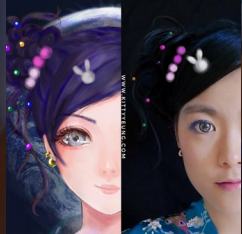


# Introduction to Quantum Computing



Kitty Yeung, Ph.D. in Applied Physics

Creative Technologist + Sr. PM  
Microsoft

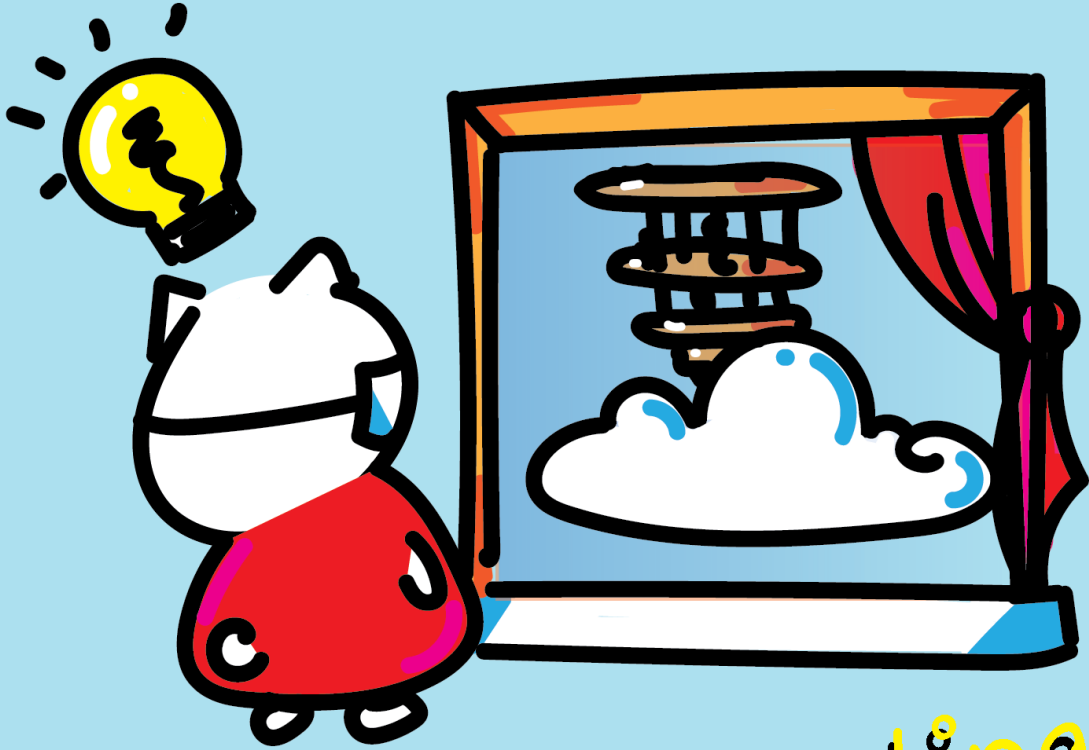
[www.artbyphysicistkittyyeung.com](http://www.artbyphysicistkittyyeung.com)

@KittyArtPhysics

@artbyphysicistkittyyeung

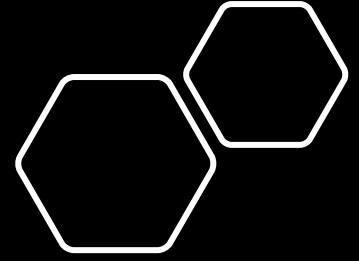


May 23, 2020



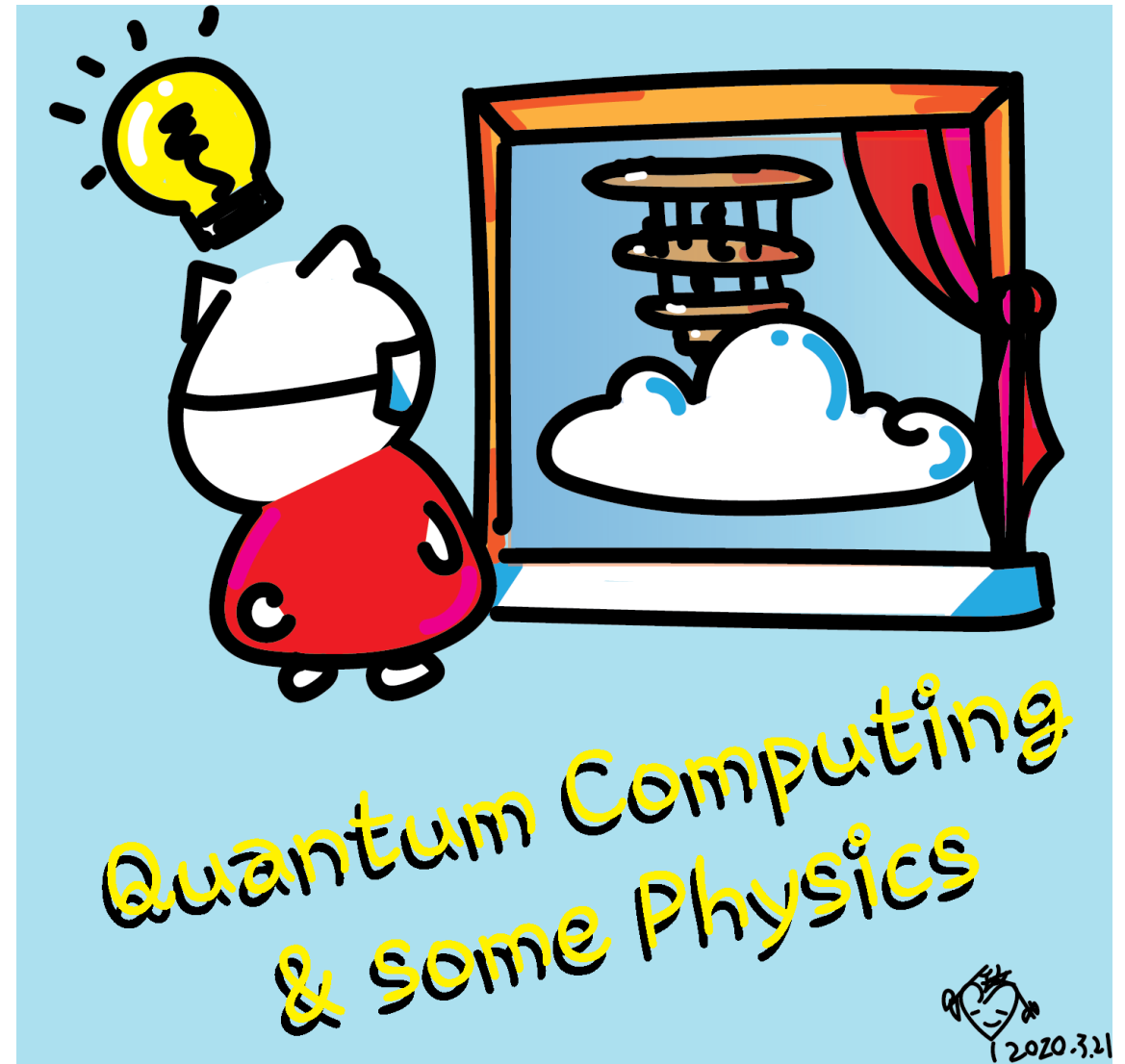
Quantum Computing  
& some Physics

 (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

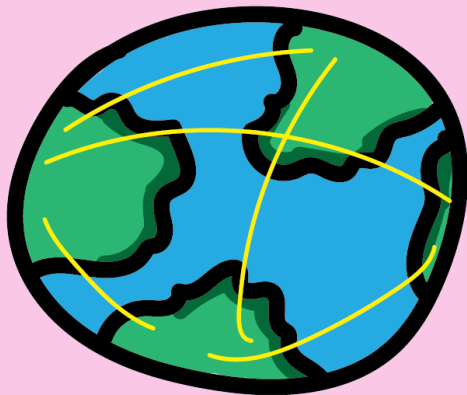


2020.3.21

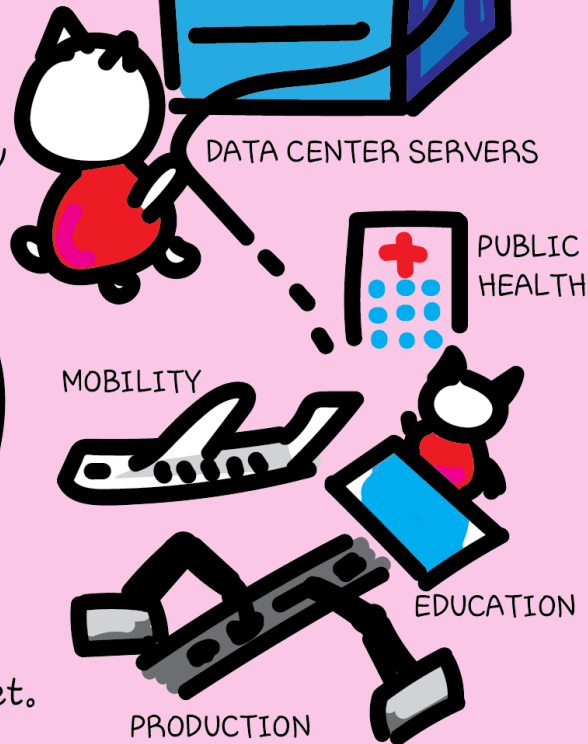
# Our world now runs on computers



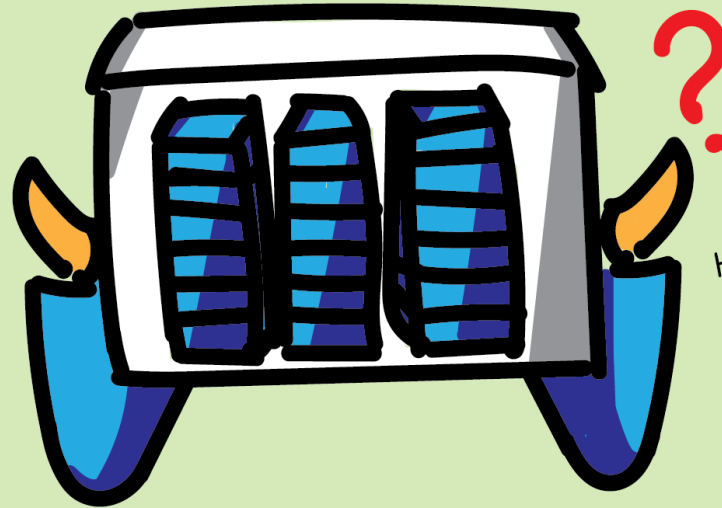
- they are machines we task to carry out work more efficiently than we ever do manually.



People and things are connected through the internet.







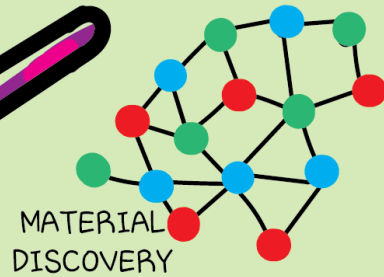
2020.3.21.

SUPERCOMPUTER  
OR  
HIGH-PERFORMANCE  
COMPUTING (HPC)  
CLUSTER

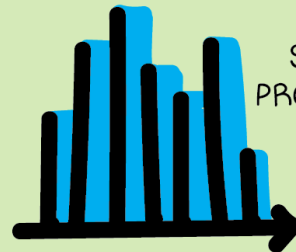
Still, for certain tasks, our most powerful computers run into fundamental limitations.



CHEMISTRY  
SIMULATION



MATERIAL  
DISCOVERY



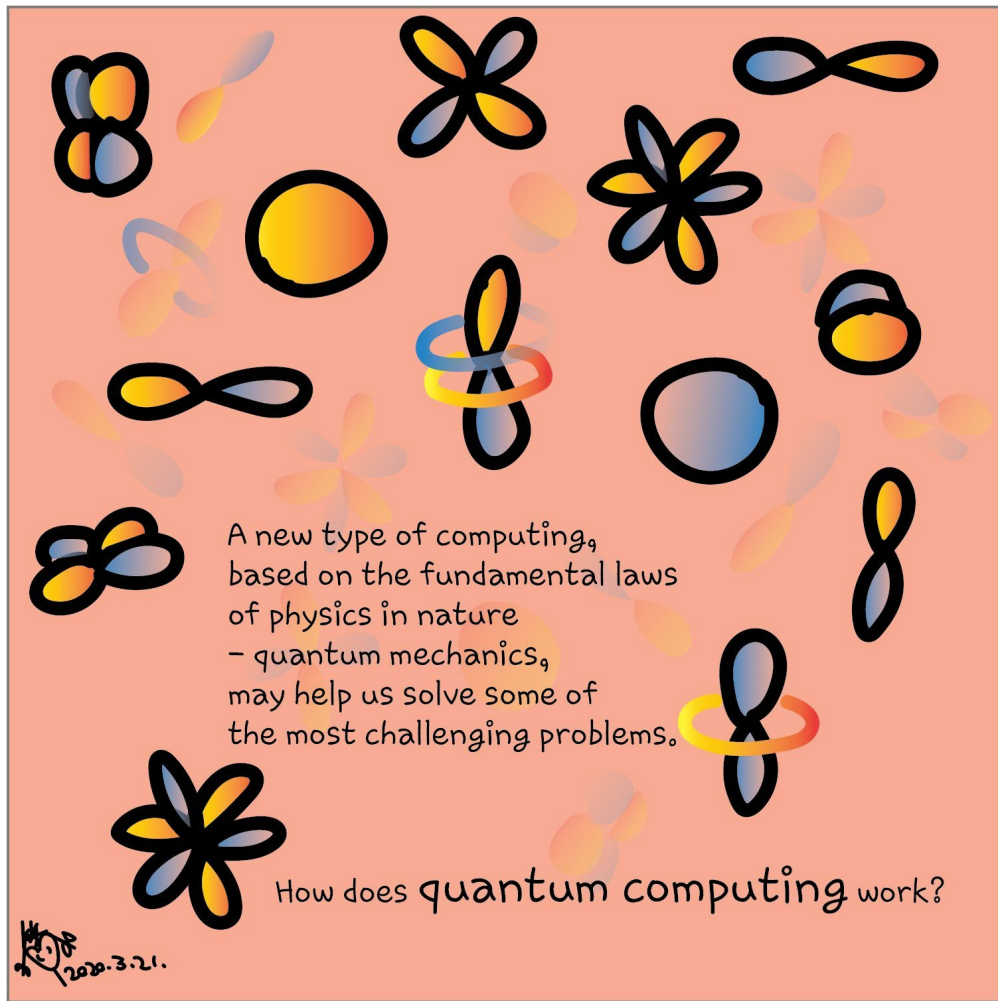
SIGNAL  
PROCESSING



LOGISTICS  
OPTIMIZATION




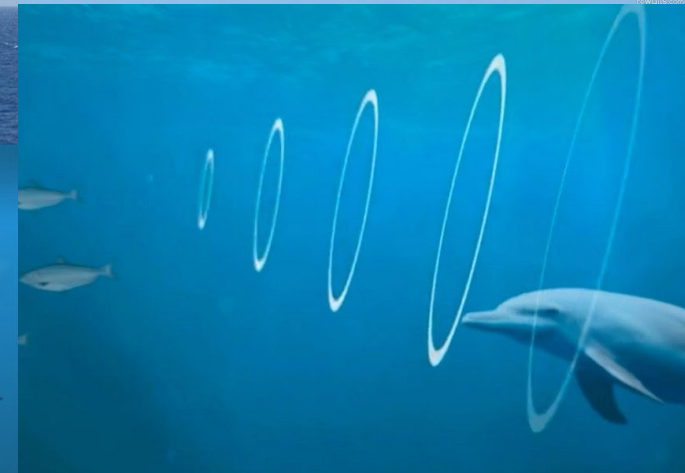
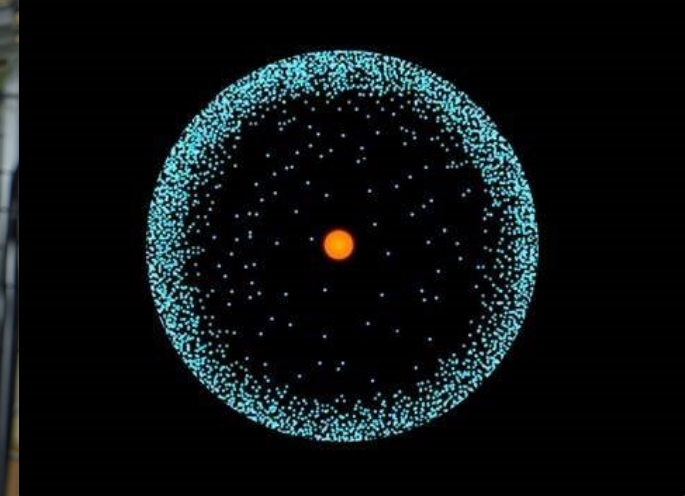
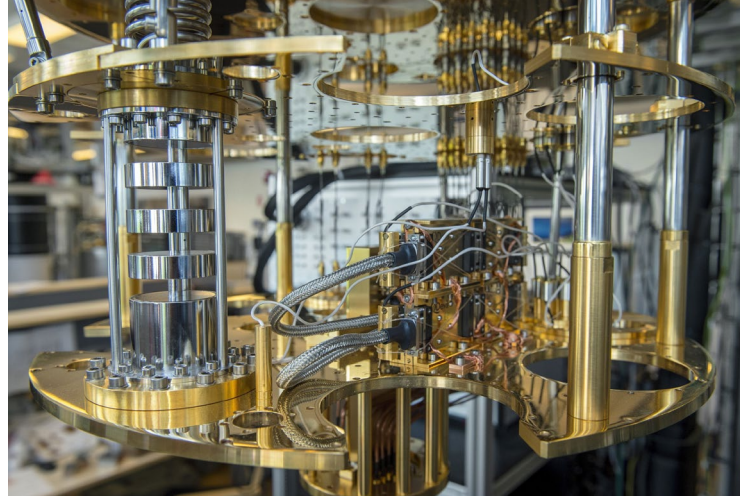
INFORMATION  
SECURITY



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.

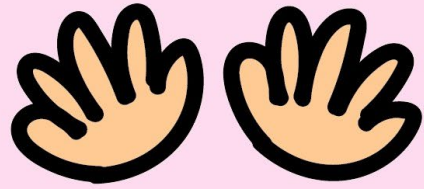




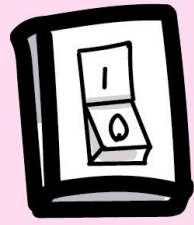
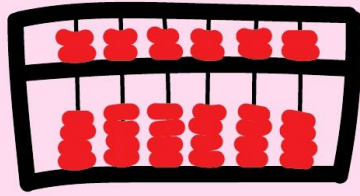
COUNT WITH 12



COUNT WITH 10

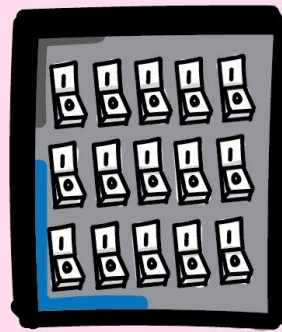


ABACUS:  
AN ANCIENT CALCULATOR

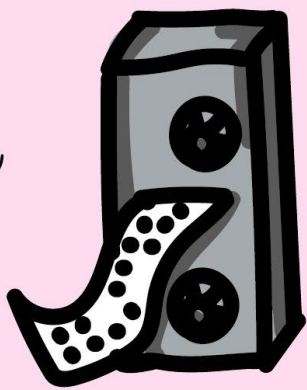


COUNT WITH 2 :  
WE CALL THEM  
A BINARY  
SYSTEM

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"



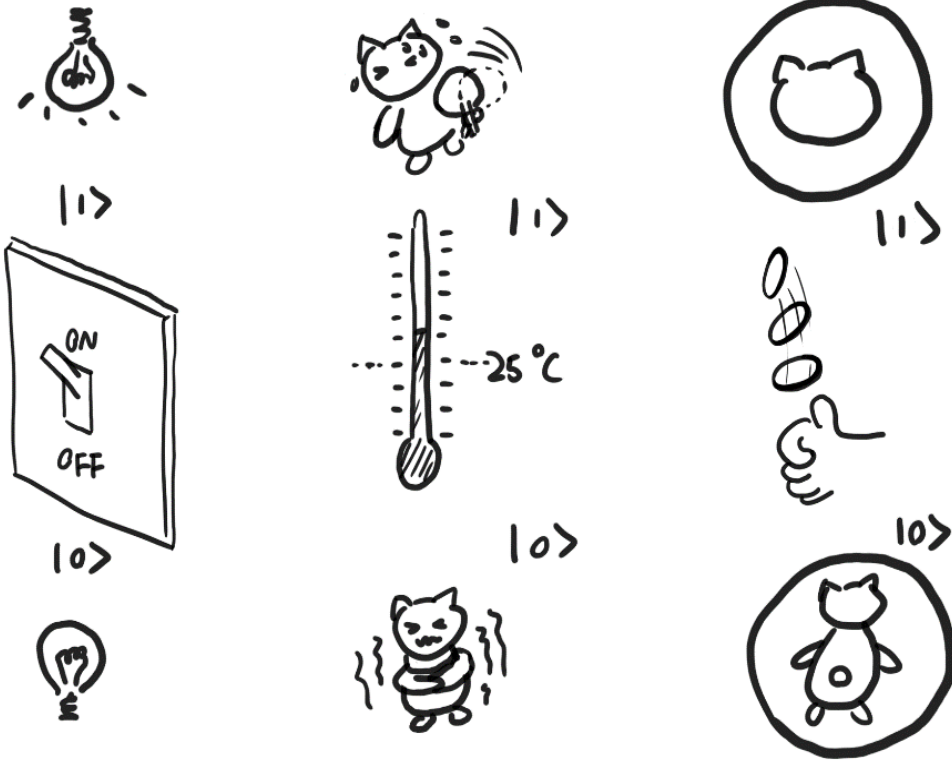
THE FIRST COMPUTERS USED PUNCH CARDS FOR PROGRAMMING

 2020.3.22.



# States – classical bits

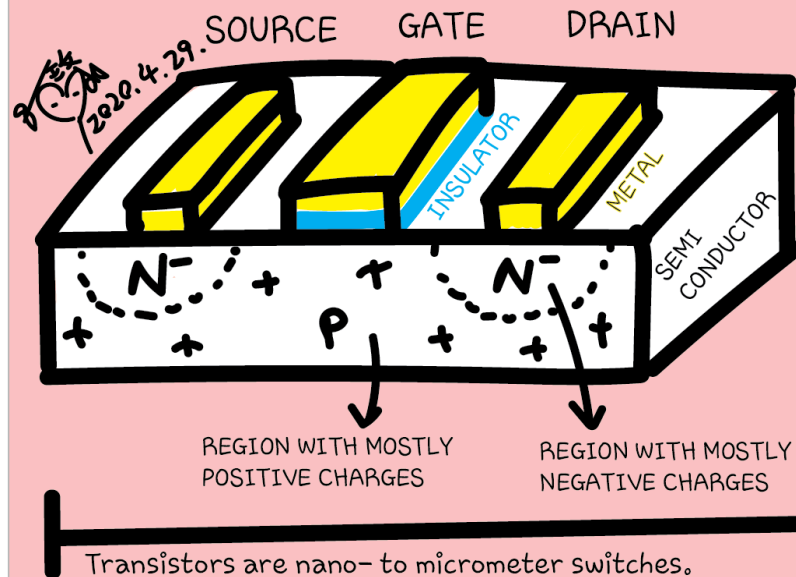
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



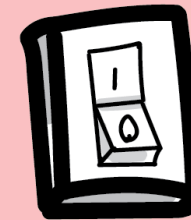


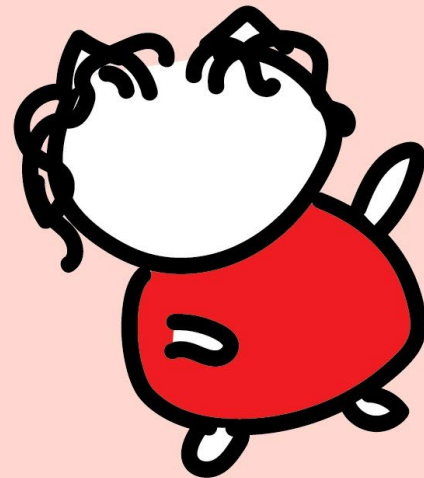
We leverage various properties of materials to make computing hardware.

25



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".



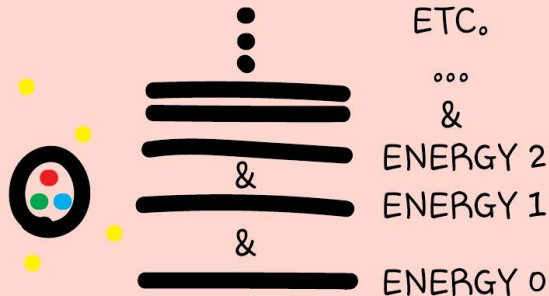


Well, it doesn't have to be this way!

$$\partial A_\mu = m^2 \phi$$
$$\partial_r = m^2 \int \phi$$



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 supersposition, while classical computing doesn't. What is it?

2020.3.25.

2020.3.28

a bit is a unit for measuring information

7

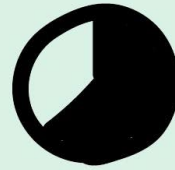
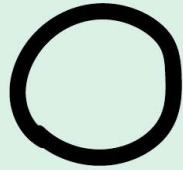
### CLASSICAL BITS

### 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



A SPINNING COIN IS LIKE A QUBIT.  
EITHER LANDING ON "HEADS" OR  
"TAILS" IS POSSIBLE  
— "HEADS" AND "TAILS"  
ARE IN SUPERPOSITION.

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = a|0\rangle + b|1\rangle$$

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



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



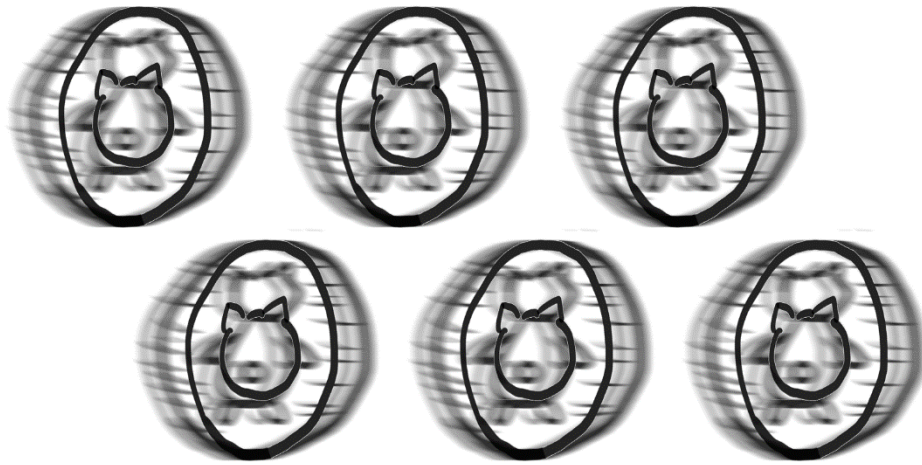
$$a^2 = 8/20$$
$$b^2 = 12/20$$



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



# Quantum bits – qubits



**MULTIPLE QUBITS.**

Two qubits:

$$\begin{aligned} |\psi\rangle &= \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} \\ &= \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \end{aligned}$$

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

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

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

CLASSICAL BITS

BIT 1      BIT 2  
**|0>**    **|1>**

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

QUANTUM BITS

QUBIT 1  
 **$a|0> + b|1>$**

a and b indicate how much of |0> and |1> are in the system

In our previous scenarios:

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

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



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



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



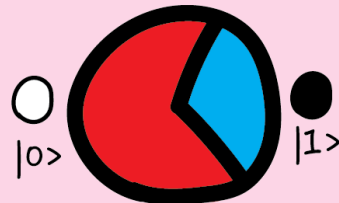
$a^2 = 50\%$   
 $b^2 = 50\%$

What do these lead to?

kk  
2020.3.28.

A qubit system is all the possible configurations in superposition.

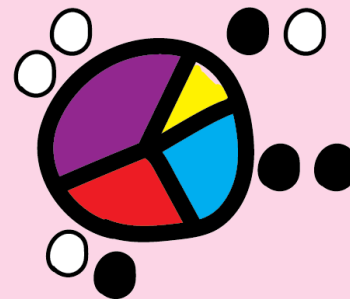
PIE CHART DENOTING PROBABILITY OF EACH CONFIGURATION



ONE QUBIT, TWO CONFIGURATIONS:

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

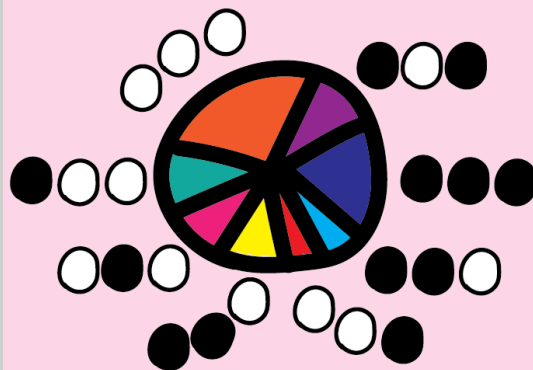
$$a^2 + b^2 = 1 \text{ (total probability adds up to 1)}$$



TWO QUBITS, FOUR CONFIGURATIONS:

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

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

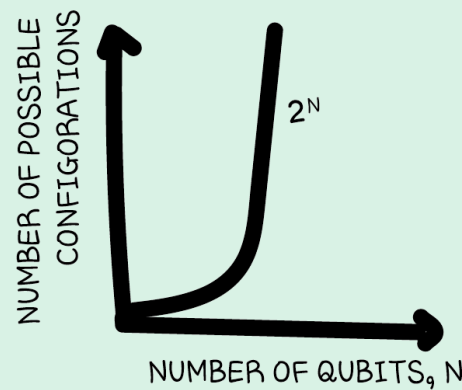


THREE QUBITS, EIGHT CONFIGURATIONS:

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

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

...  
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.

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

AN N-QUBIT STATE

EACH POSSIBLE CONFIGURATION

THIS SYMBOL MEANS SUMMING ALL N TERMS FROM 1

**NATURE DOES PLAY DICE!!!**



The amplitude  $c_i = a, b, c, d \dots n$  can be positive numbers  $1, 1/2, 1/3, 1/4 \dots n$  or negative numbers  $-1, -1/2, -1/3, -1/4 \dots n$  (these are real numbers) or imaginary numbers  $(+/-) i, 1/2i, 1/3i, 1/4i \dots ni$  or 0.

In general they can be complex numbers (with real and imaginary parts with positive or negative signs)!

What's the consequence?





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

11



AMPLITUDES CAN ADD UP =  
CONSTRUCTIVE INTERFERECE

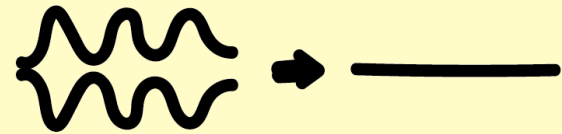


AMPLITUDES CAN CANCEL OUT =  
DESTRUCTIVE INTERFERENCE

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



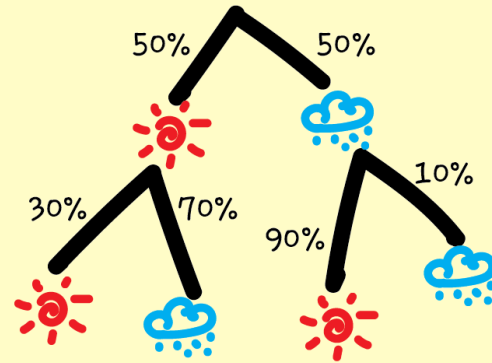
AMPLITUDES CAN ADD UP =  
CONSTRUCTIVE INTERFERECE



AMPLITUDES CAN CANCEL OUT =  
DESTRUCTIVE INTERFERECE

How likely will it be sunny the day after tomorrow?

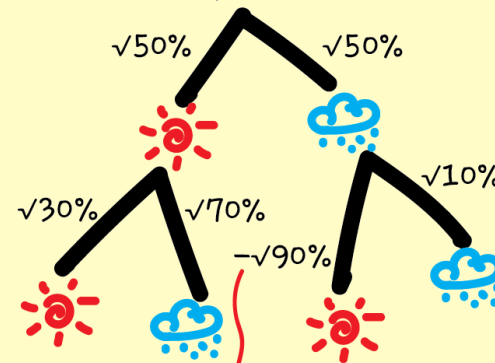
**CLASSICAL**  
USES PROBABILITY DIRECTLY



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

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.

*Handwritten signature and date*  
2020.4.4.

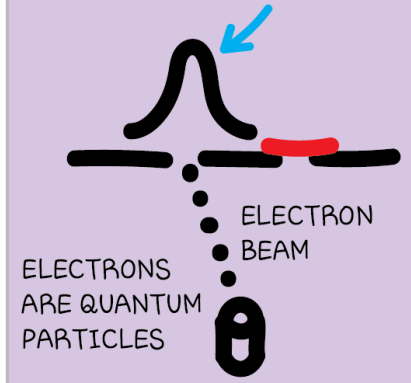


So, the things we observe (measure) are the results of interference. Possible results from constructive interference are more likely to be measured. The other possibilities cancel each other out through destructive interference.

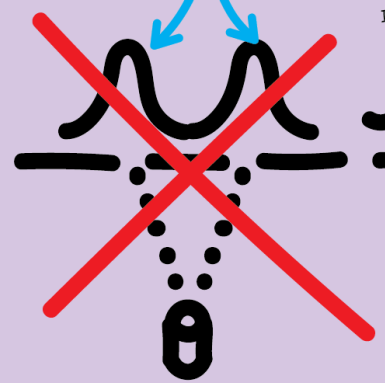
2020.4.5.

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

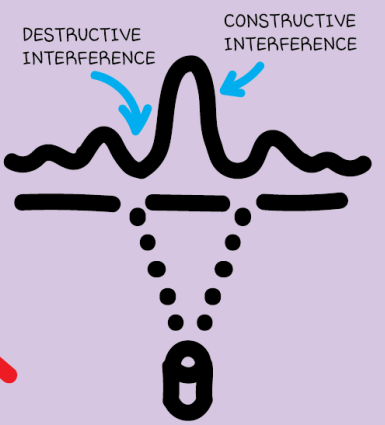
When one slit is blocked, most electrons are found here



When two slits are open, we don't see these



Instead, most electrons appear in the center



ELECTRONS ARE QUANTUM PARTICLES

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

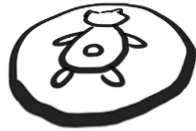
# Measurement

BOTH HEAD AND TAIL  
ARE POSSIBLE



MEASUREMENT

ONLY ONE OUTCOME  
CANNOT RETURN  
TO PREVIOUS STATE



Not reversible

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

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

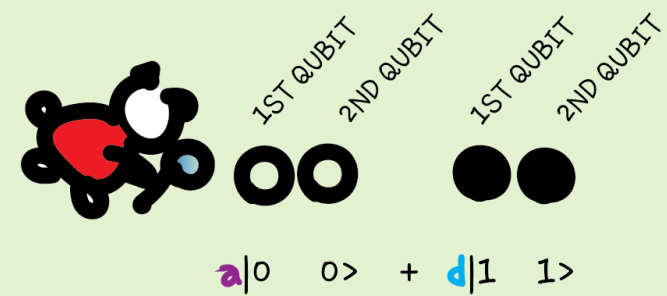
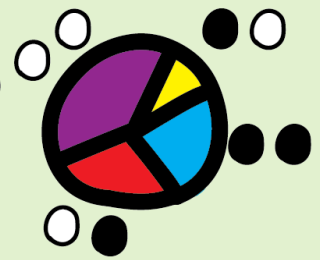
If first qubit is 0

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

After measurement

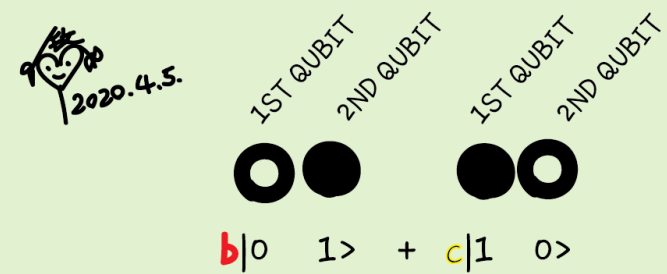


We've seen in page 9 that with two qubits, there are four possible configurations: both qubits in  $|0\rangle$ s or  $|1\rangle$ s, or one in  $|0\rangle$  with the other in  $|1\rangle$ . What if we make the  $|0\rangle|0\rangle$  case in superposition with the  $|1\rangle|1\rangle$  case? Or  $|0\rangle|1\rangle$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



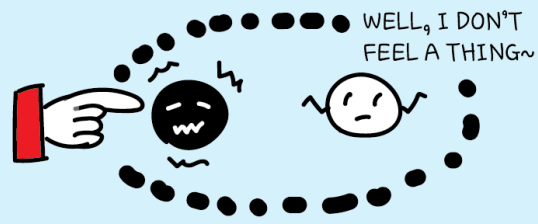
If we set the system to be in this case, we know that if we measure the first qubit and get  $|0\rangle$ , the second qubit must be in  $|0\rangle$ , without needing to measure it.

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

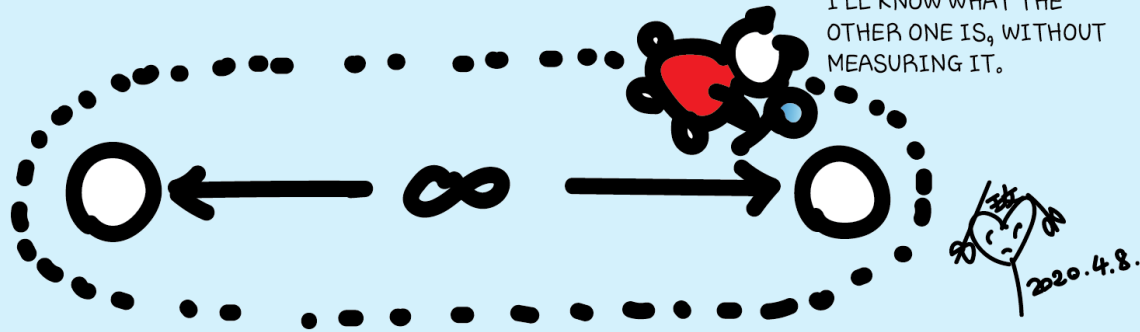


Similarly in this case, if the first qubit is  $|0\rangle$ , the second qubit must be  $|1\rangle$ . If the first is  $|1\rangle$ , the second must be  $|0\rangle$ .

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



14  
 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.

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

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

# Entanglement

Bell states

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

BY MEASURING ONE OF THE  
ENTANGLED QUBITS, I KNOW  
WHAT THE OTHER  
QUBIT WOULD BE.



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  $\frac{1}{2}$ .
2. First qubit is 1, get a state  $|\phi''\rangle = |11\rangle$  with probability  $\frac{1}{2}$ .

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.

We can use entanglement to our advantage, such as in communication or encryption.

First prepare a Bell state, e.g.  $(|01\rangle + |10\rangle)/\sqrt{2}$

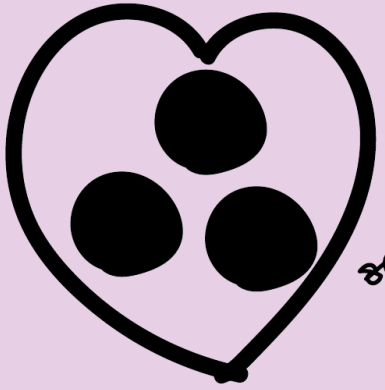
If Alice measures and gets  $|0\rangle$ , she knows Bob will get  $|1\rangle$ . If she wants him to get  $|0\rangle$ , she'll ask him to flip his qubit.



Give the 1st qubit to Alice, and the 2nd to Bob.

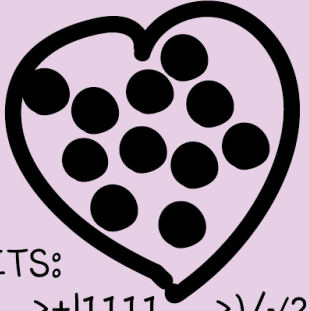


Of course, entanglement can happen between any number of qubits. The multi-qubit counterpart of Bell states are called the Greenberger-Horne-Zeilinger (GHZ) states.



THREE QUBITS:  
 $(|000\rangle + |111\rangle)/\sqrt{2}$

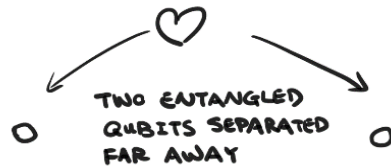
2020.4.11.



N QUBITS:  
 $(|0000\dots\rangle + |1111\dots\rangle)/\sqrt{2}$   
 $= (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$

# A common mistake

A COMMON MISTAKE ON ENTANGLEMENT :



• ) ) ) ) •  
IF ONE CHANGES THE  
OTHER ONE IMMEDIATLY CHANGES TOO

~~X~~ WRONG

INFORMATION CANNOT TRAVEL  
FASTER THAN LIGHT

SEE PHASE 3



ALICE AND BOB HAVE TO EXCHANGE CLASSICAL  
INFORMATION (SLOWER THAN LIGHT) IN THE  
CASE OF TELEPORTATION . FOR EXAMPLE .

# Encryption



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



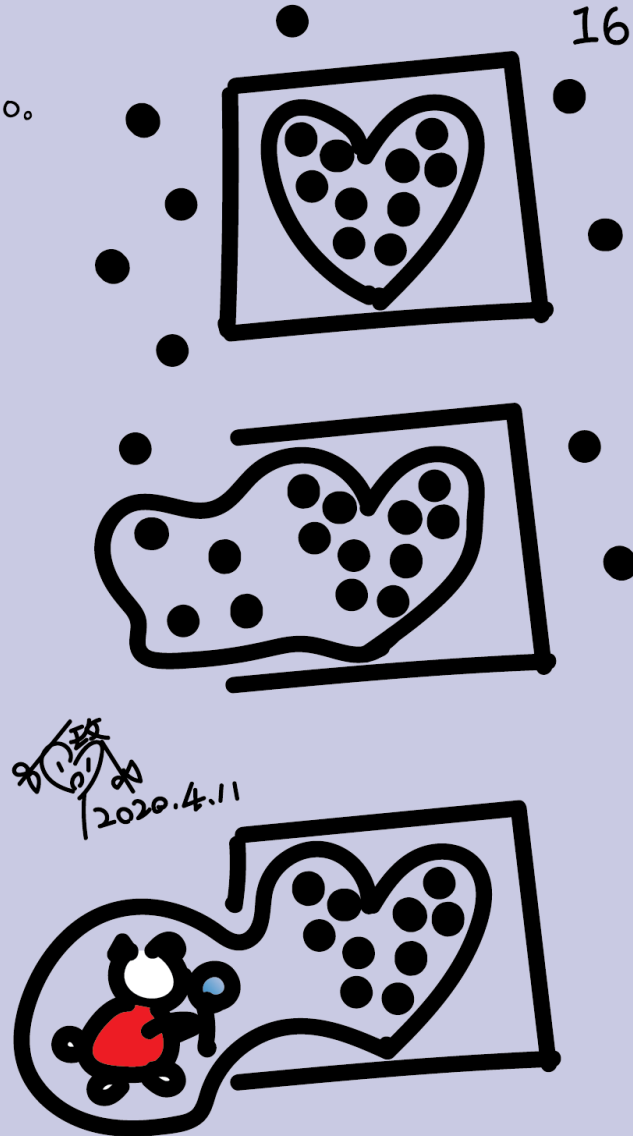
However, entanglement can be disadvantageous, too.

If the qubits are not perfectly isolated,

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

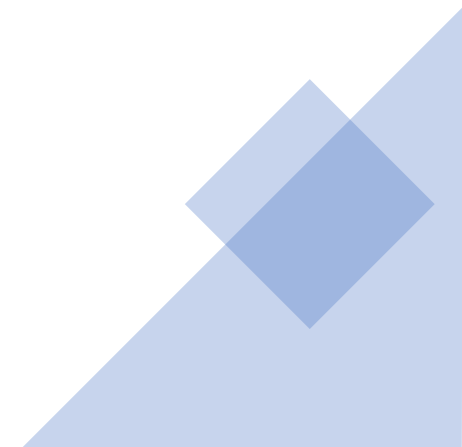
Measurements also cause decoherence, when the measuring device acts as the environment that entangles with the qubits.

