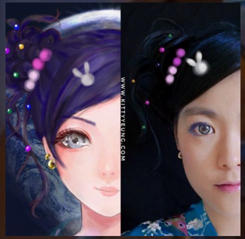
Introduction to Quantum Computing

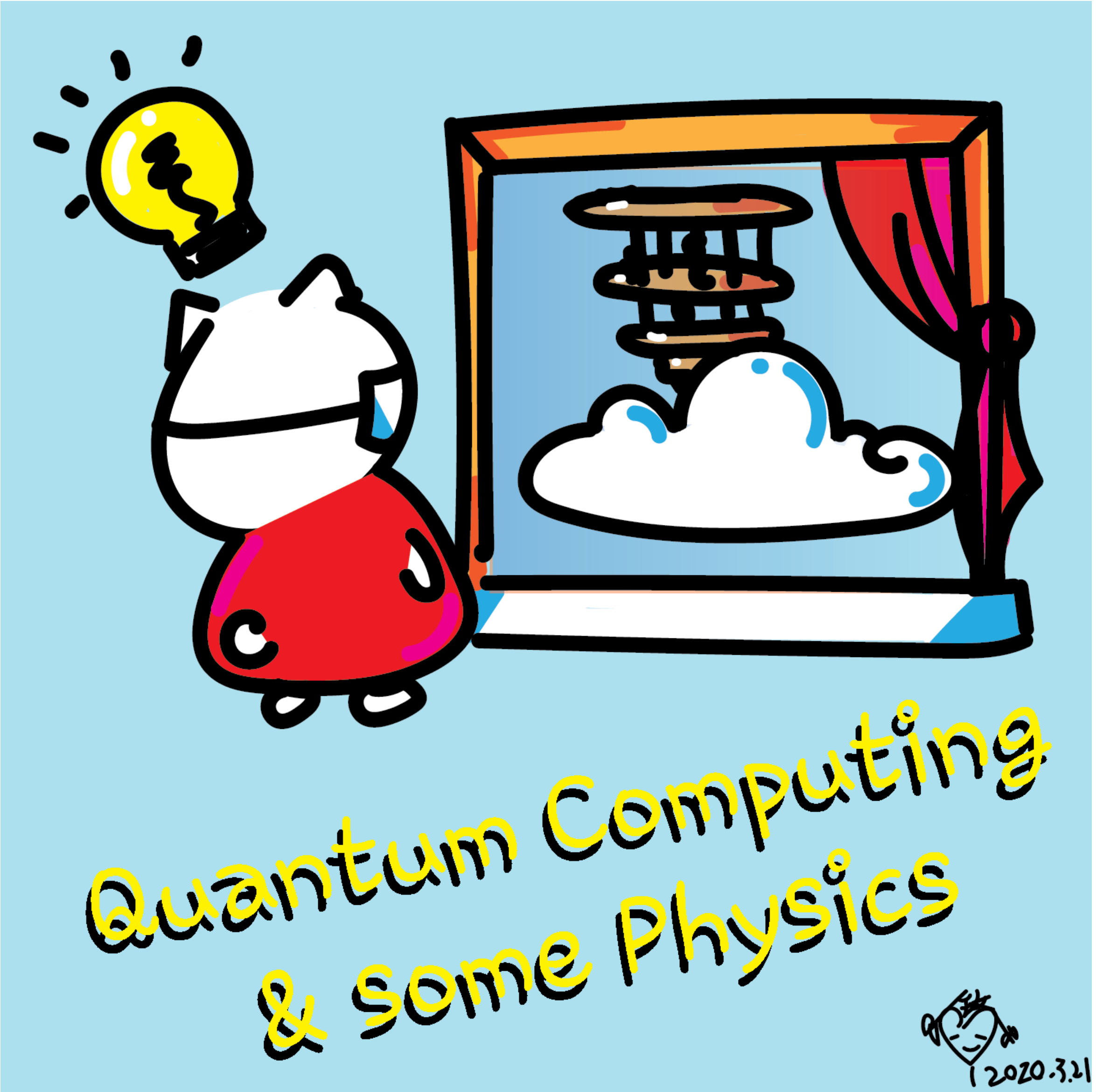


Kitty Yeung, Ph.D. in Applied Physics

Creative Technologist + Sr. PM
Microsoft

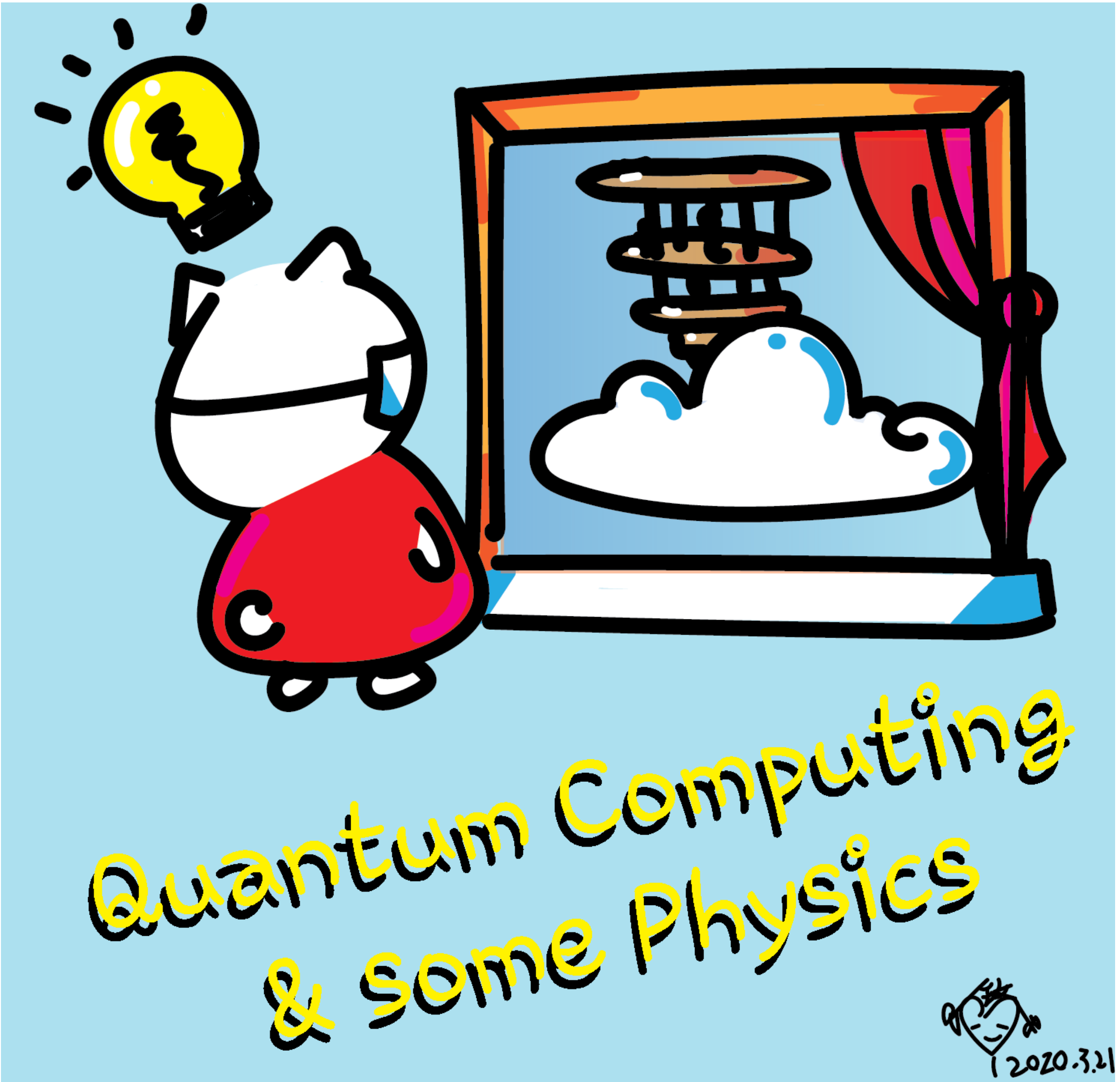
www.artbyphysicistkittyyeung.com
@KittyArtPhysics
@artbyphysicistkittyyeung

May 23, 2020

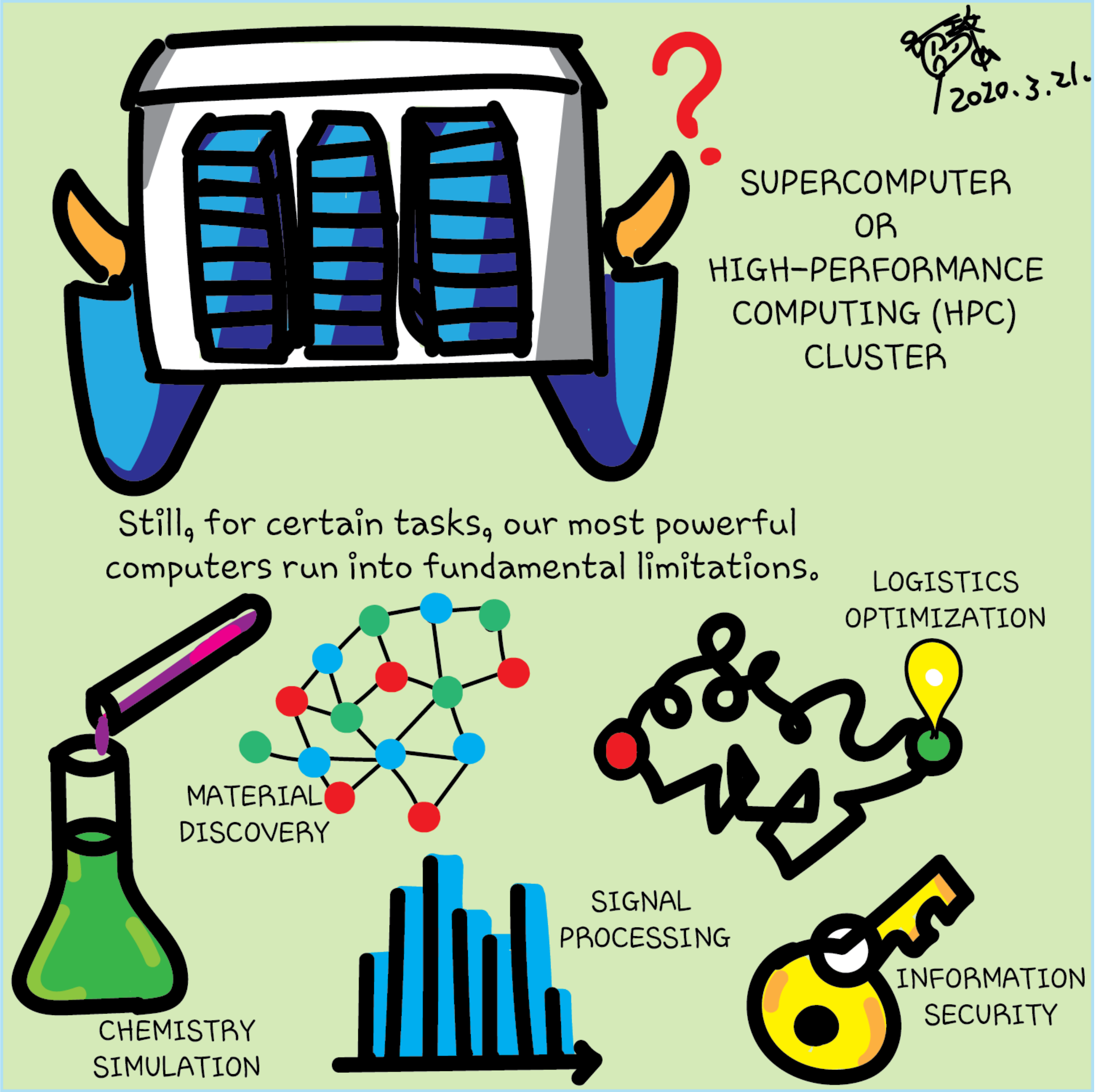

Quantum Computing
& some Physics
2020.3.21

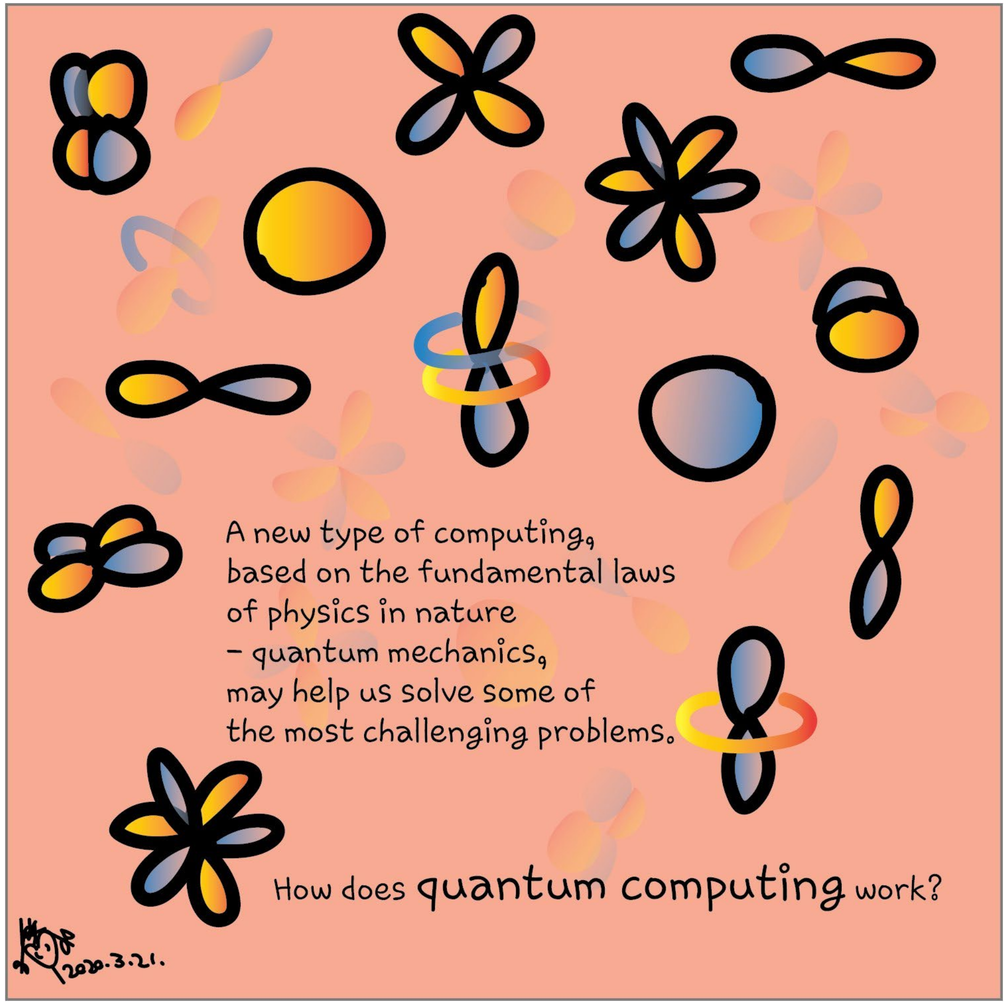
Class structure

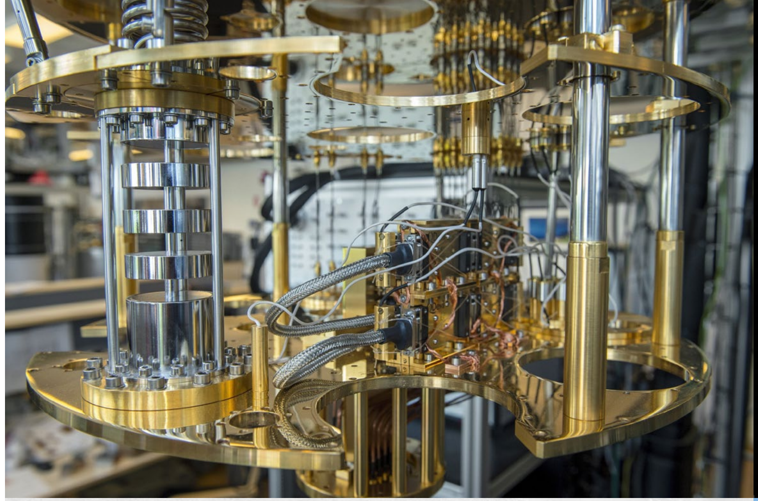
- [Comics on Hackaday – Introduction to Quantum Computing](#) every Wed & Sun
- 30 mins every Sun, one concept (theory, hardware, programming), Q&A
- Contribute to Q# documentation http://docs.microsoft.com/quantum
- Coding through Quantum Katas
- https://github.com/Microsoft/QuantumKatas/
- Discuss in Hackaday project comments
- throughout the week
- Take notes

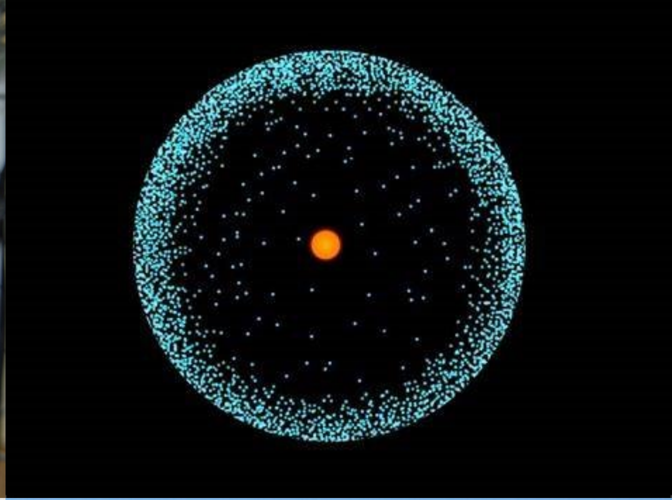


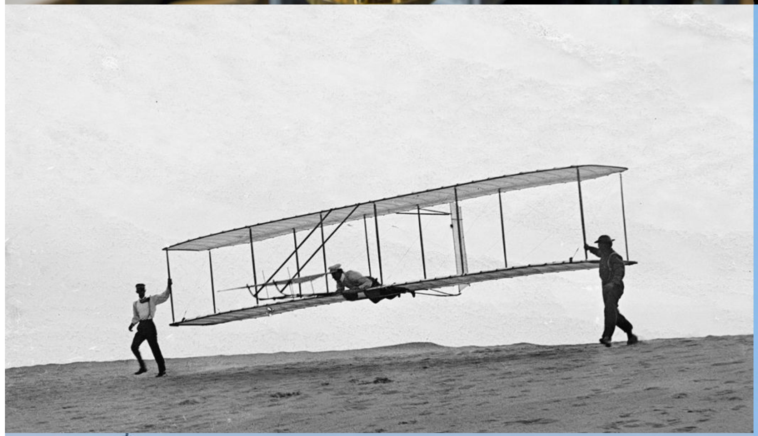

Our world now runs on computers
2020.3.21
– they are machines we task to carry out work more efficiently than we ever do manually.
DATA CENTER SERVERS
PUBLIC HEALTH
MOBILITY
EDUCATION
PRODUCTION
People and things are connected through the internet.

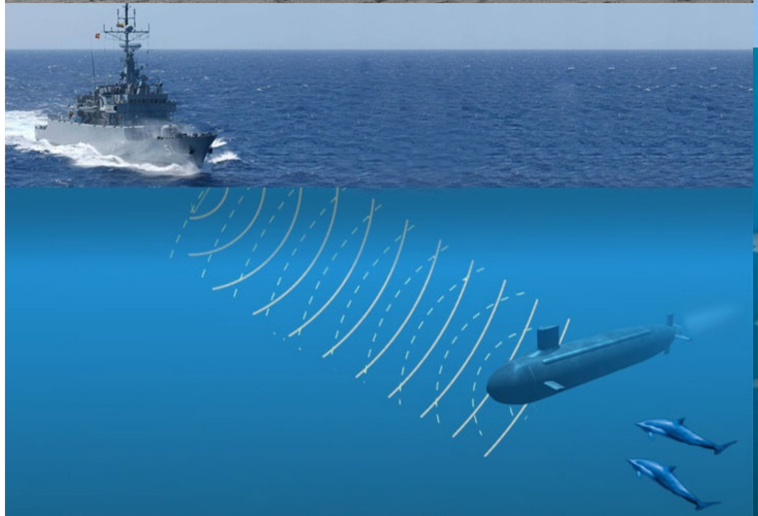

2020.3.21.
SUPERCOMPUTER
OR
HIGH-PERFORMANCE
COMPUTING (HPC)
CLUSTER
Still, for certain tasks, our most powerful computers run into fundamental limitations.
LOGISTICS
OPTIMIZATION
MATERIAL
DISCOVERY
CHEMISTRY
SIMULATION
SIGNAL
PROCESSING
INFORMATION
SECURITY

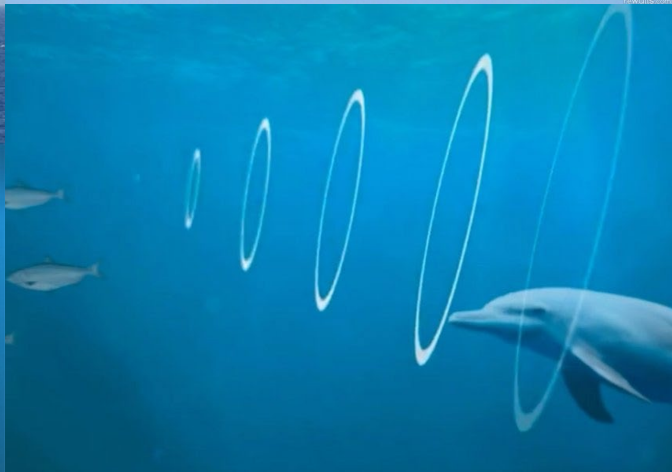

A new type of computing,
based on the fundamental laws
of physics in nature
– quantum mechanics,
may help us solve some of
the most challenging problems.
How does quantum computing work?
2020.3.21.

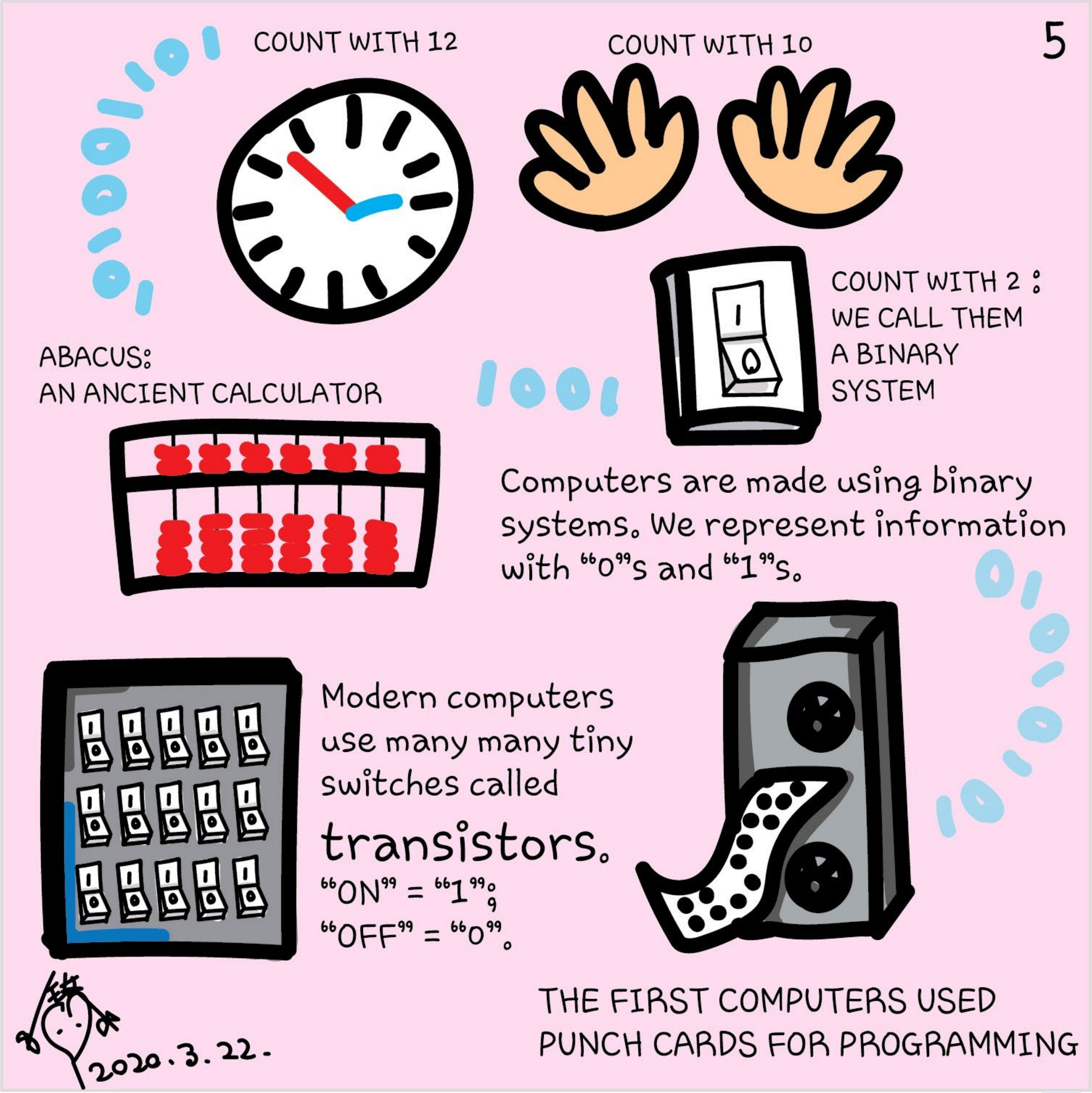






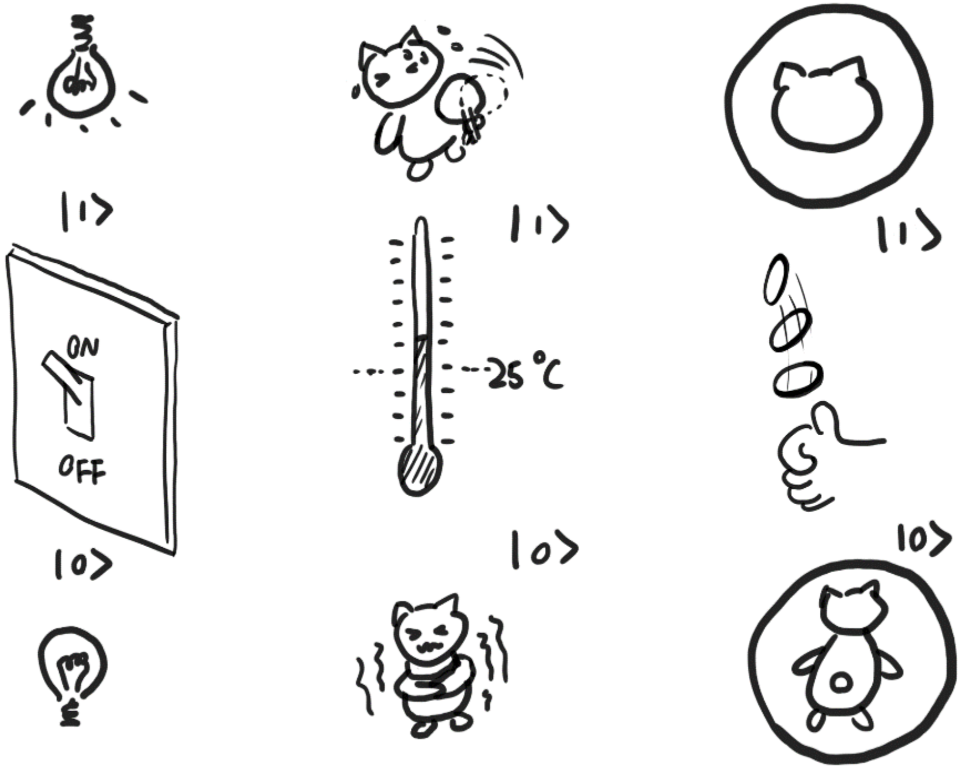




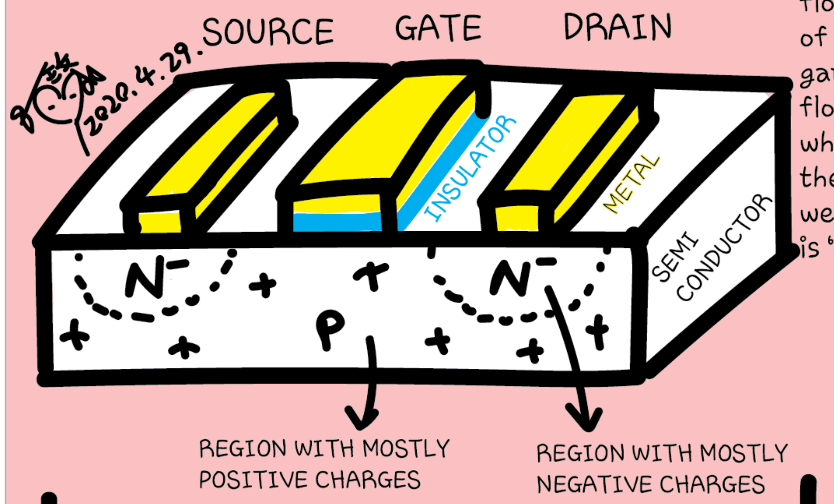

COUNT WITH 12
COUNT WITH 10
5
COUNT WITH 2: WE CALL THEM A BINARY SYSTEM
ABACUS: AN ANCIENT CALCULATOR
Computers are made using binary systems. We represent information with "0"s and "1"s.
Modern computers use many many tiny switches called transistors.
"ON" = "1";
"OFF" = "0".
THE FIRST COMPUTERS USED PUNCH CARDS FOR PROGRAMMING
2020.3.22.

