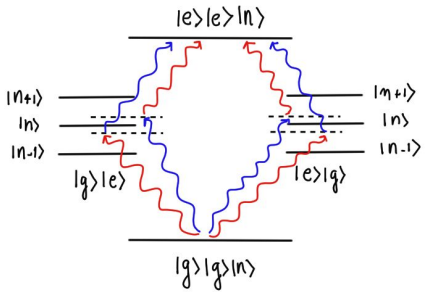
We can utilize the Mossbauer effect by cooling the ions down. This will create a quantization in space for each ion. Therefore, giving a photon to an individual qubit will not affect the other surrounding ions.

The excitation from photon gives the ion the two states which are ground states and excited states. This defines the ion as a qubit.

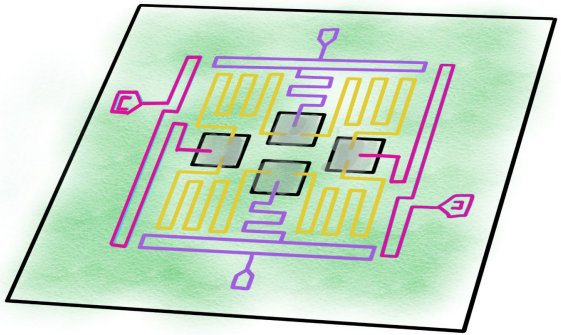


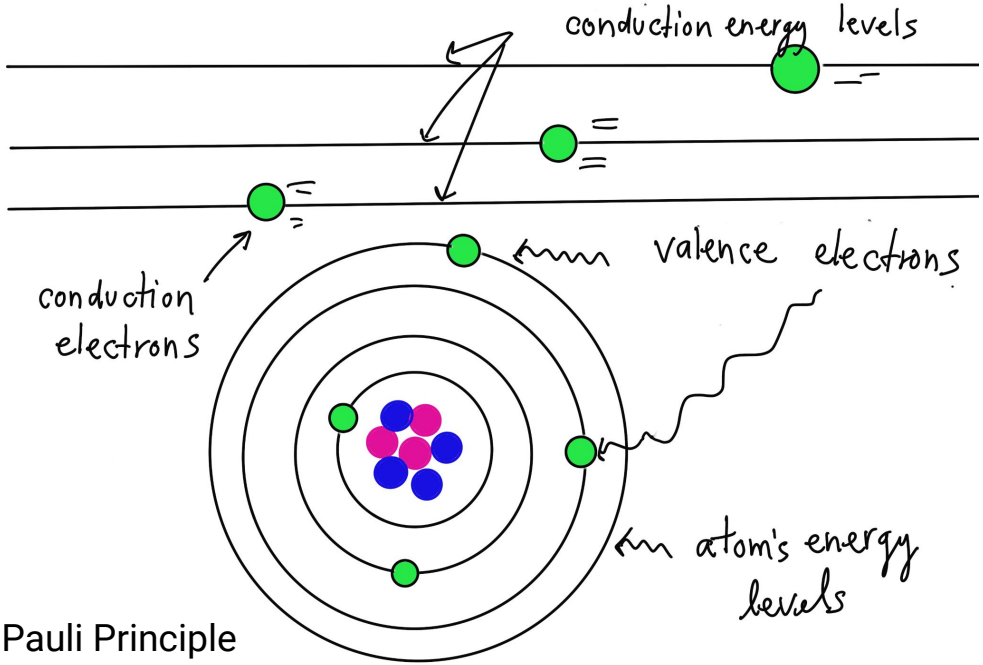
Advantages/Disadvantages

Advantage: well-defined qubit, we can initialize the state by letting the system cool down. It is possible to come up with universal gates.
Disadvantage: ions are too big which result in a shorter time for coherence, the size also results in the difficulty of scaling.