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

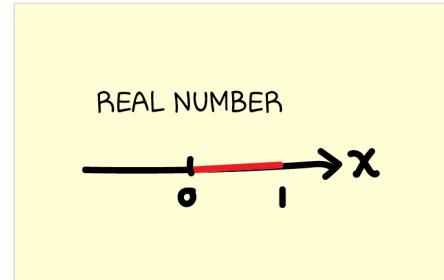




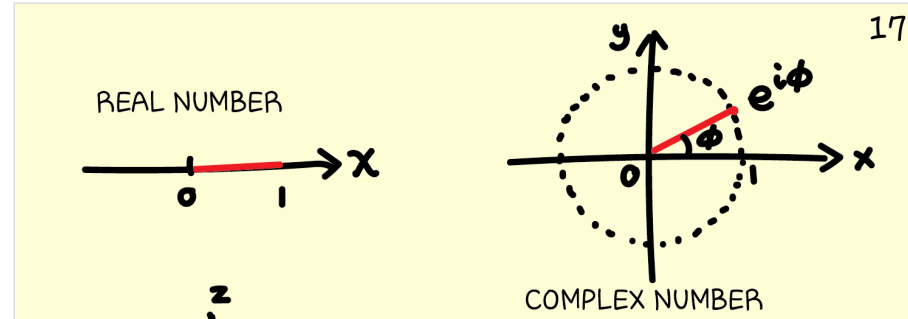
## 3 concepts

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

# Graphic representation of a qubit



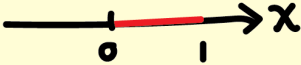
# Graphic representation of a qubit



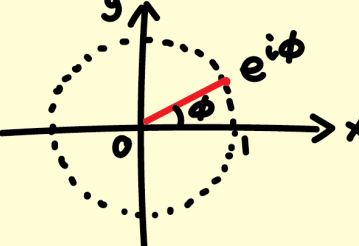
# Graphic representation of a qubit

17

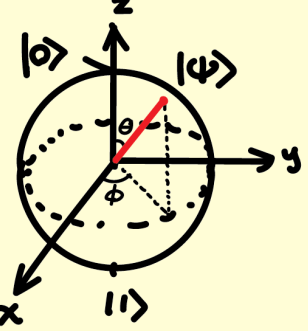
REAL NUMBER



COMPLEX NUMBER

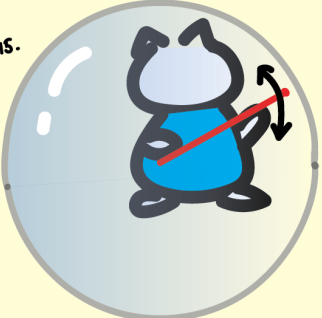


COMPLEX NUMBER



$\begin{pmatrix} a \\ b \end{pmatrix}$  VECTOR

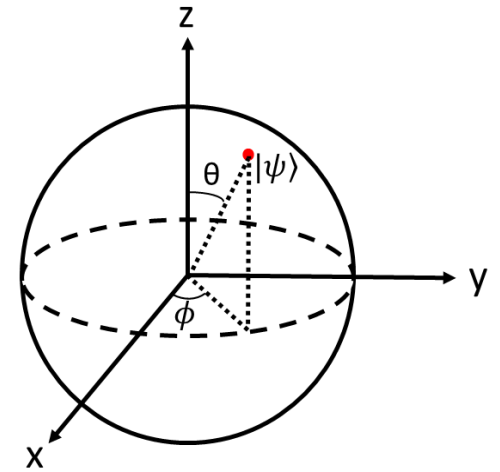
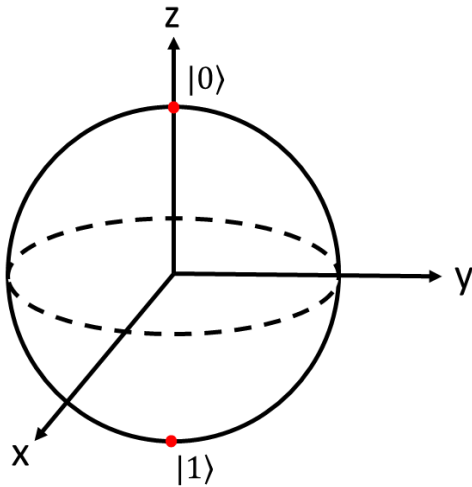
$|\Psi\rangle = \underbrace{\cos(\theta/2)}_a |0\rangle + e^{-i\phi} \underbrace{\sin(\theta/2)}_b |1\rangle$



Changing the angles of the vector in the Bloch sphere lets us manipulate the qubit and obtain any arbitrary amplitudes,  $a$  and  $b$ .

2020.4.15.

# Bloch sphere



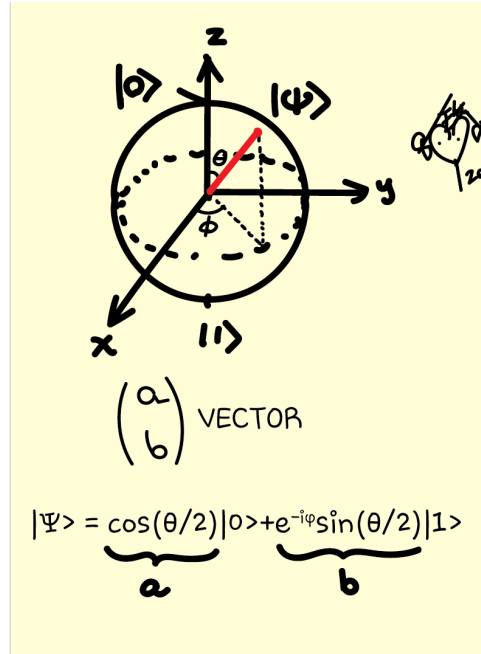
Arbitrary state

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

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



# Gates (quantum operations)



18

MATRIX THAT CHANGES $\phi$	MATRIX THAT CHANGES $\theta$	
$\begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}$	$\begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$	$\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{-i\phi}\sin\frac{\theta}{2} \end{pmatrix}$
MATRICES: GATES		VECTOR: QUBIT

MATRIX THAT  
CHANGES  $\phi$

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

MATRICES: GATES

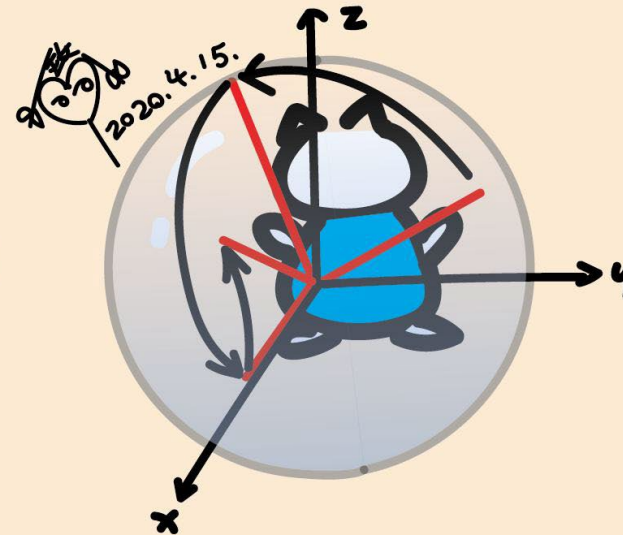
MATRIX THAT  
CHANGES  $\theta$

$$\begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

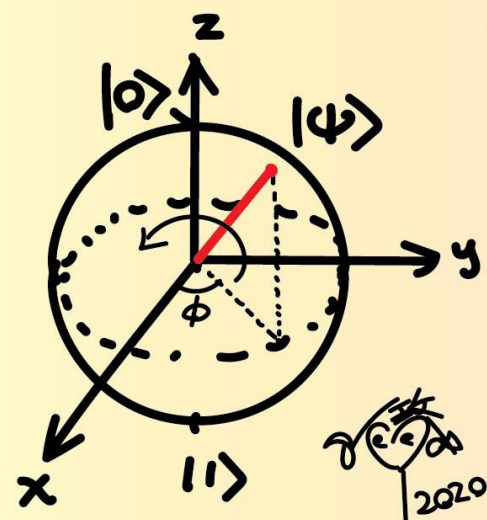
VECTOR: QUBIT



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  $\phi$ , we have a commonly used gate,  $Z$ , which rotates about the  $z$ -axis by  $180^\circ$ .

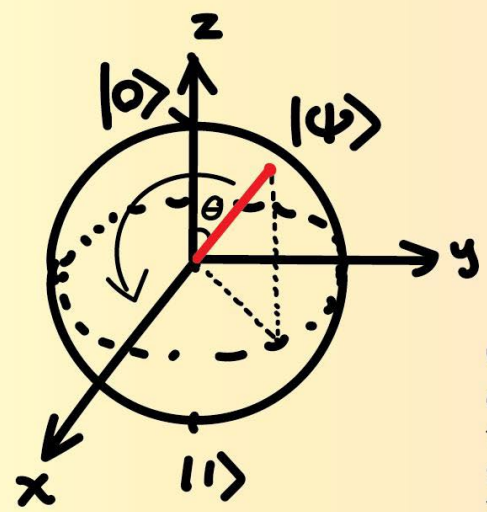
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

2020.4.18.



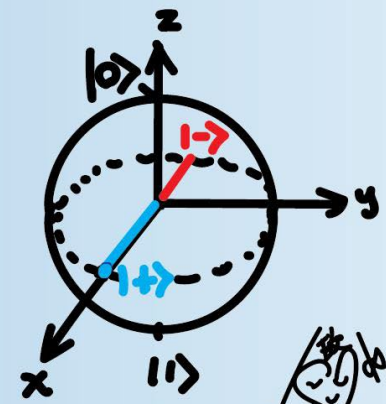
TRY THE MATH!

Similarly, the  $X$  gate rotates about the  $x$ -axis by  $180^\circ$ , rotating the angle  $\theta$  e.g.  $X|0\rangle = |1\rangle$ ,  $X|1\rangle = |0\rangle$ .



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

We have seen in page 18 the two matrices for changing  $\phi$  and  $\theta$  in arbitrary 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.



*2020.4.18*

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

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

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

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

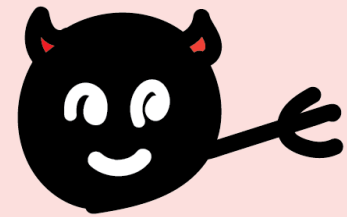
And some other commonly used gates:

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

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

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

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



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



TARGET QUBIT :  
OKAY~

~~2020.4.20~~  
2020.4.20.

**CNOT** =

A 4x4 MATRIX

1	0	0	0
0	1	0	0
0	0	0	1
0	0	1	0

PRESERVE (top two rows)  
SWITCH (bottom two rows)

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

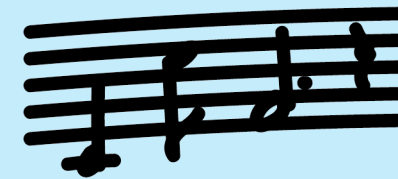
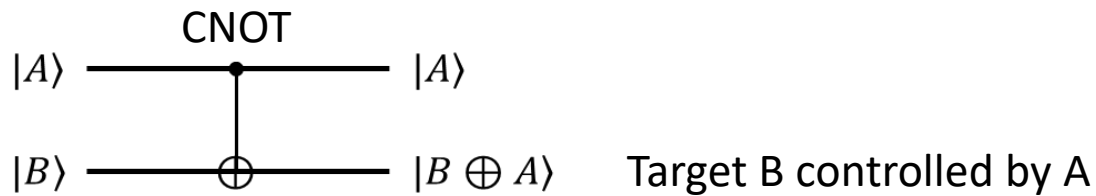
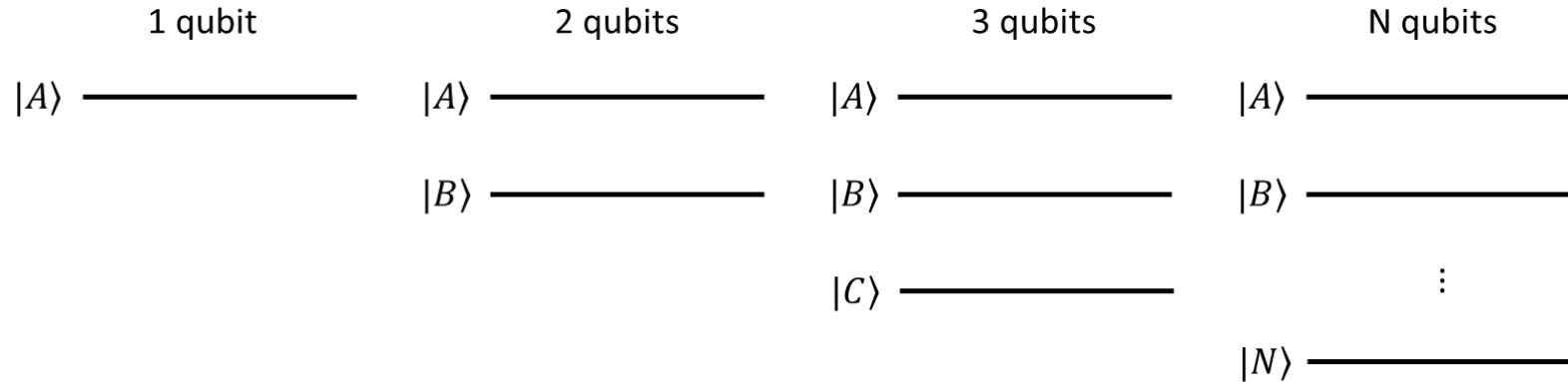
- CNOT|00>=|00>
- CNOT|01>=|01>
- CNOT|10>=|11>
- CNOT|11>=|10>



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?!)

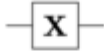

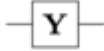
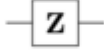
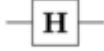
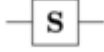
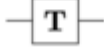
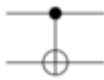
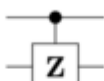



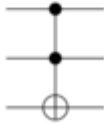
# Circuit representation

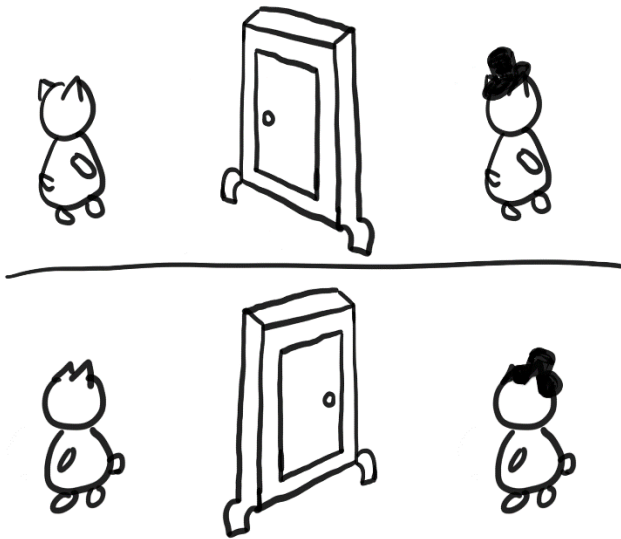


The Bloch sphere is no longer <sup>22</sup> useful when we look at more than one qubit. But we have another graphic representation to use for multi-qubit systems.

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)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

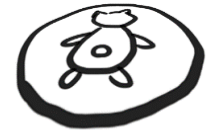


Reversible

BOTH HEAD AND TAIL  
ARE POSSIBLE

MEASUREMENT

ONLY ONE OUTCOME  
CANNOT RETURN  
TO PREVIOUS STATE



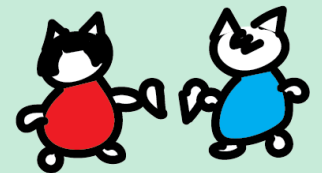
Not reversible



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

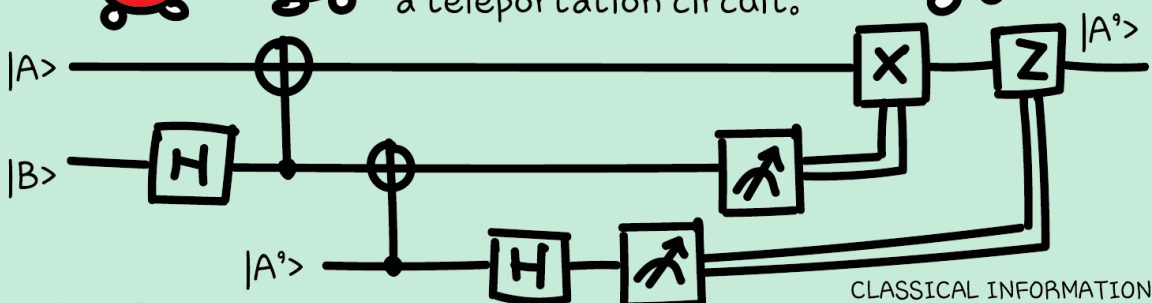
2020.4.25.

1. ALICE & BOB PREPARE AN ENTANGLED PAIR, THEN SEPARATE.



This is how we construct a teleportation circuit.

5. BOB APPLIES NO GATE, X AND/OR Z GATE TO HIS QUBIT. IT BECOMES  $|A'\rangle$ .



2. ALICE OBTAINS A NEW QUBIT  $|A'\rangle$ . SHE WANTS BOB TO KNOW WHAT IT IS WITHOUT DIRECTLY GIVING IT TO HIM.

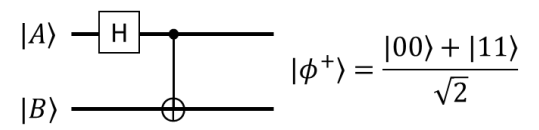


3. SHE ENTANGLES HER TWO QUBITS.



4. SHE MEASURES HER TWO QUBITS THEN TELLS BOB WHAT HE HAS TO DO TO HIS QUBIT.

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





MmmHAHAHAHA~

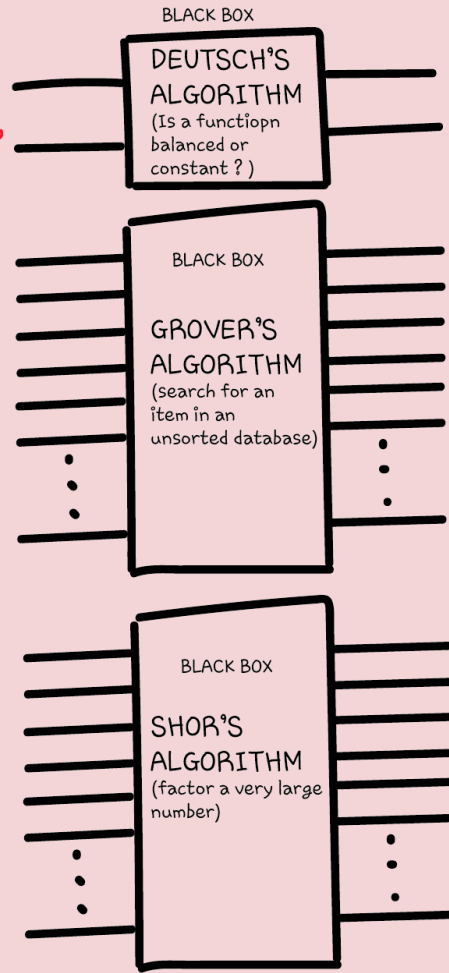
Some algorithms are neatly presented with circuits.

2020.4.25



OOPS!!!

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

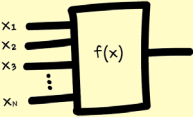


1997: Grover developed a quantum search algorithm with  $O(\sqrt{N})$  complexity



# Quantum algorithms

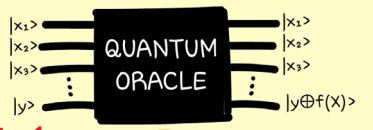
29




A classical algorithm takes inputs and produces an output. This algorithm is a function,  $f(x)$ .

(This construction is not possible for a quantum algorithm, as  $f(x)$  can not guarantee to be a reversible.)

In many quantum algorithms, we put both the inputs and the output through a black box - a quantum oracle. The classical function  $f(x)$  is used to construct the black box.

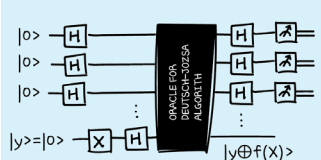


Your life shall be **BALANCED**.



2020. 5. 10.

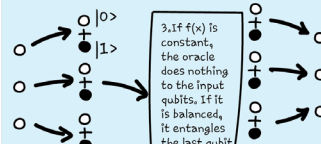
30



What the Deutsch-Jozsa algorithm does is to find out if  $f(x)$  is **CONSTANT** ( $f(x)=0$  or  $1$  for any  $x$ ) or **BALANCED** (half of the time  $f(x)=0$ , half of the time  $f(x)=1$ ).

Classically, we would have to test every output given an input. Here, we only need to run the oracle once and measure the resulting qubits to find out what the nature of  $f(x)$  is.

But intuitively, what is this algorithm really doing?



1. The H gates make the input qubits into superpositions.

2. The last qubit comes in, introducing a negative sign in half of the amplitudes.

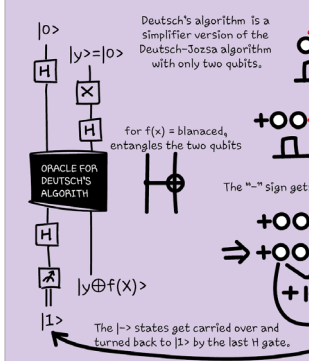
3. If  $f(x)$  is constant, the oracle does nothing to the input qubits. If it is balanced, it entangles the last qubit to one of the input qubits.

4(a). If nothing happens to the input qubits, they come out unchanged. The H gates put the superpositions back to  $|000\dots\rangle$ . Hence, if  $|000\dots\rangle$  is the state measured after the oracle,  $f(x)$  must be constant.

4(b). If entanglement happens the negative sign gets carried over. Half of the time there's  $|000\dots\rangle$ , half of the time there's  $|1000\dots\rangle$ . They destructively interfere. Thus, if we measure a  $|1\rangle$  for any qubit at all,  $f(x)$  must be balanced, since there's zero probability of getting  $|000\dots\rangle$  after the oracle.

2020. 5. 10.

31



Deutsch's algorithm is a simpler version of the Deutsch-Jozsa algorithm with only two qubits.

for  $f(x)$  = balanced, entangles the two qubits

AMPLITUDES


THE "-" SIGN FROM  $|y\rangle$

The "-" sign gets introduced to half of the amplitudes.

The  $|-\rangle$  states cancel each other out.

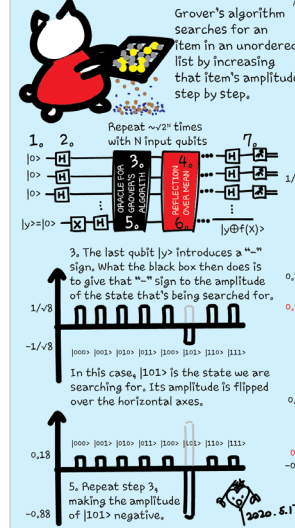
The  $|-\rangle$  states get carried over and turned back to  $|1\rangle$  by the last H gate.

Now that we've seen how negative amplitudes can be used to destructively interfere, we can also use negative amplitudes to enhance signals we wish to find - next up - Grover's algorithm.



2020. 5. 17.

32



Grover's algorithm searches for an item in an unordered list by increasing that item's amplitude step by step.

1. Let  $N=3$ , and initialize the input qubits. The amplitude of  $|000\rangle$  is 1.

2. The H gates put all input qubits into a superposition. There are eight possible states with equal amplitudes.

3. The last qubit  $|y\rangle$  introduces a "-" sign. What the black box then does is to give that "-" sign to the amplitude of the state that's being searched for.

4. We can also flip the amplitudes over the mean value of all the amplitudes. This is what the next box does. Now the amplitude of  $|101\rangle$  is enhanced.

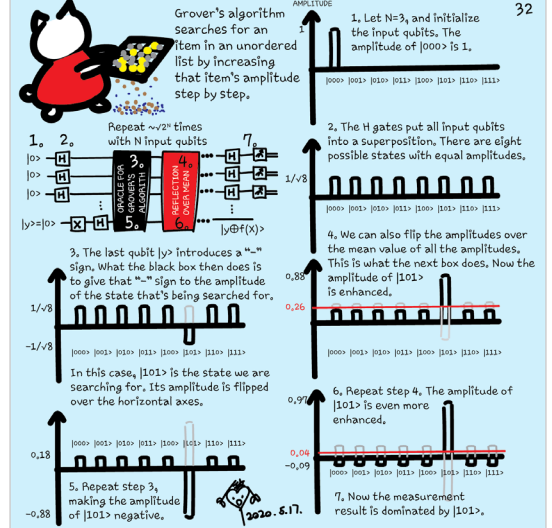
5. Repeat step 3, making the amplitude of  $|101\rangle$  negative.

6. Repeat step 4. The amplitude of  $|101\rangle$  is even more enhanced.

7. Now the measurement result is dominated by  $|101\rangle$ .

Repeat  $\sim\sqrt{2^N}$  times with  $N$  input qubits

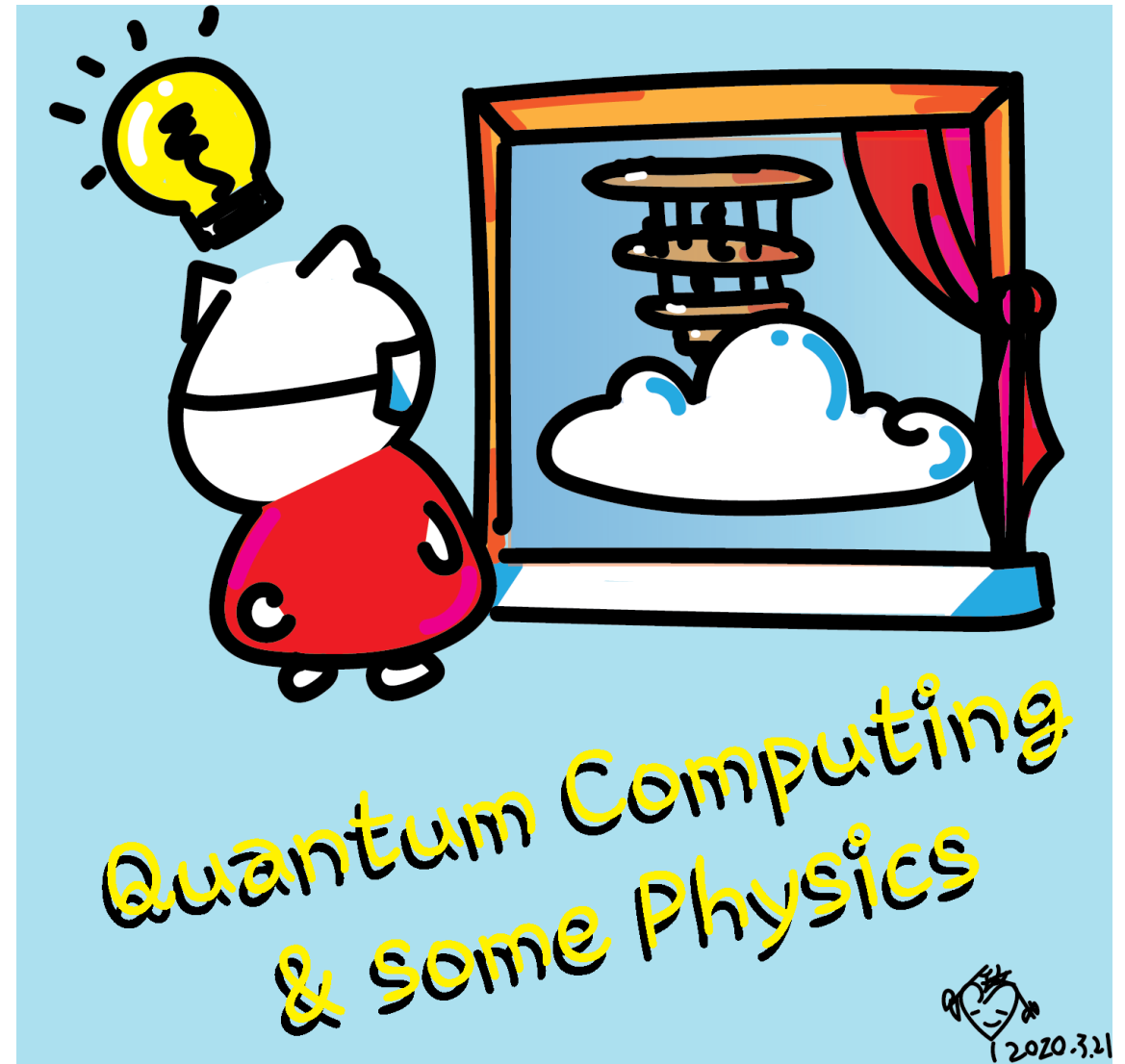
AMPLITUDE



2020. 5. 17.

# 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

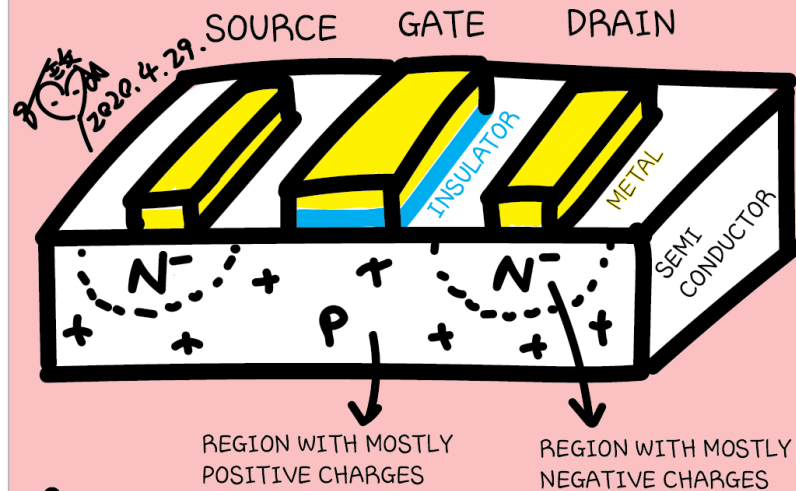


# For certificate 1

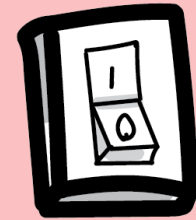
- Complete any one quantum kata
- Take a screenshot or photo
- Post on Twitter or LinkedIn
- Tag the following
- **Twitter:** @KittyArtPhysics  
@MSFTQuantum @QSharpCommunity  
#QSharp #QuantumComputing #comics  
#physics
- **LinkedIn:** @Kitty Y. M Yeung  
#MSFTQuantum #QSharp  
#QuantumComputing #comics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



We leverage various properties of materials to make computing hardware.



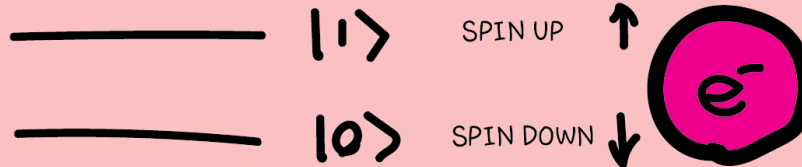
The gate applies voltage to control the electron flow from source to drain of a transistor. At a certain gate voltage level, electrons flow. This is the "on" state which we call "1". When there's no electron flow, we say the transistor is "off", or "0".



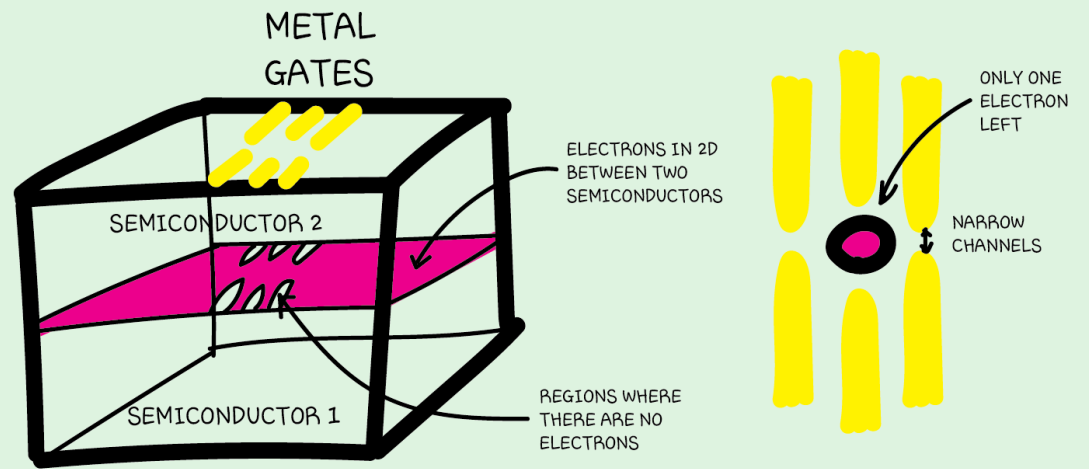
Transistors are nano- to micrometer switches.

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

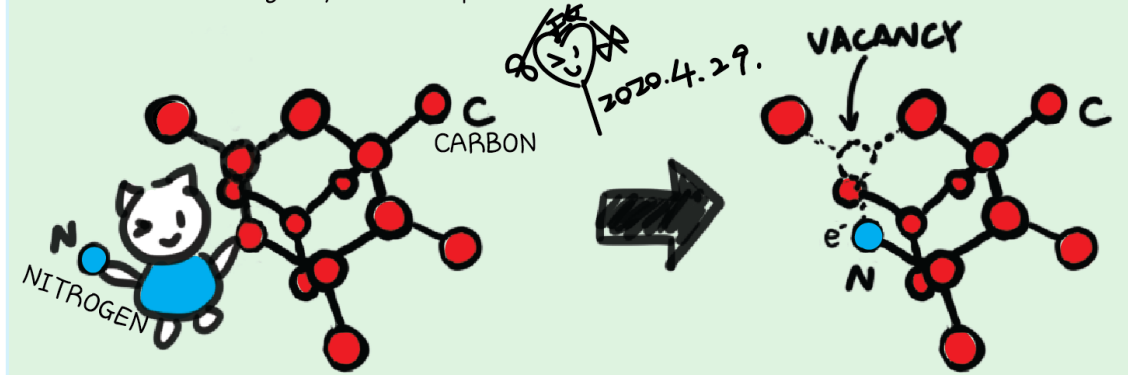
The electron spin seems to be a natural candidate.



But how do we isolate and control electrons?

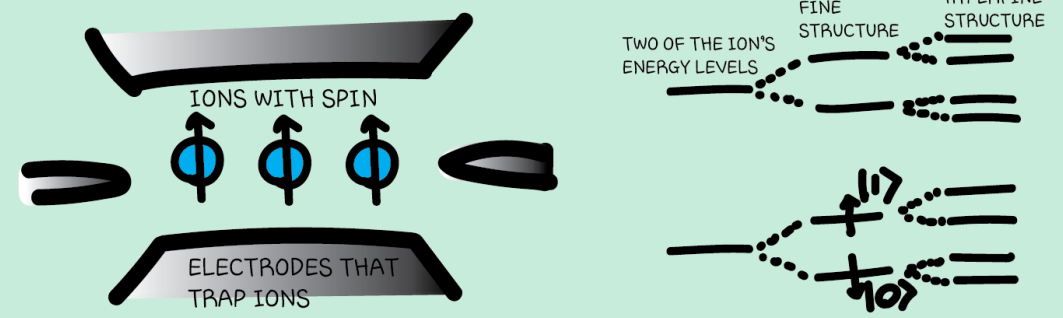


We can create a semiconductor stack. At the interface between the two semiconductors, electrons can be confined in 2D. By applying a gate voltage, the electrons underneath are removed, until there is only one electron left in a small region, called a "quantum dot".

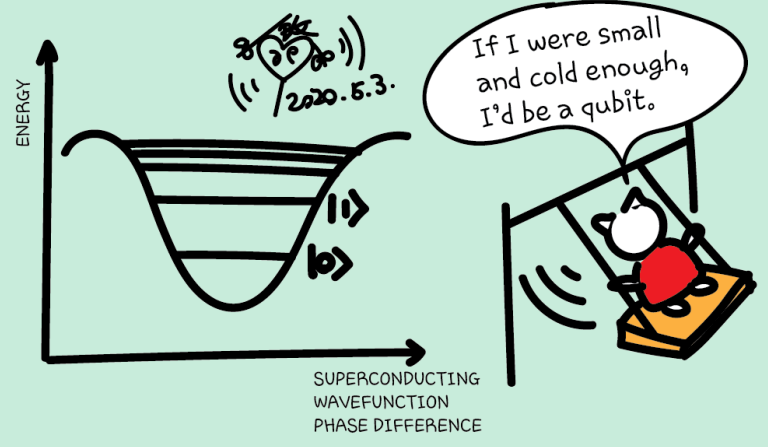
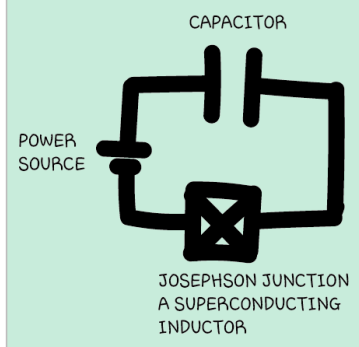


We can also use a crystal lattice, e.g. diamond. We can remove two carbon atoms (each has 6 electrons), replacing them with a single nitrogen atom (which has 7 electrons). The extra electron is bound to the nitrogen-vacancy region.

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.

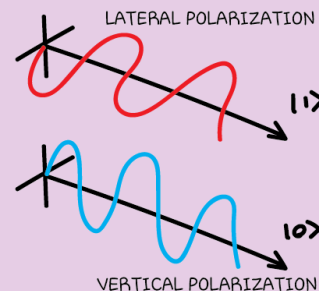
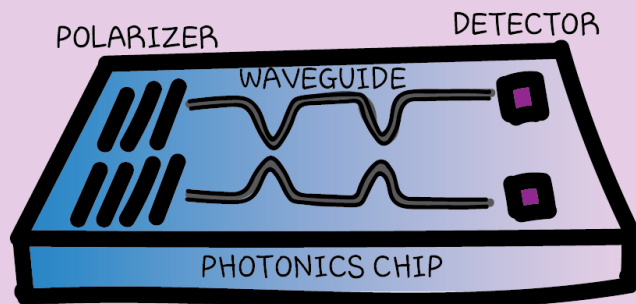


We can use two of an ion's electronic energy levels as the two qubit states. They can be the fine structure due to the ion's electron spins or the hyperfine structure due to electrons' interactions with the ion's nucleus. We can also make an "artificial atom" and use its energy levels as qubit states, e.g. a superconducting circuit. Its oscillation creates a set of discrete energies.

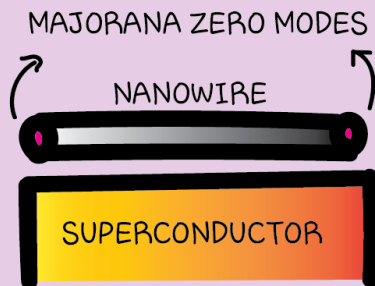




If we can use natural and artificial particles, such as electrons, ions or oscillating circuits, we can also try other types of particles and quasiparticles, and parameters other than energy levels.

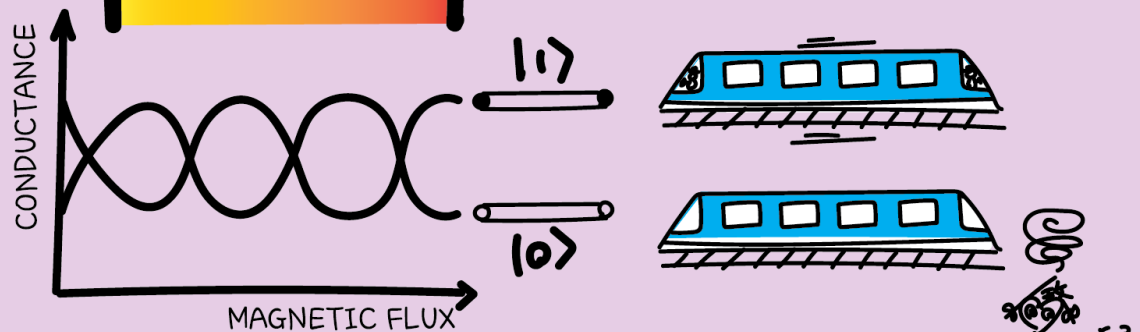


We can use photons' polarizations to encode qubit states.



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)



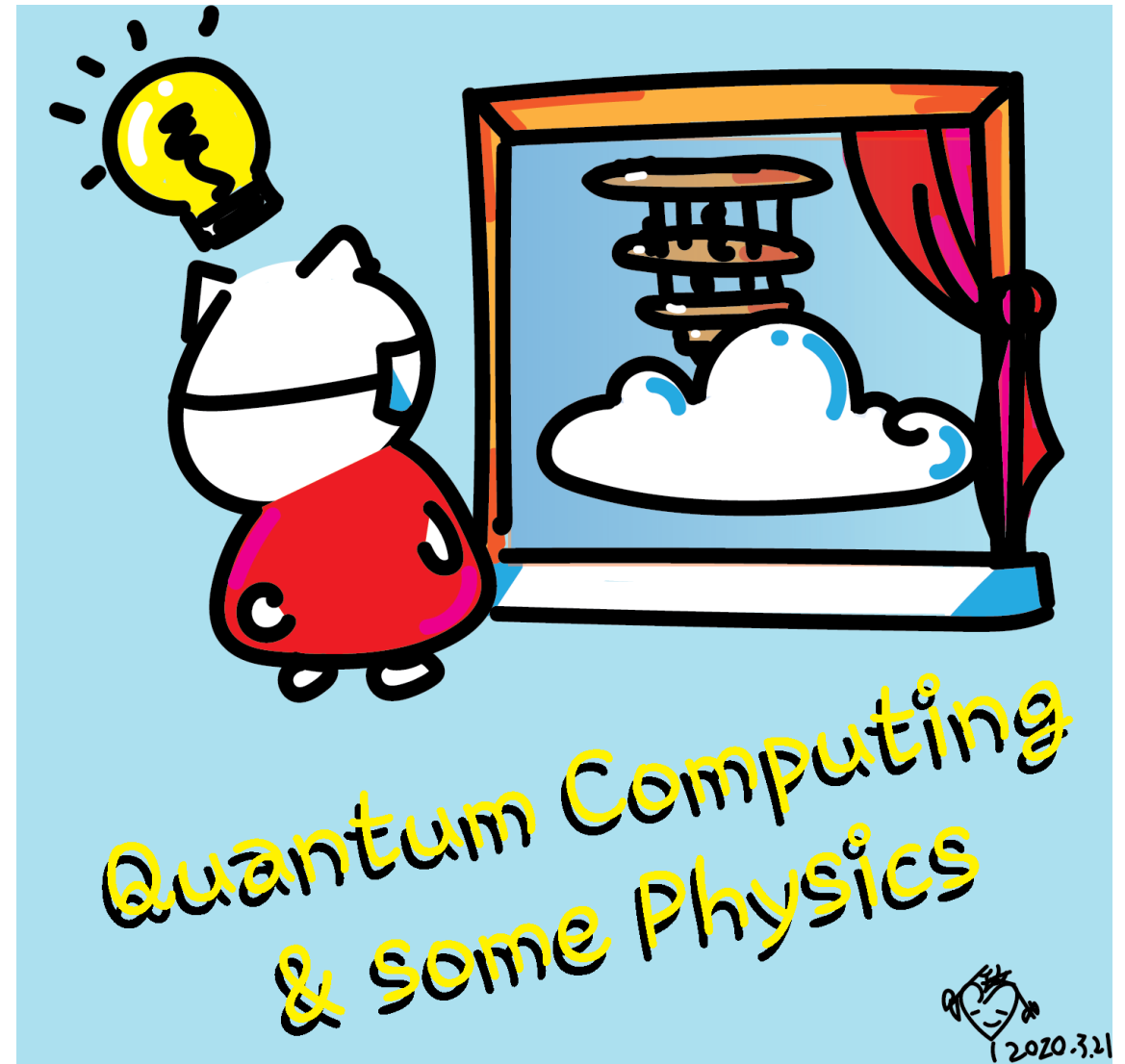
Algorithms (intuition)



Hardware (condensed matter physics)

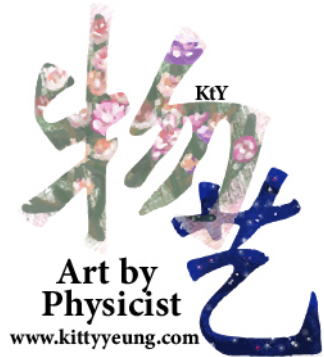
# Class structure

- [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

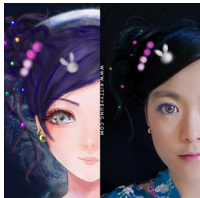


[aka.ms/learnqc](https://aka.ms/learnqc)





# 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](http://www.artbyphysicistkittyyeung.com)



- @KittyArtPhysics



- @artbyphysicistkittyyeung

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