States – classical bits

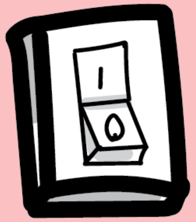
$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$



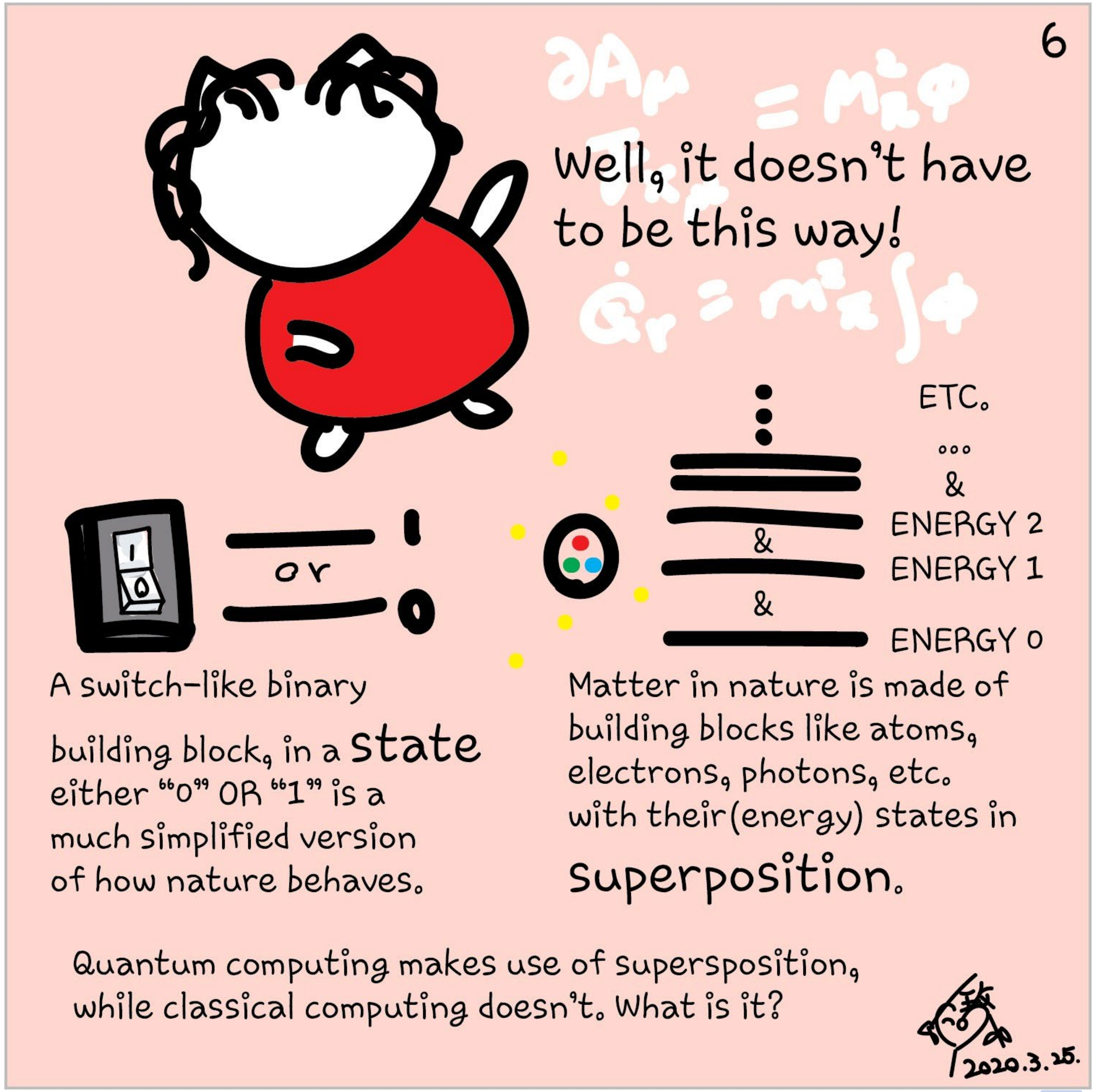
We leverage various properties of materials to make computing hardware.

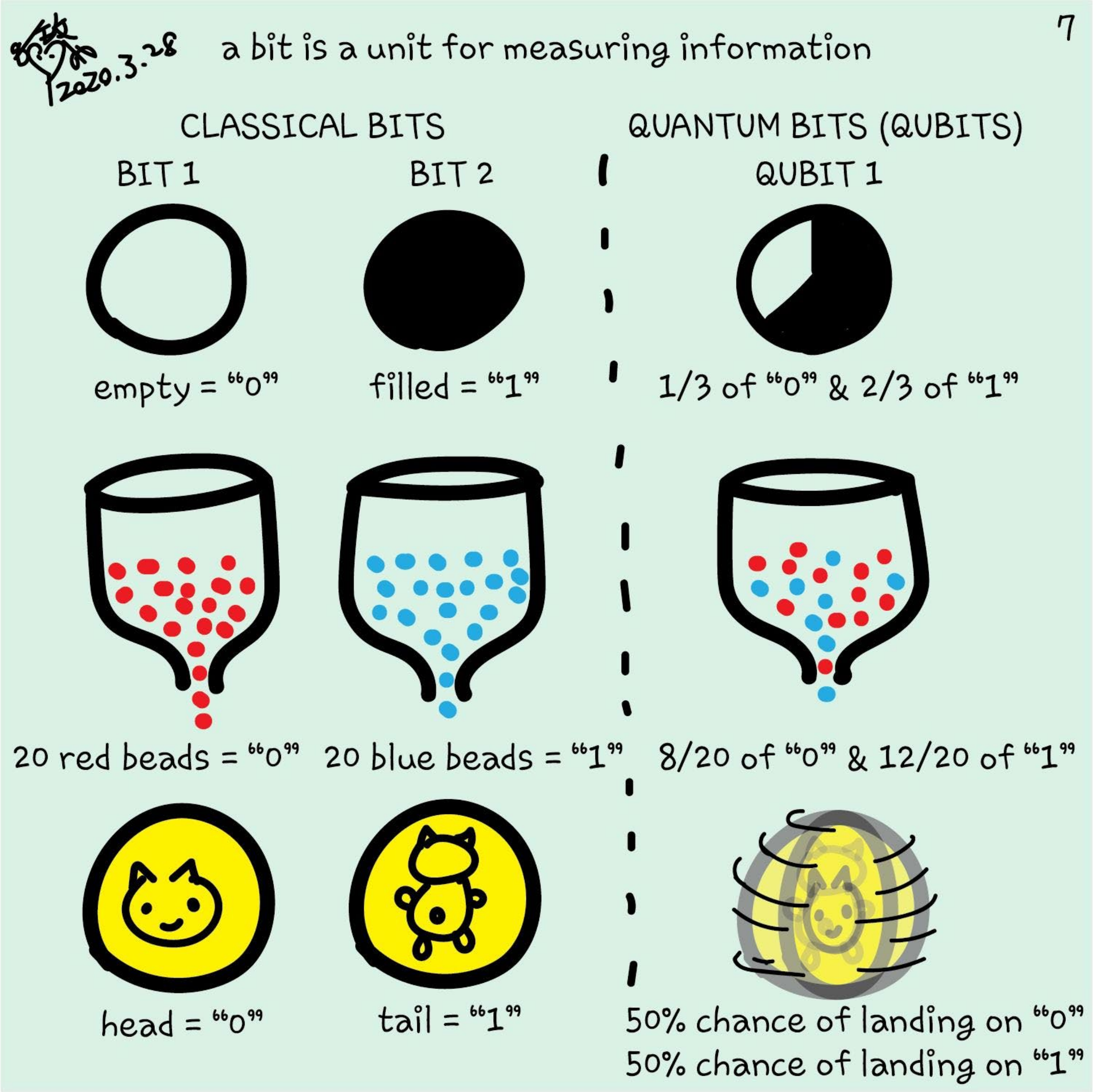


The gate applies voltage to control the electron flow from source to drain of a transistor. At a certain gate voltage level, electrons flow. This is the "on" state which we call "1". When there's no electron flow, we say the transistor is "off", or "0".



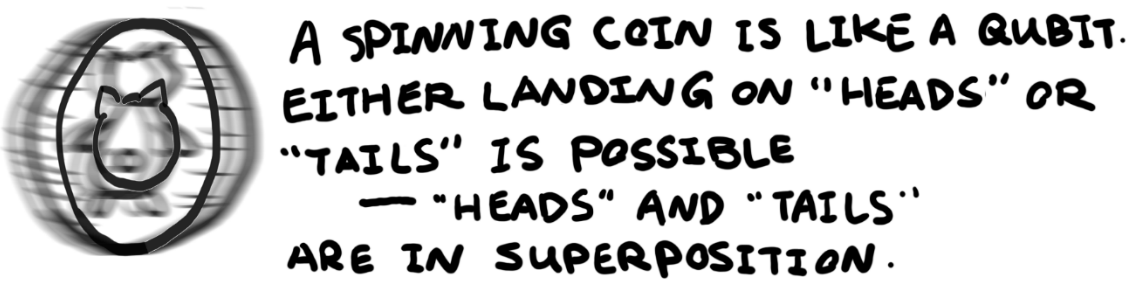
Transistors are nano- to micrometer switches.

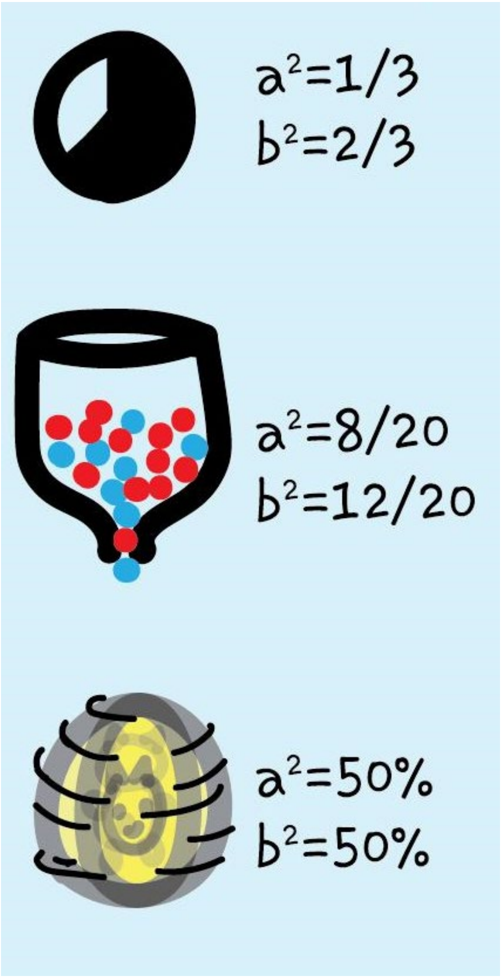

6
Well, it doesn't have to be this way!
or
1
0
ETC.
...
&
ENERGY 2
&
ENERGY 1
&
ENERGY 0
A switch-like binary building block, in a state either "0" OR "1" is a much simplified version of how nature behaves.
Matter in nature is made of building blocks like atoms, electrons, photons, etc. with their (energy) states in superposition.
Quantum computing makes use of superposition, while classical computing doesn't. What is it?
2020.3.25.



2020.3.28
a bit is a unit for measuring information
7
CLASSICAL BITS
QUANTUM BITS (QUBITS)
BIT 1
BIT 2
QUBIT 1
empty = "0"
filled = "1"
1/3 of "0" & 2/3 of "1"
20 red beads = "0"
20 blue beads = "1"
8/20 of "0" & 12/20 of "1"
head = "0"
tail = "1"
50% chance of landing on "0"
50% chance of landing on "1"

Quantum bits – qubits

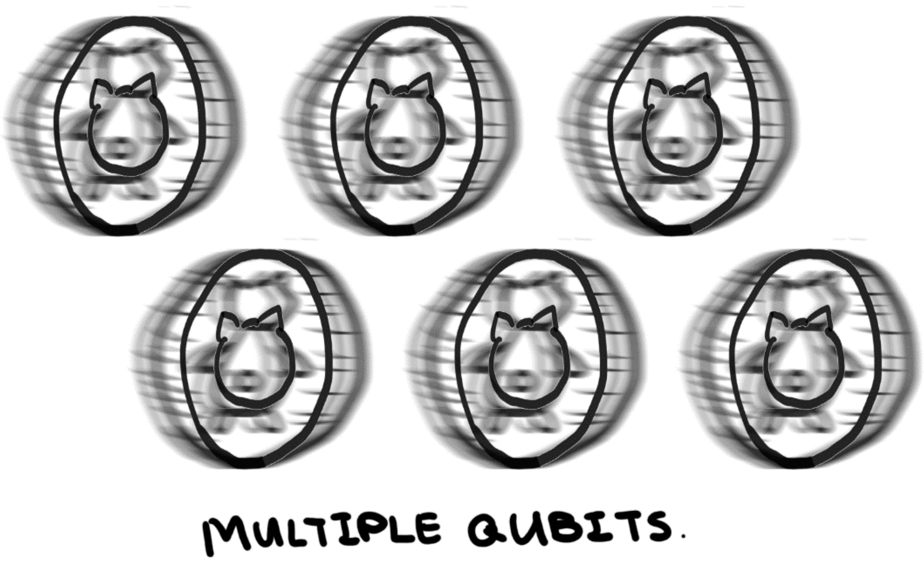




$$|\psi\rangle = \binom{a}{b} = a|0\rangle + b|1\rangle$$

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

Quantum bits – qubits



Two qubits:

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

$$= \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

$$= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

$$|ac|^2 + |ad|^2 + |bc|^2 + |bd|^2 = 1$$

If we can represent the ideas with pictures, we can also represent them with numbers and symbols, i.e. MATHS!

CLASSICAL BITS		QUANTUM BITS
BIT 1	BIT 2	QUBIT 1
$\|0\rangle$	$\|1\rangle$	$a\|0\rangle + b\|1\rangle$

(This $|...\rangle$ symbol is called a Dirac notation. It means a state in ... We mentioned "state" in page 5.)

a and b indicate how much of $|0\rangle$ and $|1\rangle$ are in the system

In our previous scenarios:

$a^2=1/3$
$b^2=2/3$

$a^2=8/20$
$b^2=12/20$

$a^2=50\%$
$b^2=50\%$

In other words, a and b are **amplitudes** of states $|0\rangle$ and $|1\rangle$. Their squares, a^2 and b^2, are the **probabilities** of finding the system in the state $|0\rangle$ and $|1\rangle$, respectively.

The qubit, $a|0\rangle+b|1\rangle$, is represented as a linear combination of states $|0\rangle$ and $|1\rangle$, equivalent of saying $|0\rangle$ and $|1\rangle$ are in superposition.

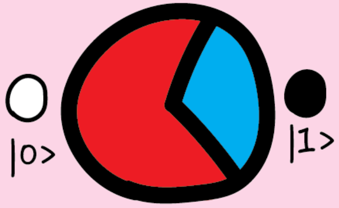
What do these lead to?

2020.3.28.

2020.3.28.

A qubit system is all the possible configurations in superposition.

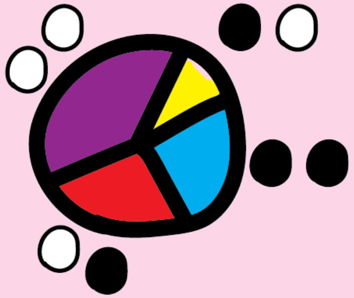
PIE CHART DENOTING PROBABILITY OF EACH CONFIGURATION



ONE QUBIT, TWO CONFIGURATIONS:

$a|0\rangle+b|1\rangle$

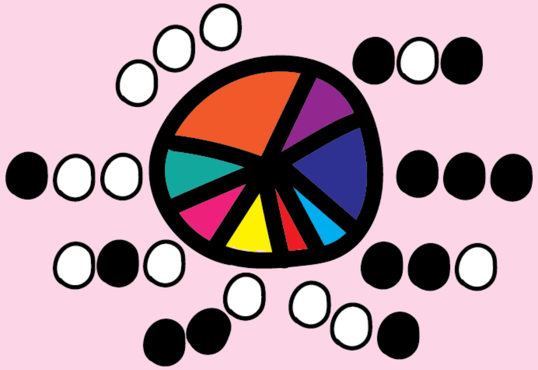
$a^2+b^2=1$ (total probability adds up to 1)



TWO QUBITS, FOUR CONFIGURATIONS:

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

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



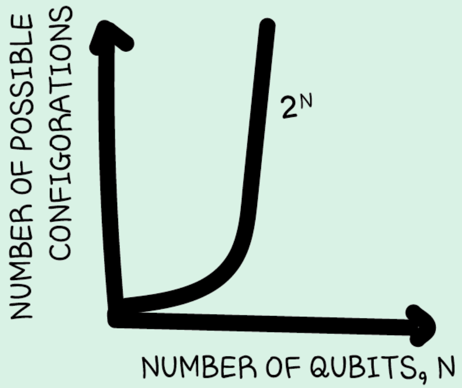
THREE QUBITS, EIGHT CONFIGURATIONS:

$a|000\rangle+b|001\rangle+c|010\rangle+d|100\rangle+e|110\rangle+f|101\rangle+g|011\rangle+h|111\rangle$

$a^2+b^2+c^2+d^2+e^2+f^2+g^2+h^2=1$

...

N qubits will have 2^N possible configurations in superposition!



Not only does the number of possible configurations grow exponentially with the number of qubits as 2^N, the number of possible combinations of amplitudes is infinite, as long as their squares – the probabilities – add up to 1.

THIS SYMBOL MEANS SUMMING ALL N TERMS FROM 1

$$|\psi\rangle = \sum_{i=1}^{N} c_i |\psi_i\rangle$$

AN N-QUBIT STATE

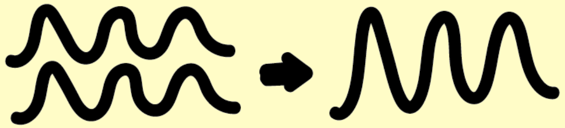
EACH POSSIBLE CONFIGURATION

The amplitude ci = a, b, c, d ...n
can be positive numbers 1, 1/2, 1/3, 1/4 ...n
or negative numbers −1, −1/2, −1/3, −1/4 ...n
(these are real numbers)
or imaginary numbers (+/−) i, 1/2i, 1/3i, 1/4i...ni
or 0.
In general they can be complex numbers
(with real and imaginary parts with
positive or negative signs)!

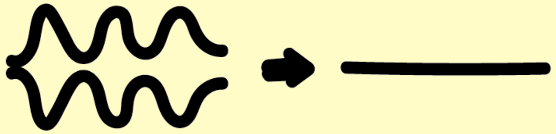
What's the consequence?

2020.4.1.

Our daily experience of amplitudes(like those of water waves, light waves, sound waves, etc.) has told us:

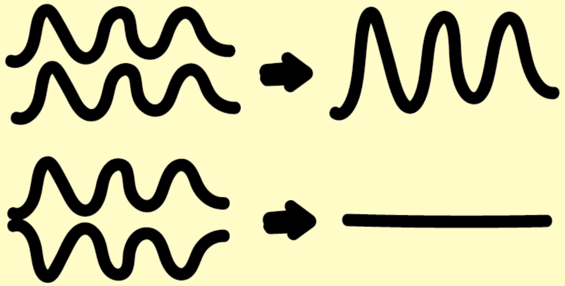


AMPLITUDES CAN ADD UP =
CONSTRUCTIVE INTERFERECE



AMPLITUDES CAN CANCEL OUT =
DESTRUCTIVE INTERFERENCE

Our daily experience of amplitudes(like those of water waves, light waves, sound waves, etc.) has told us:



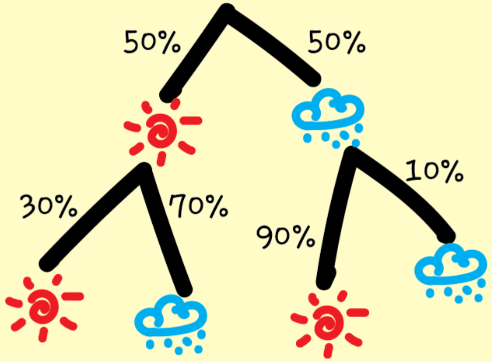
AMPLITUDES CAN ADD UP = CONSTRUCTIVE INTERFERECE

AMPLITUDES CAN CANCEL OUT = DESTRUCTIVE INTERFERENCE

How likely will it be sunny the day after tomorrow?

CLASSICAL

USES PROBABILITY DIRECTLY

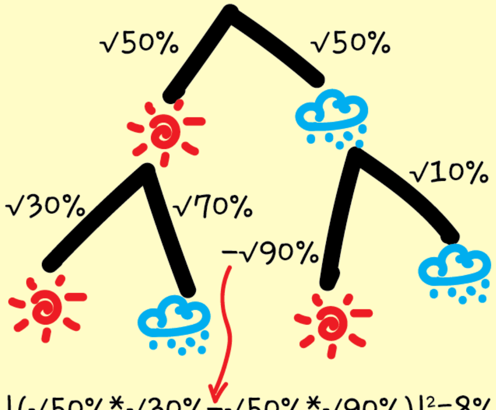


$$50\%*30\%+50\%*90\%=60\%$$

Having more paths in classical case always leads to more likelihood.

QUANTUM

USES AMPLITUDE, AND CAN BE NEGATIVE



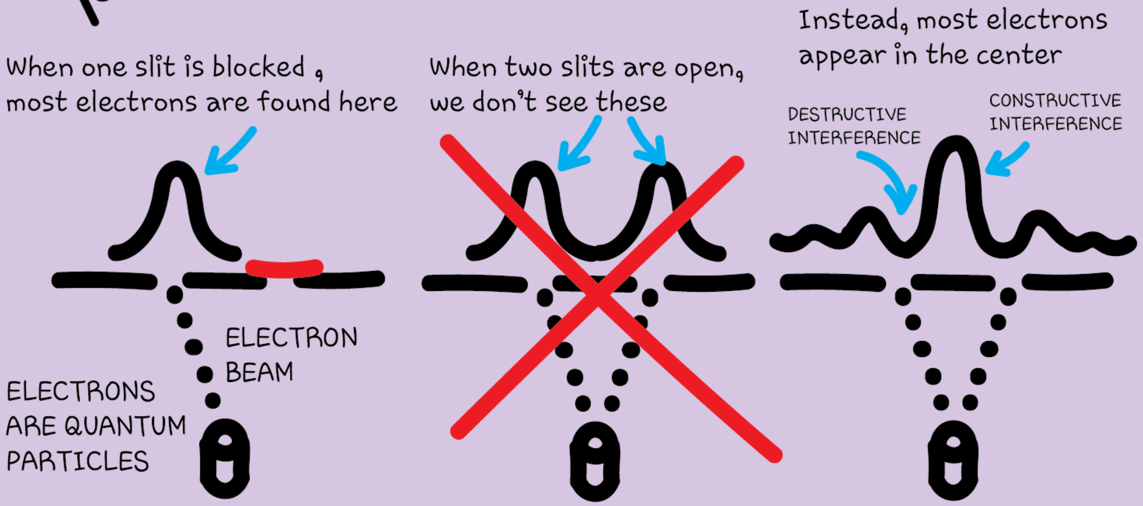
$$|(\sqrt{50\%}*\sqrt{30\%}-\sqrt{50\%}*\sqrt{90\%})|^2=8\%$$

But in quantum case, the 2nd path of having a sunny day destructively interferes with the 1st one, making it less likely.

2020.4.4.

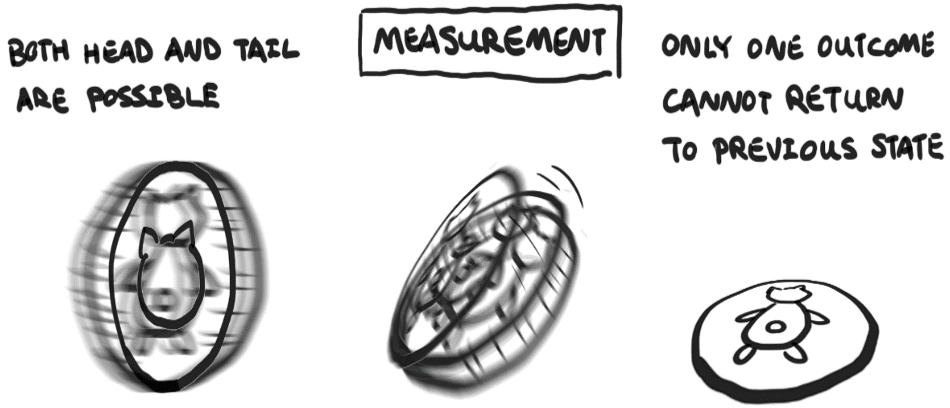
So, the things we observe (**measure**) are the results of interference. Possible results from constructive interference are more likely to be measured. The other possibilities cancel each other out through destructive interference.

The famous double-slit experiment is a direct manifestation of quantum interference.



Interference is one of the "strange" behaviours of quantum systems enabled by superposition. What else?

Measurement



Not reversible

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

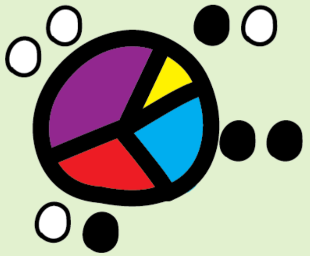
$$P = |c_{00}|^2 + |c_{01}|^2$$

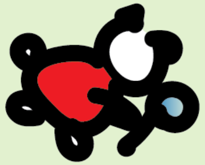
If first qubit is 0

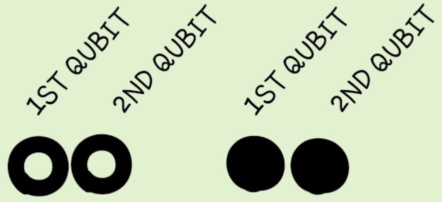
$$|\psi'\rangle = \frac{c_{00}|00\rangle + c_{01}|01\rangle}{\sqrt{P}}$$

After measurement

We've seen in page 9 that with two qubits, there are four possible configurations: both qubits in |0>s or |1>s, or one in |0> with the other in |1>. What if we make the |0>|0> case in superposition with the |1>|1> case? Or |0>|1> in superposition with |1>|0>?



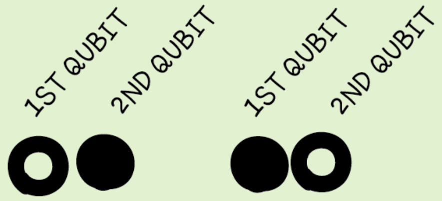




$a|0\quad 0\rangle + d|1\quad 1\rangle$

If we set the system to be in this case, we know that if we measure the first qubit and get |0>, the second qubit must be in |0>, without needing to measure it.

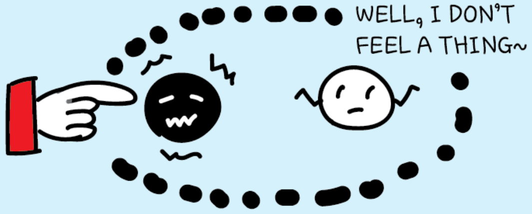
We can also measure the second qubit to know what the first qubit is without measuring it.



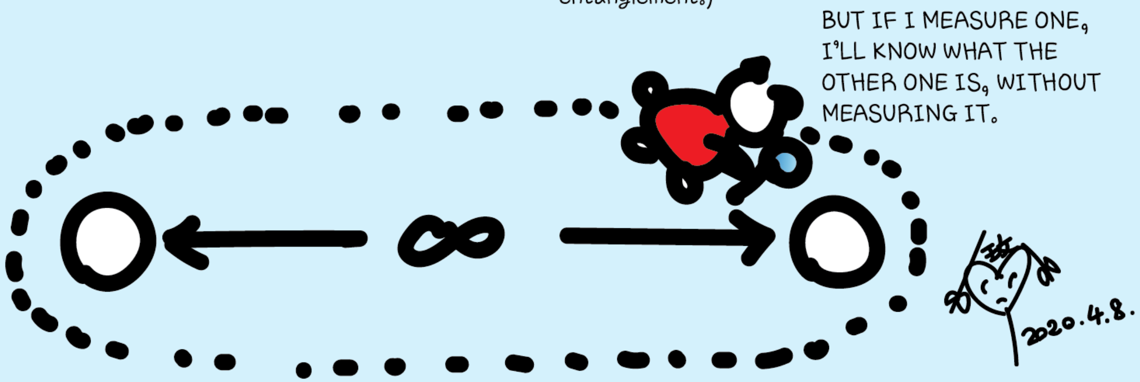
$b|0\quad 1\rangle + c|1\quad 0\rangle$

Similarly in this case, if the first qubit is |0>, the second qubit must be |1>. If the first is |1>, the second must be |0>.

The qubits are correlated. This is called "**entanglement**".



When we change one of the entangled qubits, the other qubit does not instantaneously change. (That would imply faster-than-light information transfer, which is prohibited. This is a common mistake people make when talking about entanglement.)



They can remain entangled even if they are separated infinitely far apart. There is no "spooky" interaction between them. All it means is that their measurement results are correlated. And entanglement simply does not depend on distance.

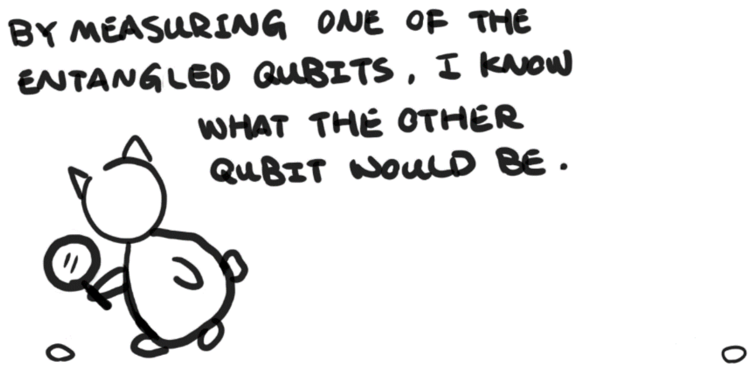
$$1/\sqrt{2}(|00\rangle+|11\rangle) \qquad 1/\sqrt{2}(|01\rangle+|10\rangle)$$
$$1/\sqrt{2}(|00\rangle-|11\rangle) \qquad 1/\sqrt{2}(|01\rangle-|10\rangle)$$

A special set of entangled two qubits is the four Bell states. We use them in every quantum algorithm.

Entanglement

Bell states

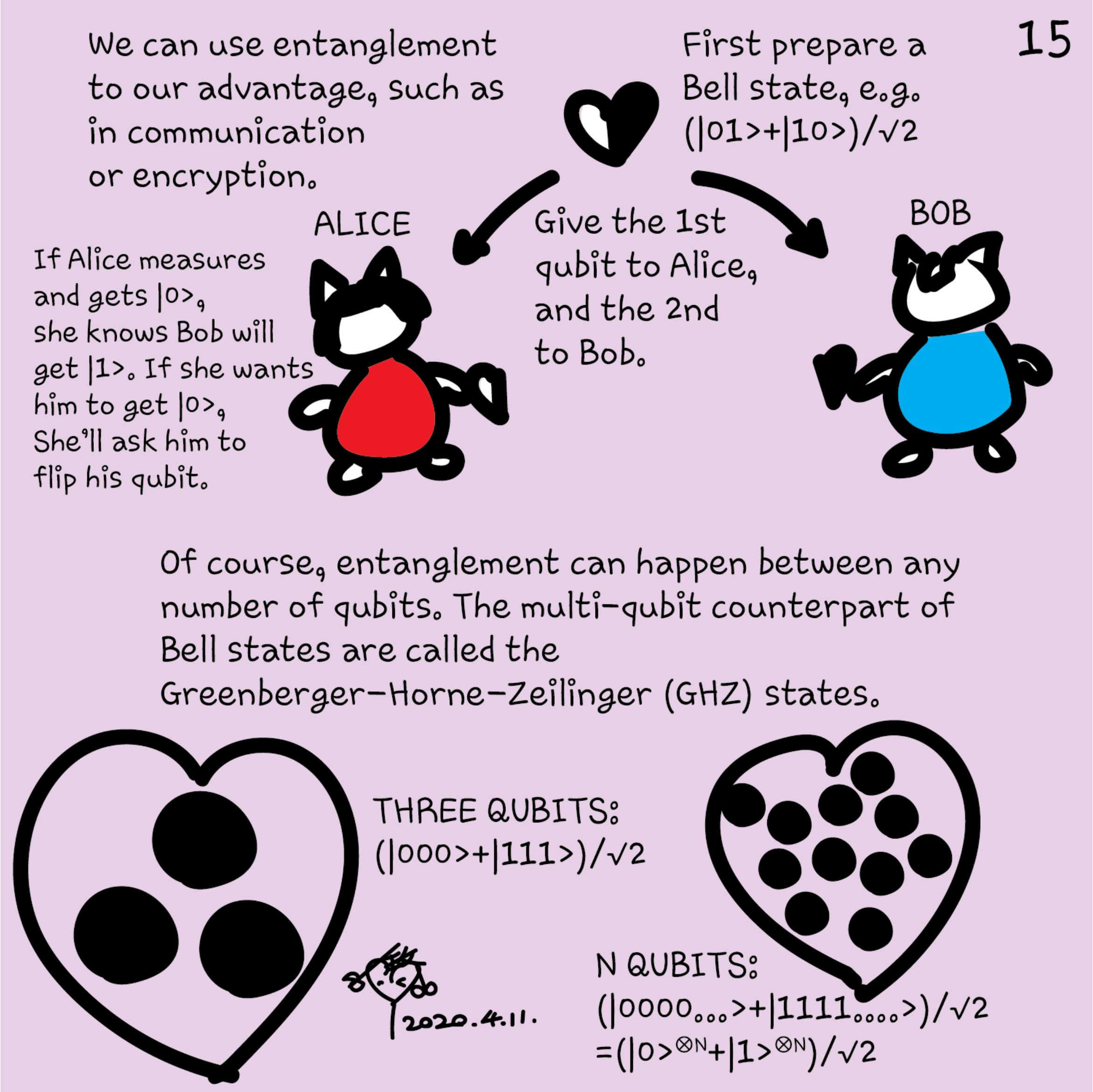
$$|\varphi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \text{ and } |\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$$



Take $|\phi^{+}\rangle$ as an example, upon measuring the first qubit, one obtains two possible results:

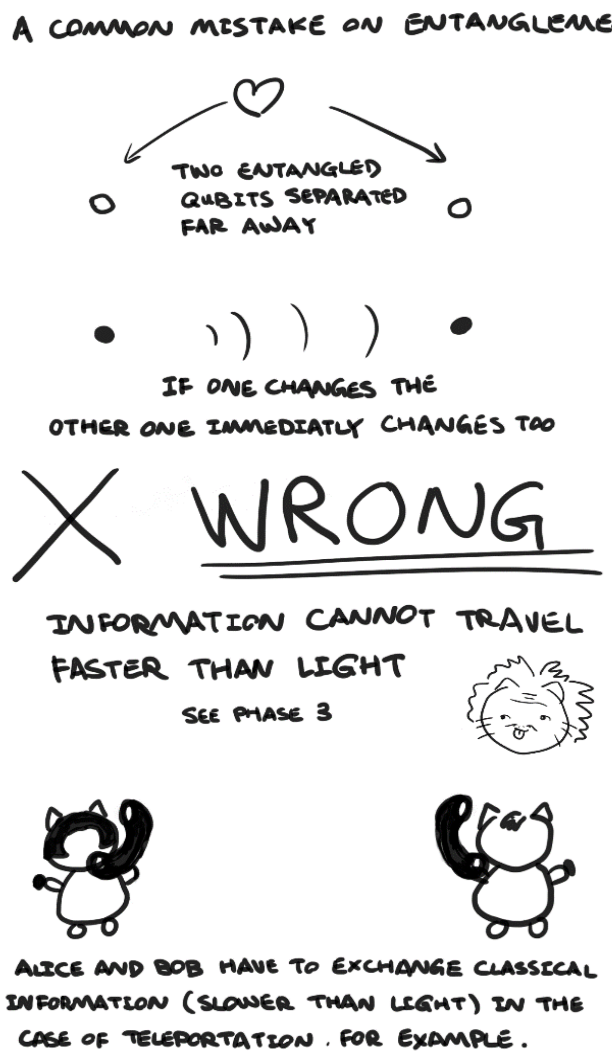
1. First qubit is 0, get a state $|\phi'\rangle = |00\rangle$ with probability ½.
2. First qubit is 1, get a state $|\phi''\rangle = |11\rangle$ with probability ½.

If the second qubit is measured, the result is the same as the above. This means that measuring one qubit tells us what the other qubit is.

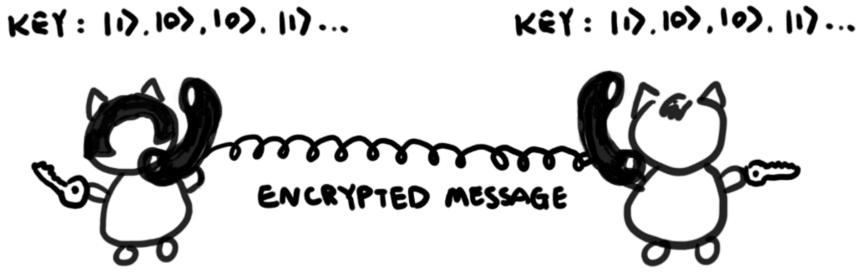

15
We can use entanglement to our advantage, such as in communication or encryption.
First prepare a Bell state, e.g. $(|01\rangle+|10\rangle)/\sqrt{2}$
ALICE
BOB
Give the 1st qubit to Alice, and the 2nd to Bob.
If Alice measures and gets $|0\rangle$, she knows Bob will get $|1\rangle$. If she wants him to get $|0\rangle$, She'll ask him to flip his qubit.
Of course, entanglement can happen between any number of qubits. The multi-qubit counterpart of Bell states are called the Greenberger-Horne-Zeilinger (GHZ) states.
THREE QUBITS: $(|000\rangle+|111\rangle)/\sqrt{2}$
N QUBITS: $(|0000...\rangle+|1111....\rangle)/\sqrt{2}$
$=(|0\rangle^{\otimes N}+|1\rangle^{\otimes N})/\sqrt{2}$
2020.4.11.

https://quantumfactsheet.github.io/

A common mistake



Encryption



They can’t communicate faster than light, but at least they can communicate securely.

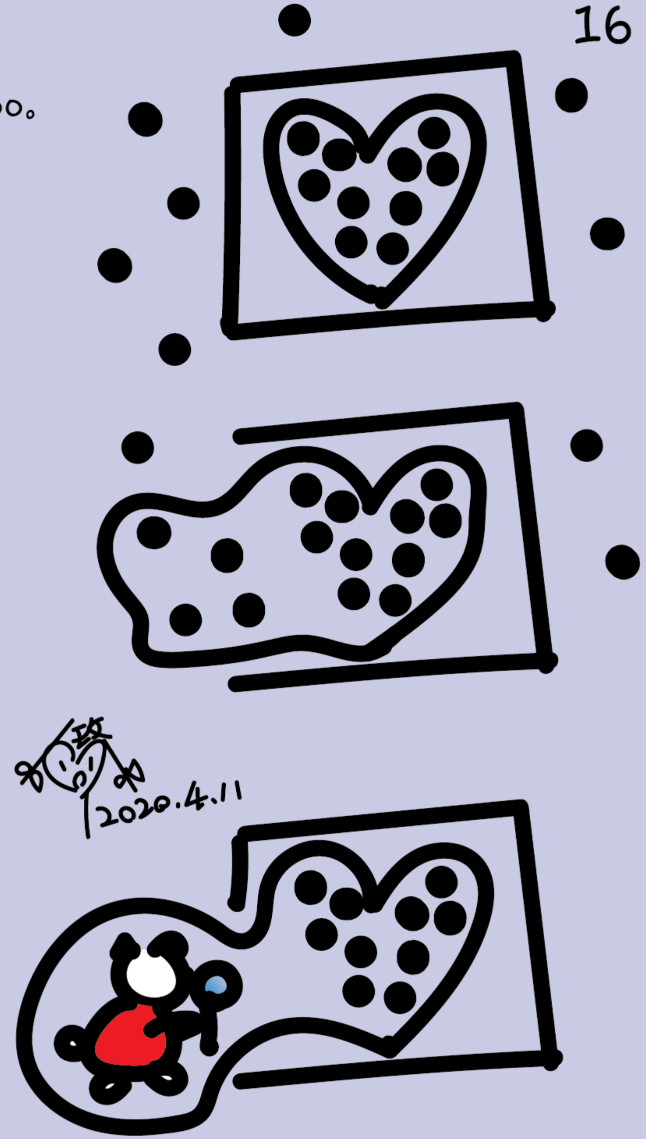
However, entanglement can be disadvantageous, too.

If the qubits are not perfectly isolated,

entanglement with their environment can easily happen, causing the qubits to **decohere** from each other.

Measurements also cause decoherence, when the measuring device acts as the environment that entangles with the qubits.

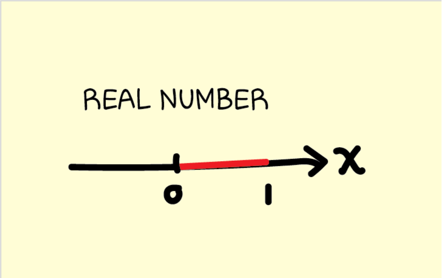
Therefore, measurements must be delicately done. Otherwise, they cause errors.



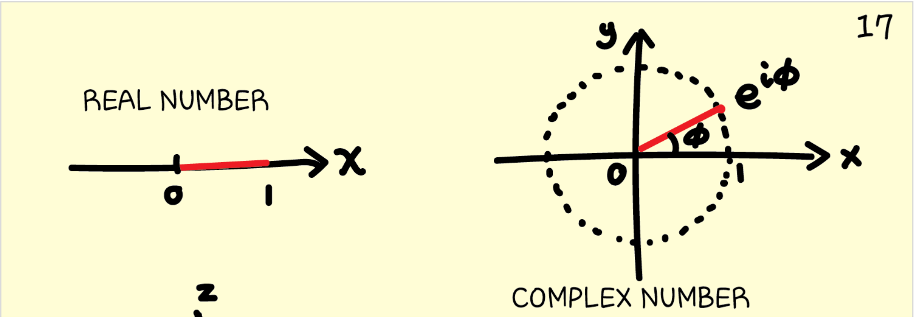
3 concepts

- Superposition
- Interference (measurement result is a result of interference)
- Entanglement (results of entangled qubits are correlated)

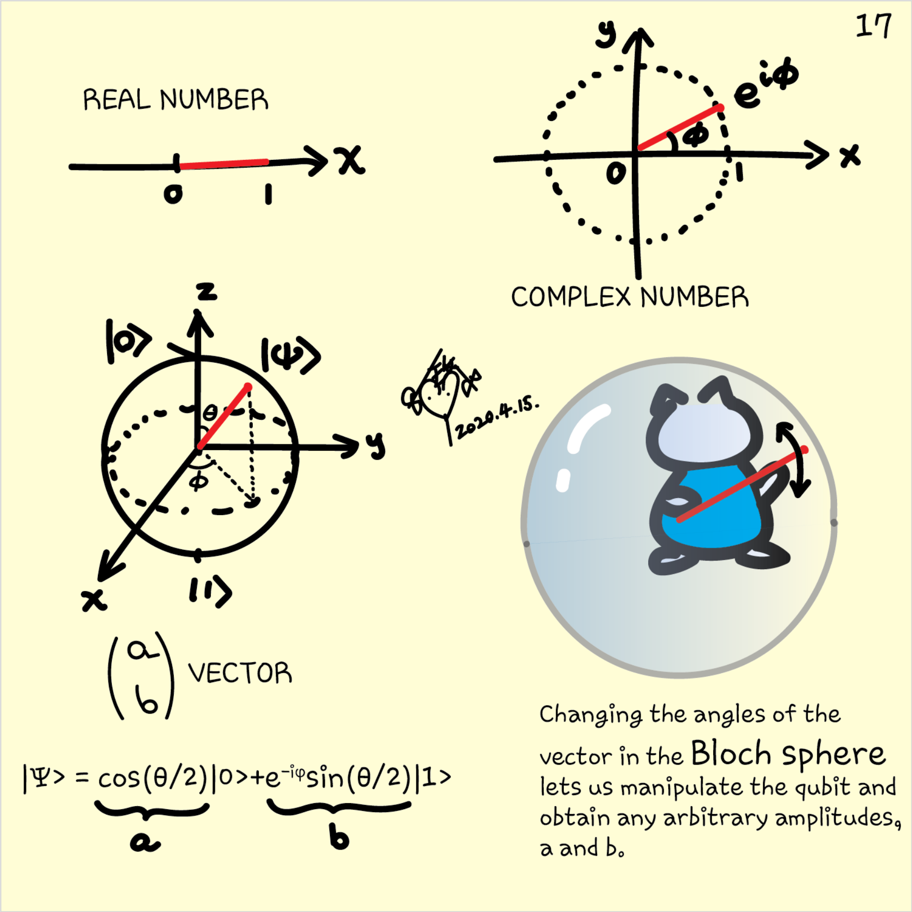
Graphic representation of a qubit



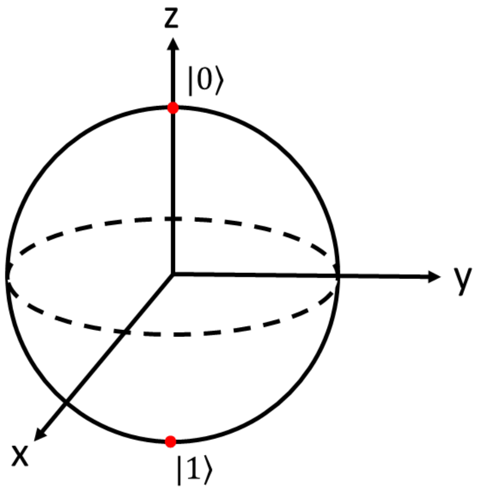
Graphic representation of a qubit

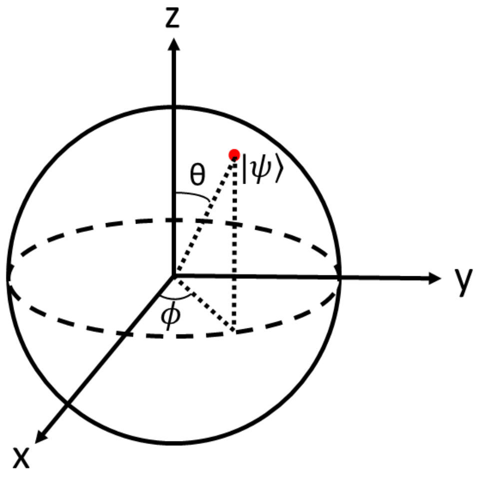


Graphic representation of a qubit



Bloch sphere



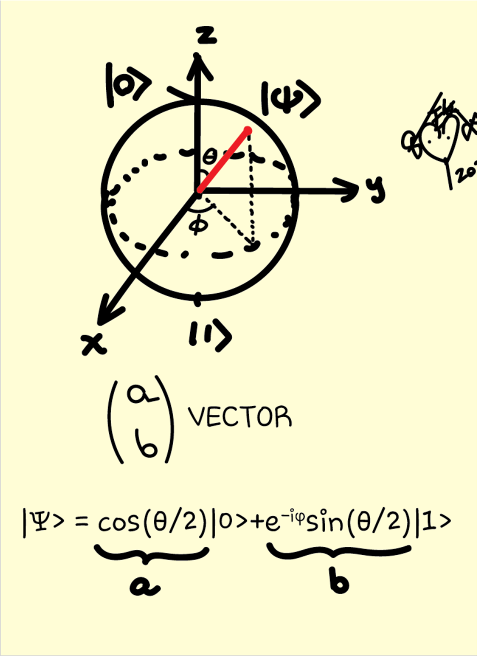


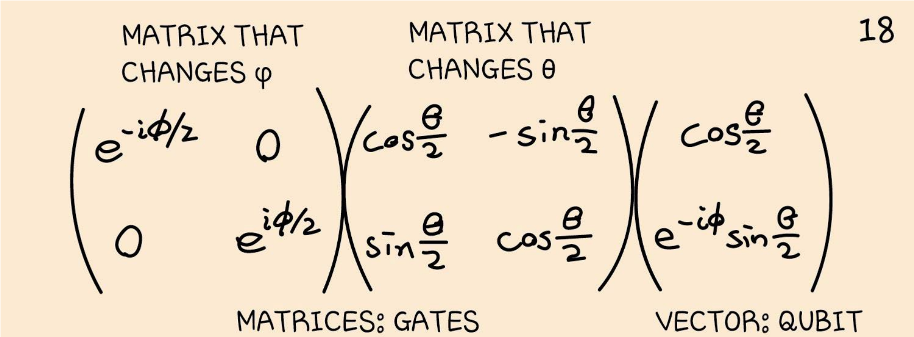
Arbitrary state

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{-i\phi}\sin\frac{\theta}{2}|1\rangle$$

the states $|0\rangle$ and $|1\rangle$ are just two special cases with θ = 0° and 180°, respectively.

Gates (quantum operations)





MATRIX THAT CHANGES φ

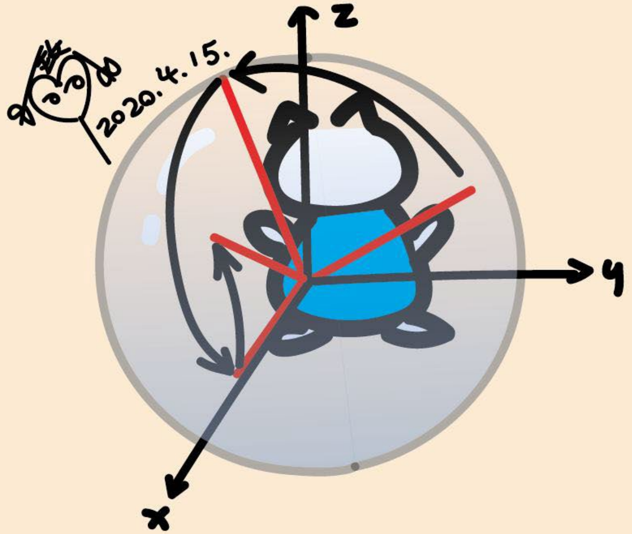
MATRIX THAT CHANGES θ

$$\begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{-i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

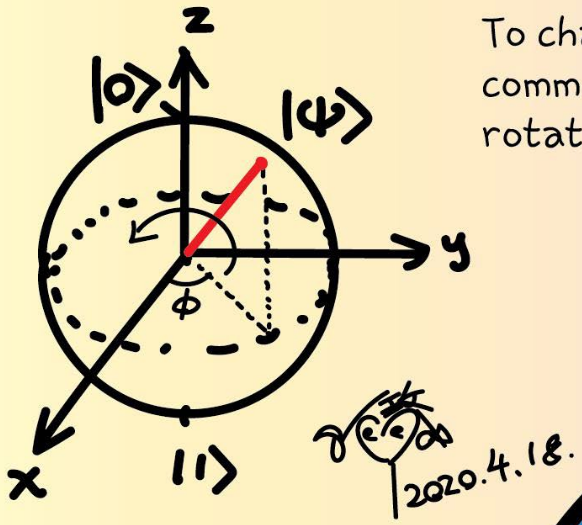
MATRICES: GATES

VECTOR: QUBIT

Like a set of coins, a combination of them can make up any number.

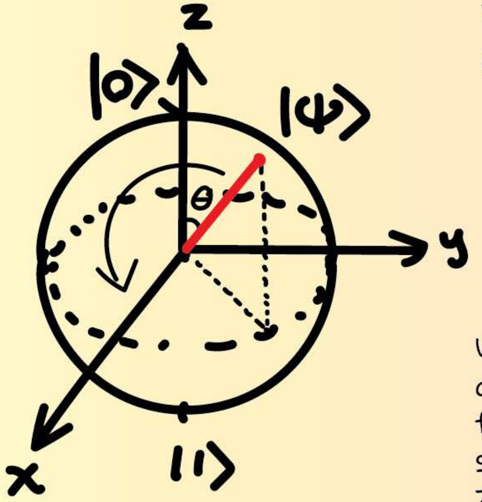


We can have a set of matrix operations (gates) that moves the qubit to anywhere on the Bloch sphere.



To change the phase φ, we have a commonly used gate, Z, which rotates about the z-axis by 180°.

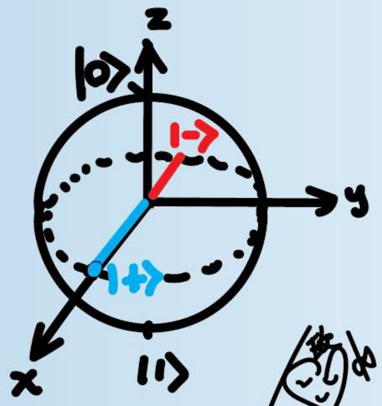
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Similarly, the X gate rotates about the x-axis by 180°, rotating the angle θ e.g. X|0> = |1>, X|1> = |0>.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

We have seen in page 18 the two matrices for changing φ and θ in arbitraty amounts. They form a universal gate set – they can put a state anywhere on the Bloch Sphere. The gates Z and X are special cases of them.



Another important gate is the H (or Hadamard) gate. It changes states |0> and |1> and creates two new states in between them:

$$H|0\rangle=|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$$
$$H|1\rangle=|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

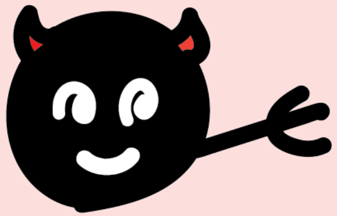
And some other commonly used gates:

$$S = \sqrt[2]{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$ Rotates about z-axis by 90°

$$T = \sqrt[4]{Z} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$ Rotates about z-axis by 45°

$$R8 = \sqrt[8]{Z} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$ Rotates about z-axis by 22.5°

But these are all for a single qubit. What about gates for multiple qubits?



CONTROL QUBIT:
YOU STAY THE SAME IF I'M $|0\rangle$;
YOU CHANGE IF I'M $|1\rangle$.

TARGET QUBIT:
OKAY~

2020.4.20.

PRESERVE

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

A 4X4 MATRIX

SWITCH

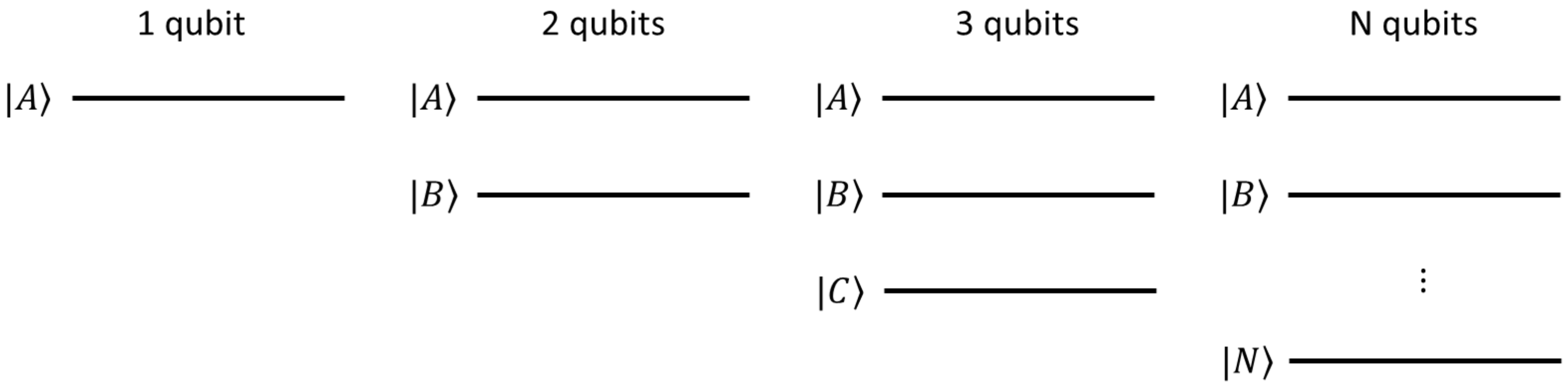
The controlled-not gate manipulates the target qubit based on the state of the control qubit.

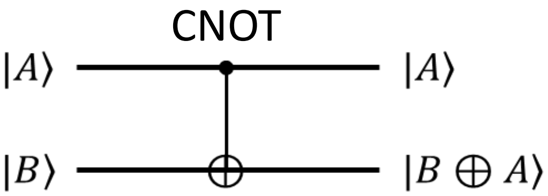
$CNOT|00\rangle = |00\rangle$
$CNOT|01\rangle = |01\rangle$
$CNOT|10\rangle = |11\rangle$
$CNOT|11\rangle = |10\rangle$

TRY THE MATH!

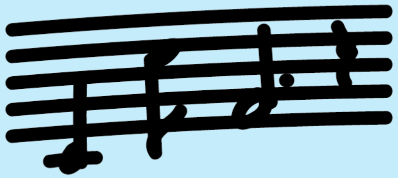
There are other controlled gates for multiple qubits you should look up.
We highlight CNOT as it will be used in every(?) algorithm (sounds familiar?!)

Circuit representation



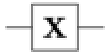
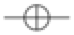
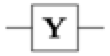
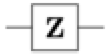
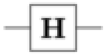
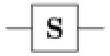
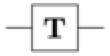
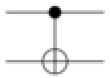
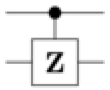
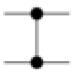
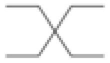
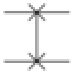
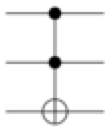


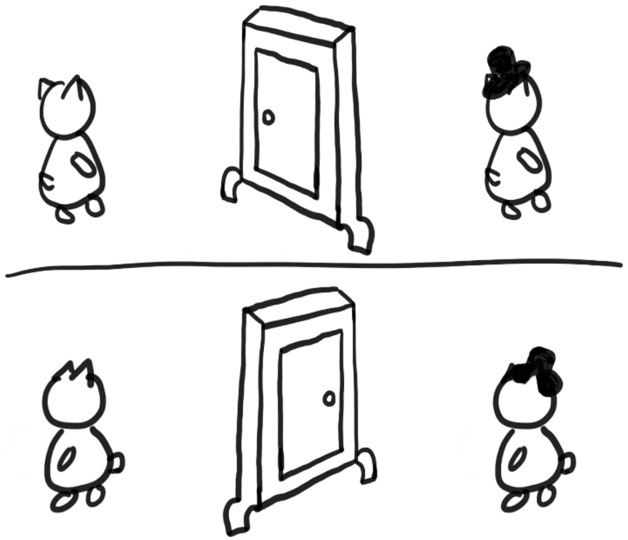
Target B controlled by A



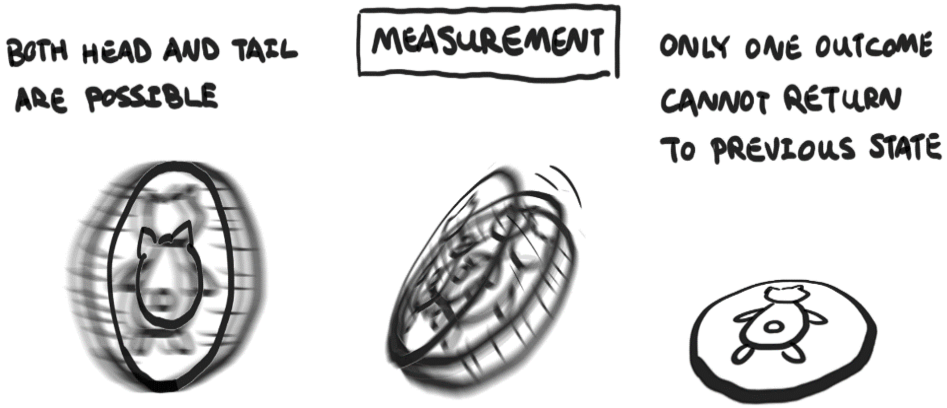
The Bloch sphere is no longer useful when we look at more than one qubit. But we have another graphic representation to use for multi-qubit systems.

Similar to how the lines in music scores denote the time-evolving music, we can use lines to represent the time-evolving qubit states:

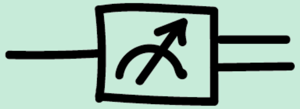
Operator	Gate(s)		Matrix
Pauli-X (X)			$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)			$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)			$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)			$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, 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)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$



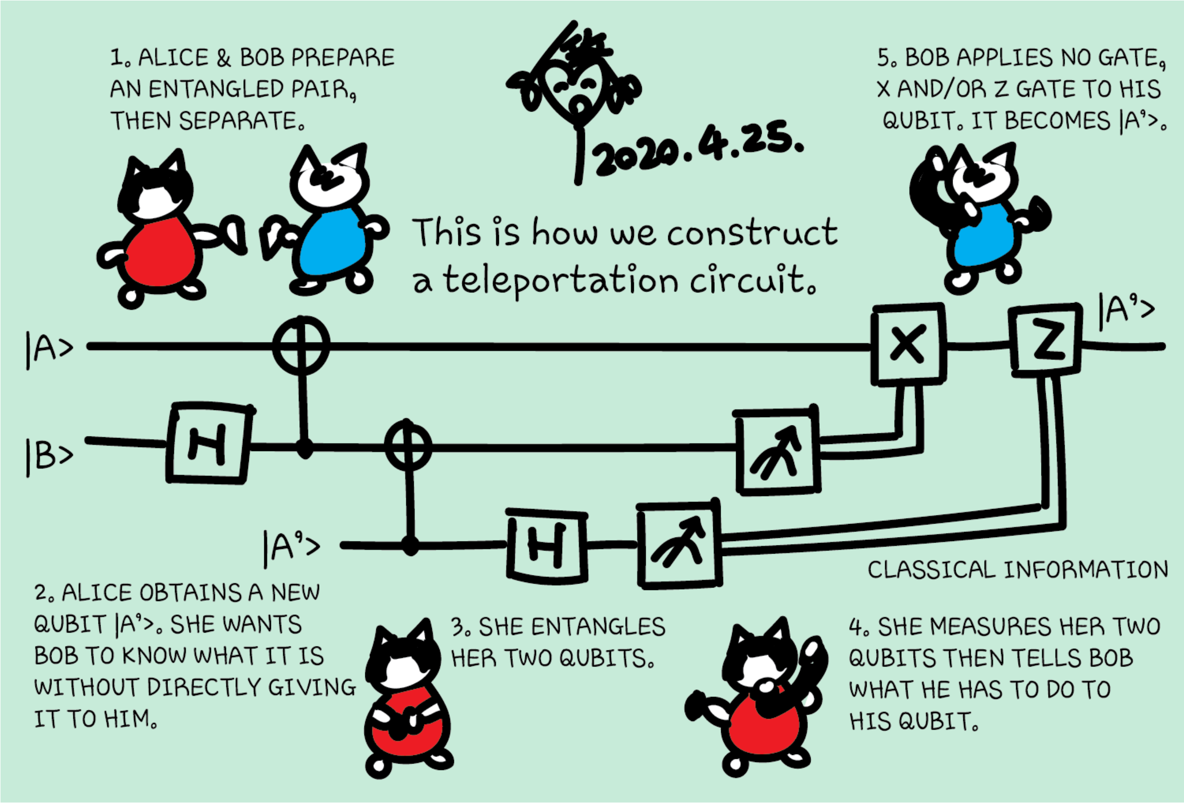
Reversible



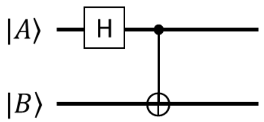
Not reversible



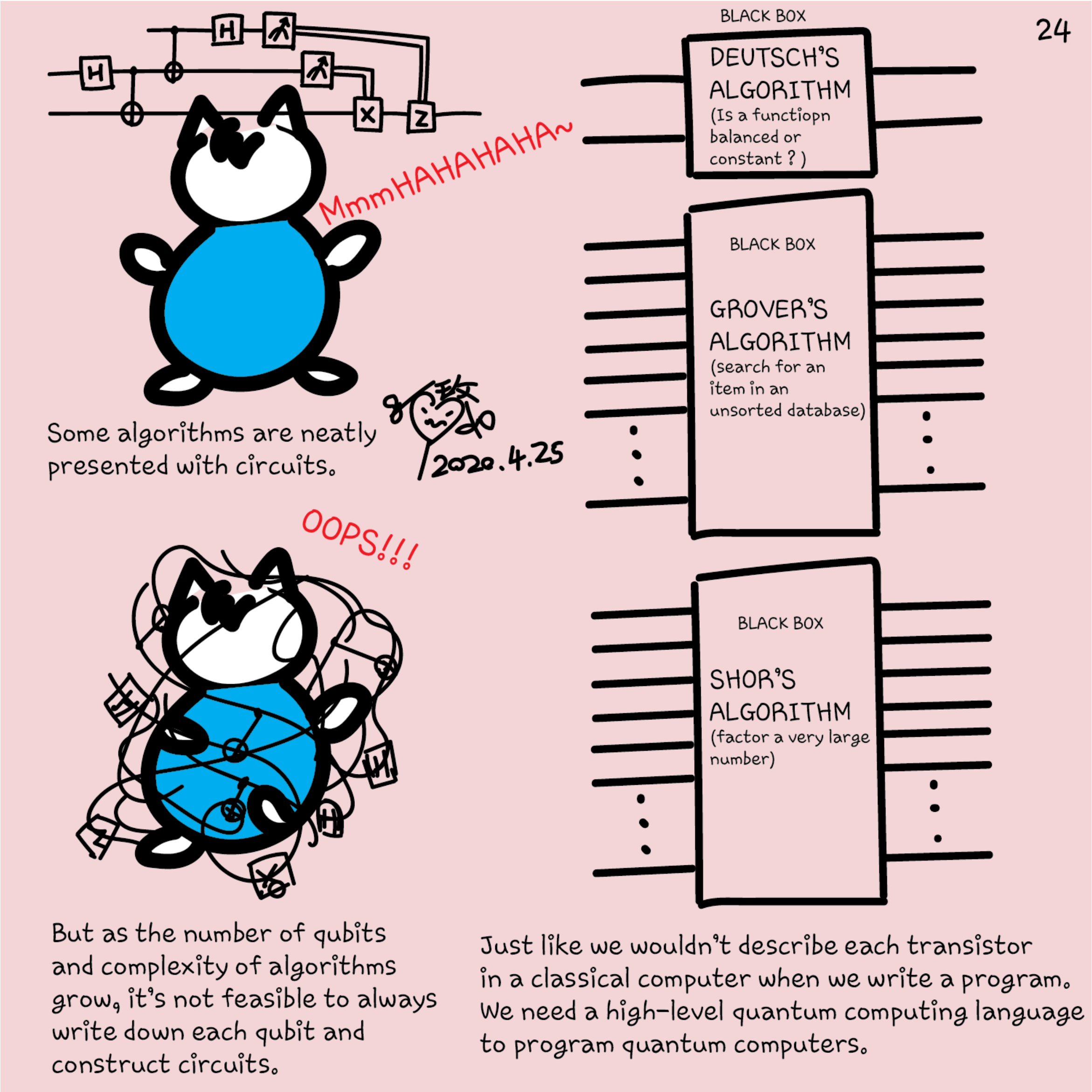
This is the circuit representation for measurement. It is not a gate. The output is a classical result, denoted by a double line.



First two qubits	Third qubit	Alice tells Bob to
00	$[\alpha\|0\rangle + \beta\|1\rangle]$	do nothing
01	$[\alpha\|1\rangle + \beta\|0\rangle]$	apply X
10	$[\alpha\|0\rangle - \beta\|1\rangle]$	apply Z
11	$[\alpha\|1\rangle - \beta\|0\rangle]$	apply X and Z



$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

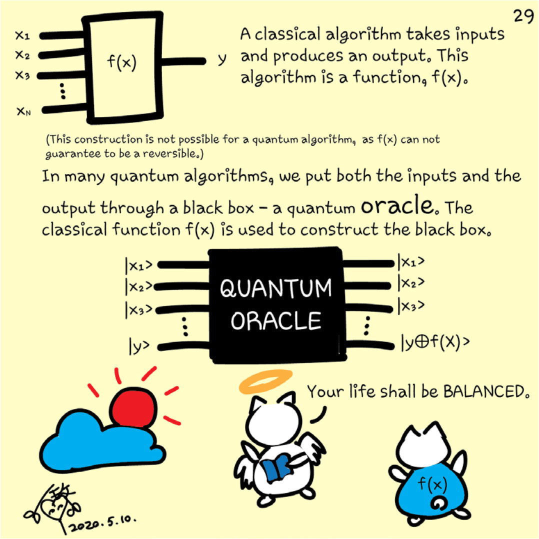

24
MmmHAHAHAHA~
Some algorithms are neatly presented with circuits.
2020.4.25
BLACK BOX
DEUTSCH'S ALGORITHM
(Is a functiopn balanced or constant ?)
BLACK BOX
GROVER'S ALGORITHM
(search for an item in an unsorted database)
OOPS!!!
BLACK BOX
SHOR'S ALGORITHM
(factor a very large number)
But as the number of qubits and complexity of algorithms grow, it's not feasible to always write down each qubit and construct circuits.
Just like we wouldn't describe each transistor in a classical computer when we write a program.
We need a high-level quantum computing language to program quantum computers.

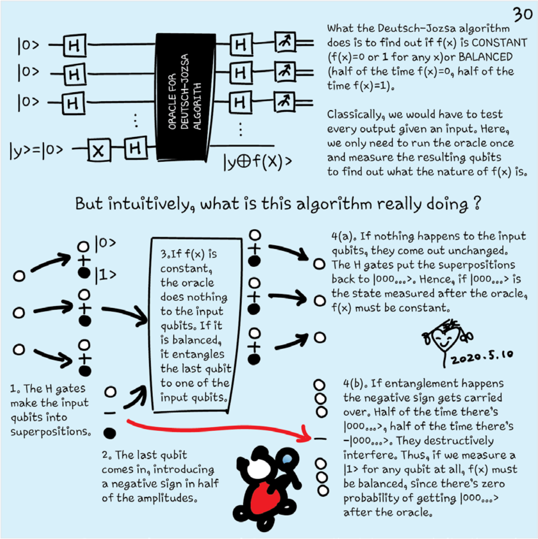
Quantum Algorithms

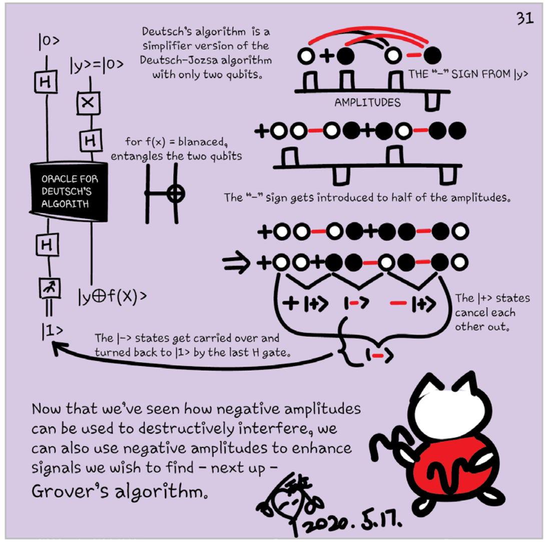
Performing calculations based on the laws of quantum mechanics

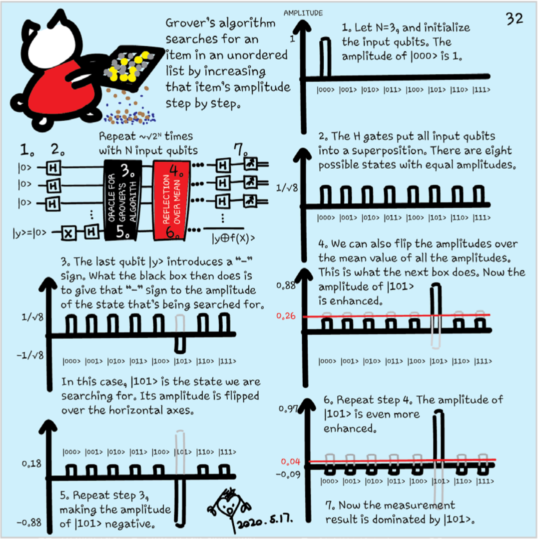
- 1980 & 1982: Manin & Feynman proposed the idea of creating machines based on the laws of quantum mechanics
- 1985: David Deutsch developed Quantum Turing machine, showing that quantum circuits are universal
- 1994: Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time
- 1997: Grover developed a quantum search algorithm with $O(\sqrt{N})$ complexity

Quantum algorithms









Class structure

- Comics on Hackaday – Introduction to Quantum Computing
every Wed & Sun

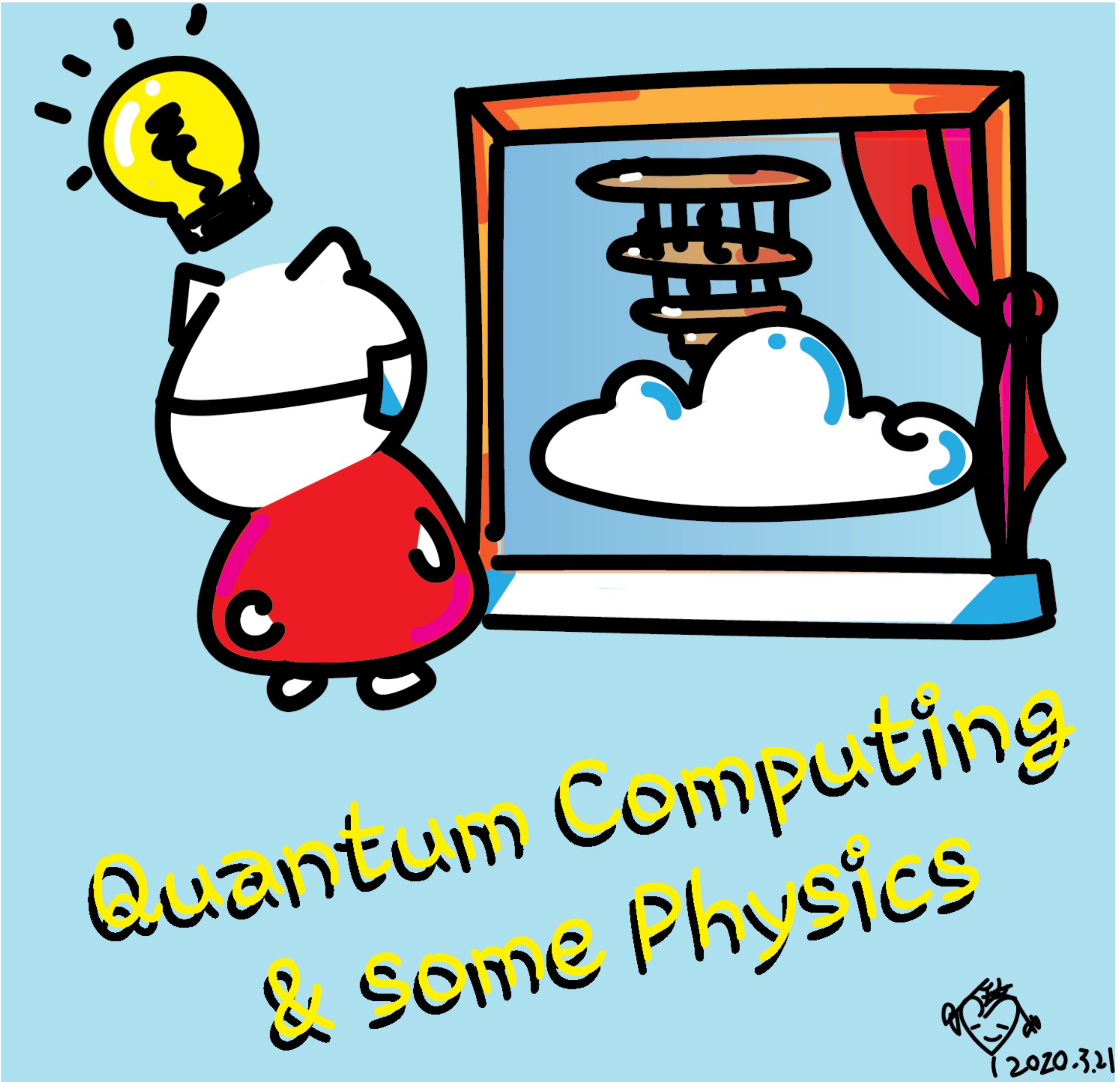
- 30 mins every Sun, one concept (theory, hardware, programming), Q&A

- Contribute to Q# documentation http://docs.microsoft.com/quantum

- Coding through Quantum Katas
- https://github.com/Microsoft/QuantumKatas/

- Discuss in Hackaday project comments
- throughout the week

- Take notes

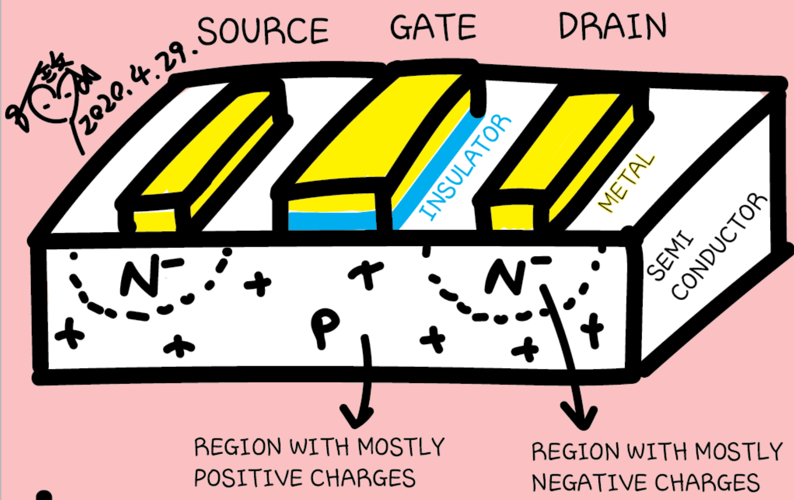


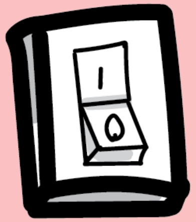
For certificate 1

- Complete any one quantum kata
- Take a screenshot or photo
- Post on Twitter or LinkedIn
- Tag the following
- **Twitter:** @KittyArtPhysics @MSFTQuantum @QSharpCommunity #QSharp #QuantumComputing #comics #physics
- **LinkedIn:** @Kitty Y. M Yeung #MSFTQuantum #QSharp #QuantumComputing #comics #physics

We leverage various properties of materials to make computing hardware.

The gate applies voltage to control the electron flow from source to drain of a transistor. At a certain gate voltage level, electrons flow. This is the "on" state which we call "1". When there's no electron flow, we say the transistor is "off", or "0".

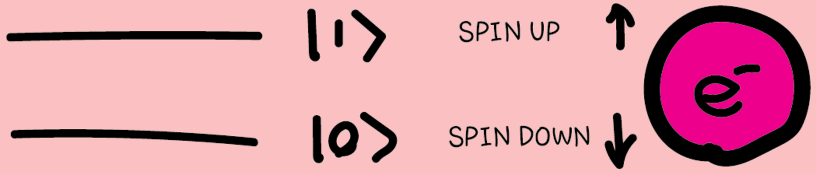




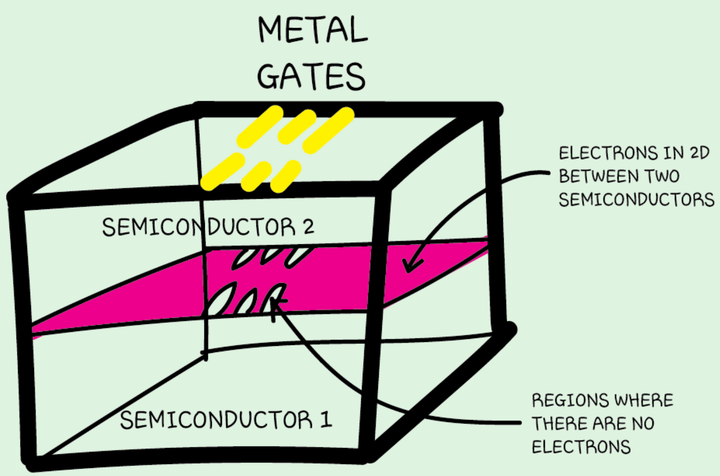
Transistors are nano- to micrometer switches.

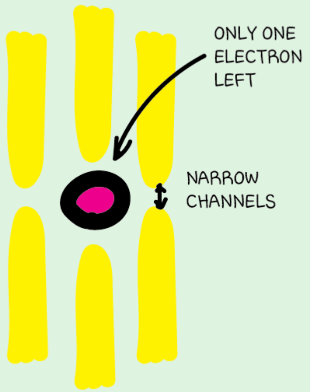
To make a qubit, we need a system with two states that can be in superposition.

The electron spin seems to be a natural candidate.

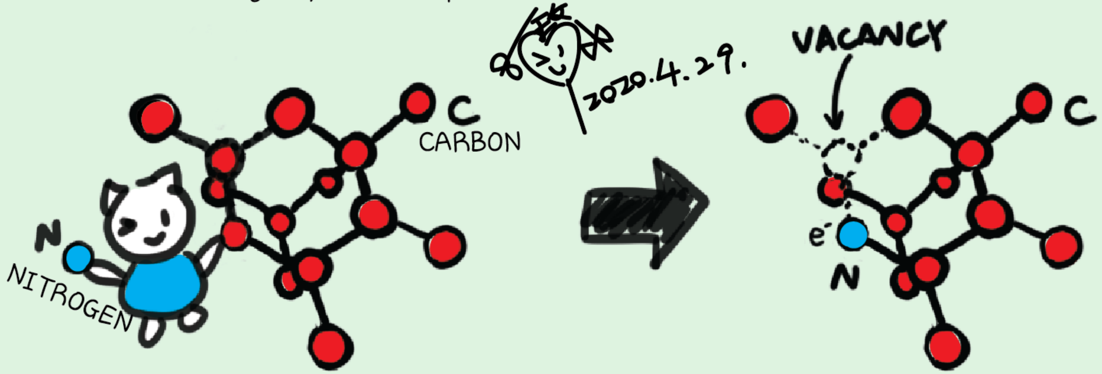


But how do we isolate and control electrons?



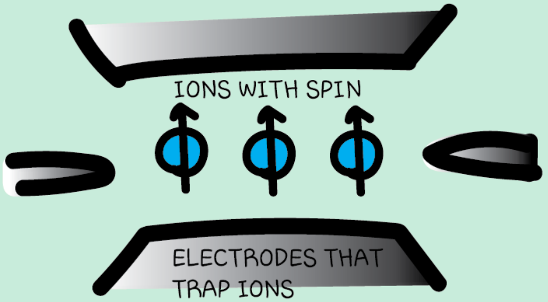


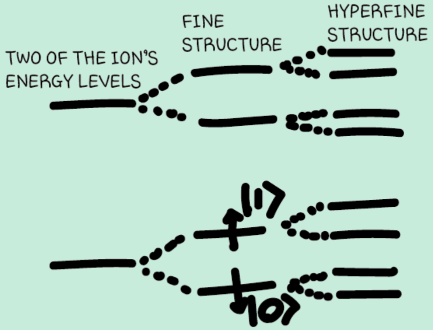
We can create a semiconductor stack. At the interface between the two semiconductors, electrons can be confined in 2D. By applying a gate voltage, the electrons underneath are removed, until there is only one electron left in a small region, called a "quantum dot".



We can also use a crystal lattice, e.g. diamond. We can remove two carbon atoms (each has 6 electrons), replacing them with a single nitrogen atom (which has 7 electrons). The extra electron is bound to the nitrogen-vacancy region.

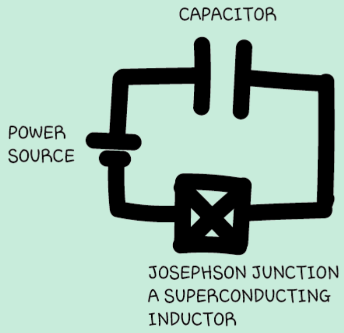
Although an electron can be conceptually the easiest qubit, it doesn't mean it is straightforward to control many electrons. There are other systems to explore.

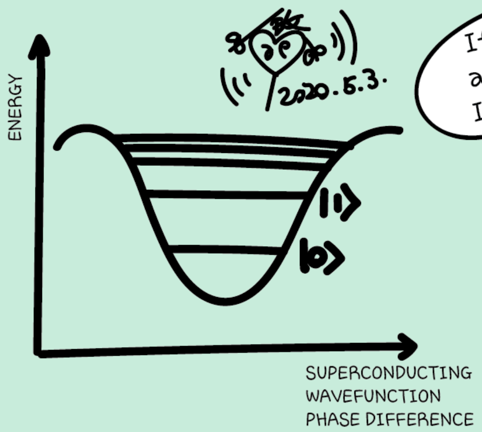




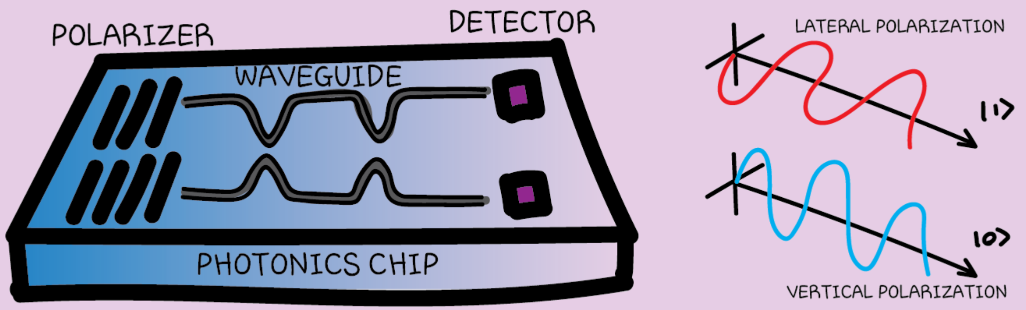
We can use two of an ion's electronic energy levels as the two qubit states. They can be the fine structure due to the ion's electron spins or the hyperfine structure due to electrons' interactions with the ion's nucleus.

We can also make an "artificial atom" and use its energy levels as qubit states, e.g. a superconducting circuit. Its oscillation creates a set of discrete energies.

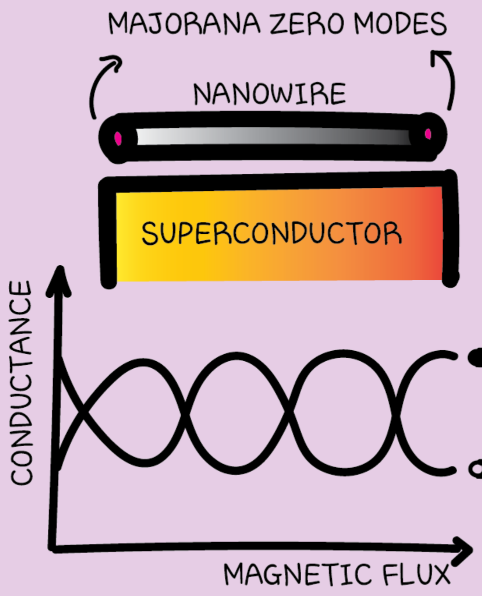




If we can use natural and artificial particles, such as electrons, ions or oscillating circuits, we can also try other types of particles and quasiparticles, and parameters other than energy levels.

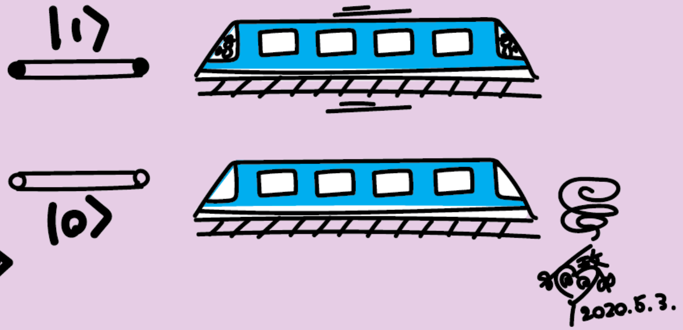


We can use photons' polarizations to encode qubit states.



Or the quasiparticles constructed in a topological material (in this case the ends of a nanowire on a superconductor).

The **zero modes** are locations that can be empty or occupied by an electron, thus giving two qubit states.



How do I learn quantum computing?

- Concepts (superposition, interference, entanglement)
- Linear algebra (matrix multiplications, complex numbers)
- Algorithms (intuition)
- Hardware (condensed matter physics)

Class structure

- Comics on Hackaday – Introduction to Quantum Computing every Wed & Sun

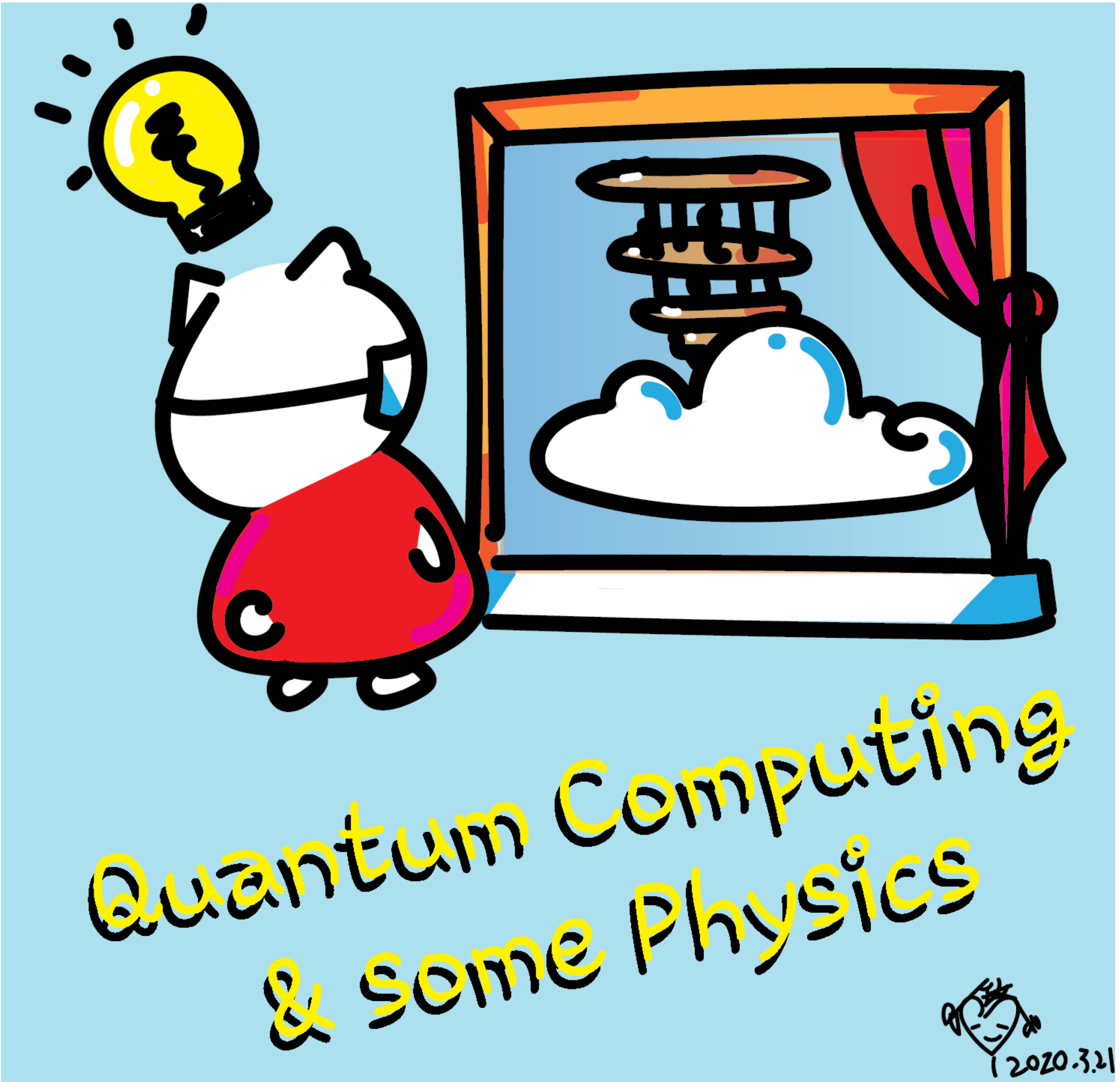
- 30 mins every Sun, one concept (theory, hardware, programming), Q&A

- Contribute to Q# documentation http://docs.microsoft.com/quantum

- Coding through Quantum Katas
- https://github.com/Microsoft/QuantumKatas/

- Discuss in Hackaday project comments
- throughout the week

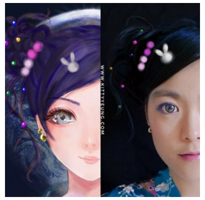
- Take notes



aka.ms/learnqc

Art by Physicist
www.kittyyeung.com

Don't blame COVID, the fashion industry needed to change for a long time



Kitty Yeung, Ph.D. Applied Physics

Creative Technologist + Sr. PM
Quantum Systems, Microsoft

Founder & Designer
Art by Physicist

- www.artbyphysicistkittyyeung.com
- @KittyArtPhysics
- @artbyphysicistkittyyeung

https://makerfaire.com/maker/entry/72417/