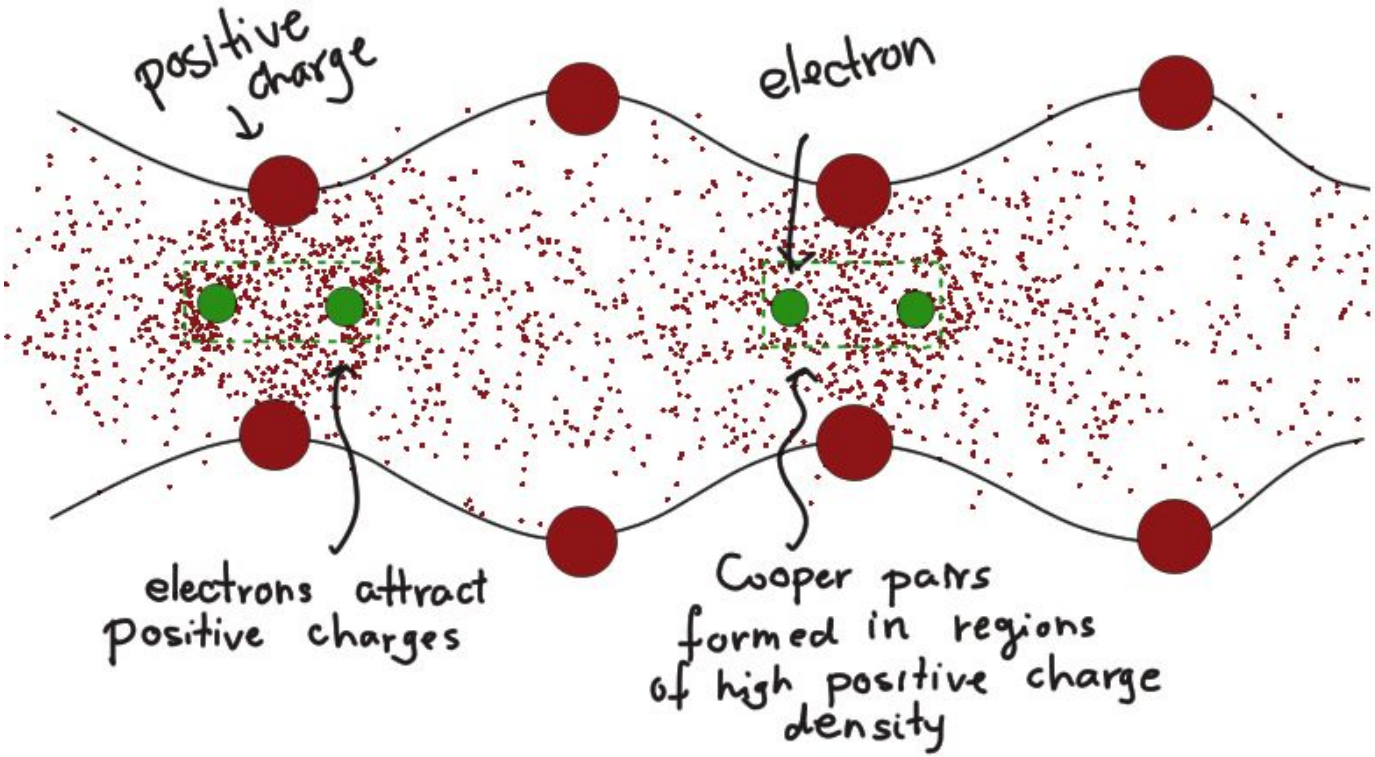
Superconducting Quantum Computer





Obeying the Pauli Principle

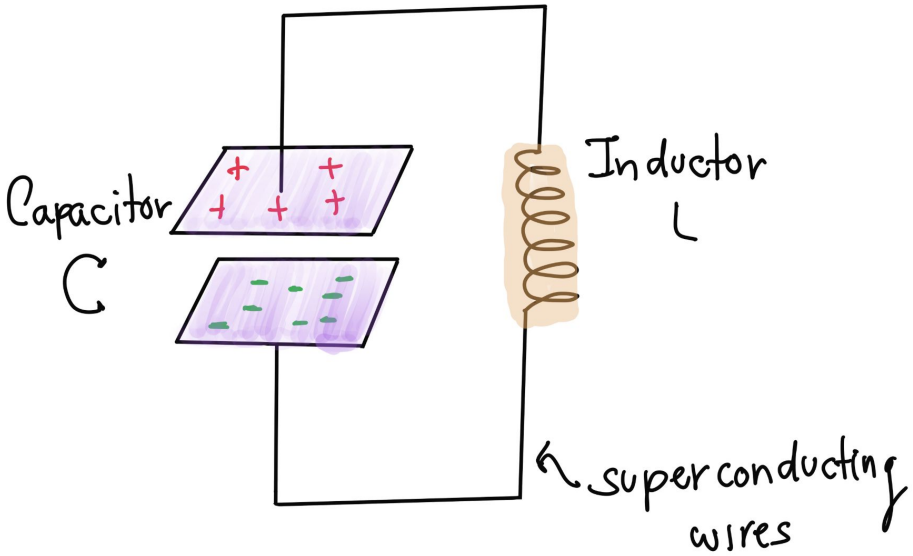
Some Materials at Low Temperature



These waves are phonons.

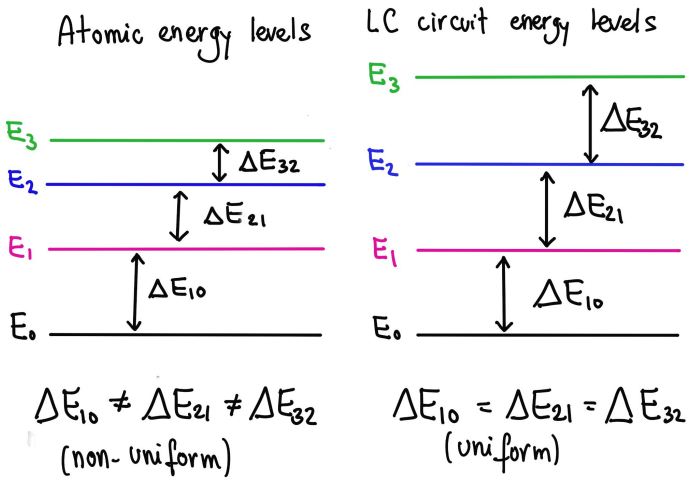
Cooper pairs act like boson which does not need to follow Pauli Principle
-> infinite states at low energy level -> infinite conductivity.

Electrical Components in Superconductor

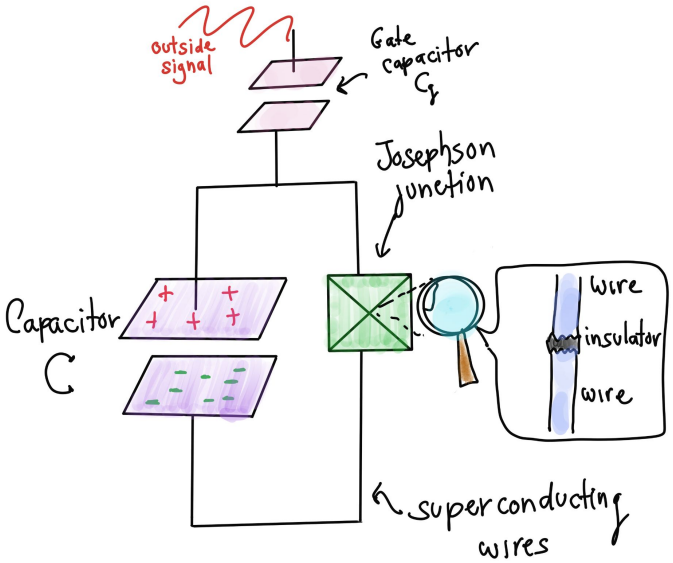


Capacitors and Inductors still act the same way in superconductors which allow us the alternating type of energy.

However, the LC circuit only allows a constant uniform transition.



Josephson Junction/Artificial Qubit



We want a non-uniform energy difference so that we can distinguish each state.
Adding an insulator to the wire will block the current. However, quantum tunneling allows Cooper pairs to tunnel through and gives us a non uniform current.

We want to control the system so we add a gate capacitor which takes in photons to determine how the circuit acts with outside signals. The energy levels become: