Quantum ML Recap + Future Quantum ML Research

Week 6 - AI Inspire 2019

Recap of Previous Week - Quantum Adder

Adding Normally With Bits - Concept of Carry Bit

- 2 operations during addition
  - Carry operation & sum operation
- Algorithm
  - Start with rightmost bit
  - Perform sum operation and pass carry bits to column to left
  - Repeat process till you reach left most column and no more carry bits

					1
10101	10101	10101	10101	10101	10101
+11010	+11010	+11010	+11010	+11010	+11010
1	11	111	1111	1111	101111

Adding 21 and 26 in binary - demonstrating the sum and carry operation

Adding on Quantum Comp

- ➢ Objective - Convert diff rules of adding in quantum ⇒ quantum gates
  - NOT, CX, CCX gates
- ➢ Algorithm
  - Flip original states of |0> to |1> of qubits in beginning to start process of adding numbers (Use X gate)
  - Need to compute “carry bit” in adding
    - Rule = if at least 2 input qubits are in 1 state ⇒ output = 1
      - 3 input qubits = input carry from previous iteration and 2 addends
    - Use CX and CCX gates for carry bit

Adding on Quantum Comp

Input Carry	Bit from A	Bit from B	Output
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Carry Gate Operation Truth Table

Addition on Quant Comp, Faster Method

- Use Quantum Fourier Transformation algo on 2 addends
  - Quantum fourier transformation - function which finds the “ingredients” of a particular “dish”
    - Obtaining the simpler waves from the complex wave
- QFT Mathematically = rotating the qubit in complex plane
  - Quantum gate equivalent = Keep on repeating controlled-U gates → applies the rotations around the circle → rotations rep as wave
    - Obtain simpler waves (rotations about plane)

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi i k j}{N}}$$

$$F(\Psi) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \Psi_j e^{\frac{2\pi i k j}{N}}$$

But How is QFT Helpful for Addition?

- Represent 2 original equations y = 7 and y = 3 as diff circles (precalc knowledge)

$$f(t) = 3e^{2\pi i 0 t}$$

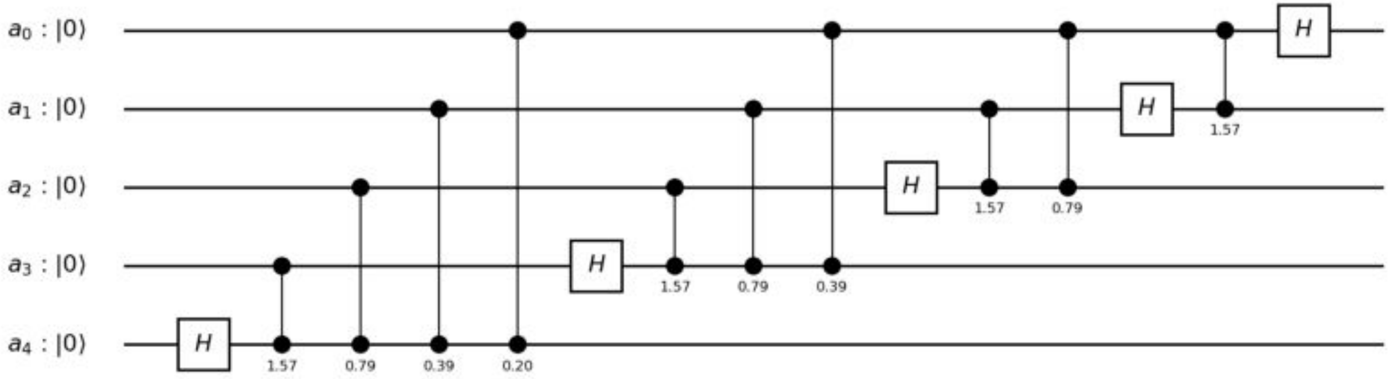
$$g(t) = 7e^{2\pi i 0 t}$$

- Once obtaining circles → can compute waves from QFT algo
- Add the 2 Fourier transformations together (the 2 waves)

$$\hat{g}(f+g) = \hat{g}(f) + \hat{g}(g)$$

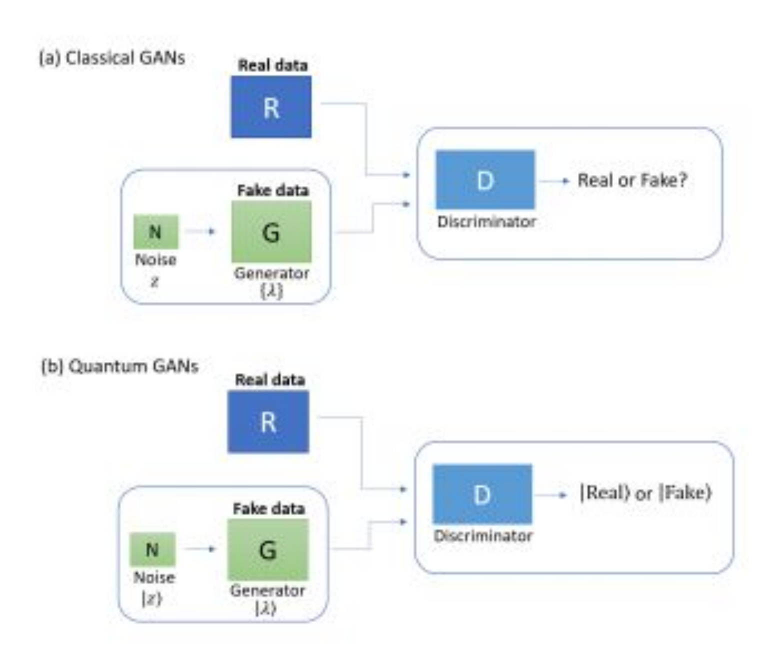
Addition on Quant Comp, Faster Method (Cont.)

➢ Algorithm
  - Take input
  - Apply Hadamard gate on qubit
  - Apply controlled-U1 gate
    - Rotates the qubit



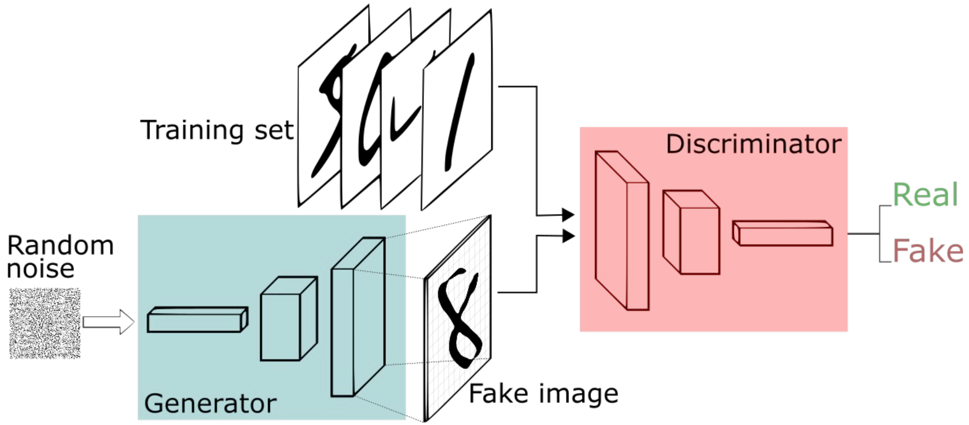
Numbers = angle by which qubit is rotated in complex plane

Recap of Quantum ML Algos - QGAN



Recap of ML - GAN

- Unsupervised model using supervised loss function
- 2 competing neural networks
  - Generative and Discriminator
- Great model which solves issue of not having enough data in real world cases → generates own data and gets trained from that
  - Still several challenges of GAN



Recap of ML-GAN (cont.)

- Generator neural network creates fake images from input vector
- Discriminator network learns to distinguish between the real and false images (real images taken from dataset)
    - Discriminator returns diff prob of each image being real (1 = real and 0 = fake)
- Cop-counterfeiter analogy
    - Counterfeiter learning to pass fake notes and cop is also in training as is able to start distinguishing

Architecture QGAN (How it Works High Level)

- 2 quantum circuits
  - 1 models the generator & the other circuit models the discriminator
  - G is generative quantum circuit & D is discriminator quantum circuit
    - Gates of G parameterized by theta_G, similar with circuit D
- Input state + noise inputted into circuit G and G feeds D various types of fake data
  - D’s job to get trained and distinguish real vs. fake
- Compute gradient of quantum optimization with quantum circuit (Quant circuit computes gradient)
  - Classical - gradient descent is used to optimize (minimize) GAN cost function
    - Cost function ⇒ measures how well algo matches estimate

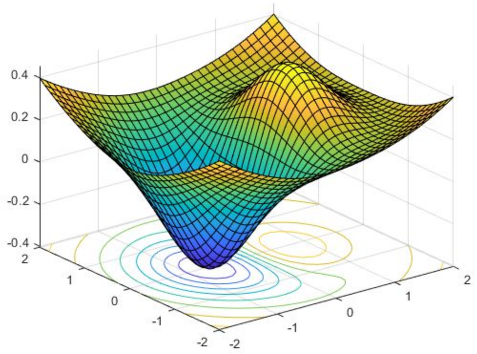
QGAN

https://arxiv.org/pdf/1804.08641.pdf

Quantum Computing/ML Research + Future Directions

HTTPS://WWW.YOUTUBE.COM/WATCH?V=MPO9IYFIWBW

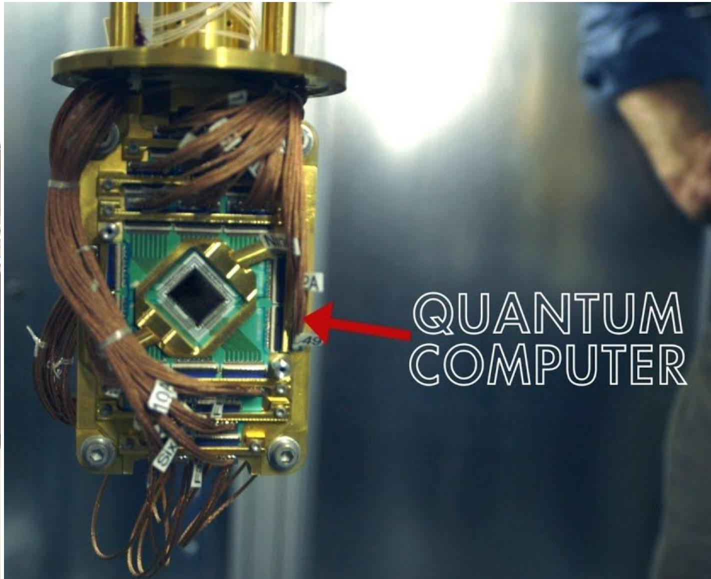
Quant Computing/Quant ML Application Areas



- **Cryptography**
- Molecular Modeling
- **Communication**
- Forecasting Weather
- Experiments Undertaken in Particle Physics
- Genomics
- **Optimization**

Some Companies+Agencies in Quantum Computing

- Some companies+agencies involved in quantum computing
- D-wave
- Google
- IBM
- Xanadu
- Microsoft
- NASA



Quantum Computing- Cryptography

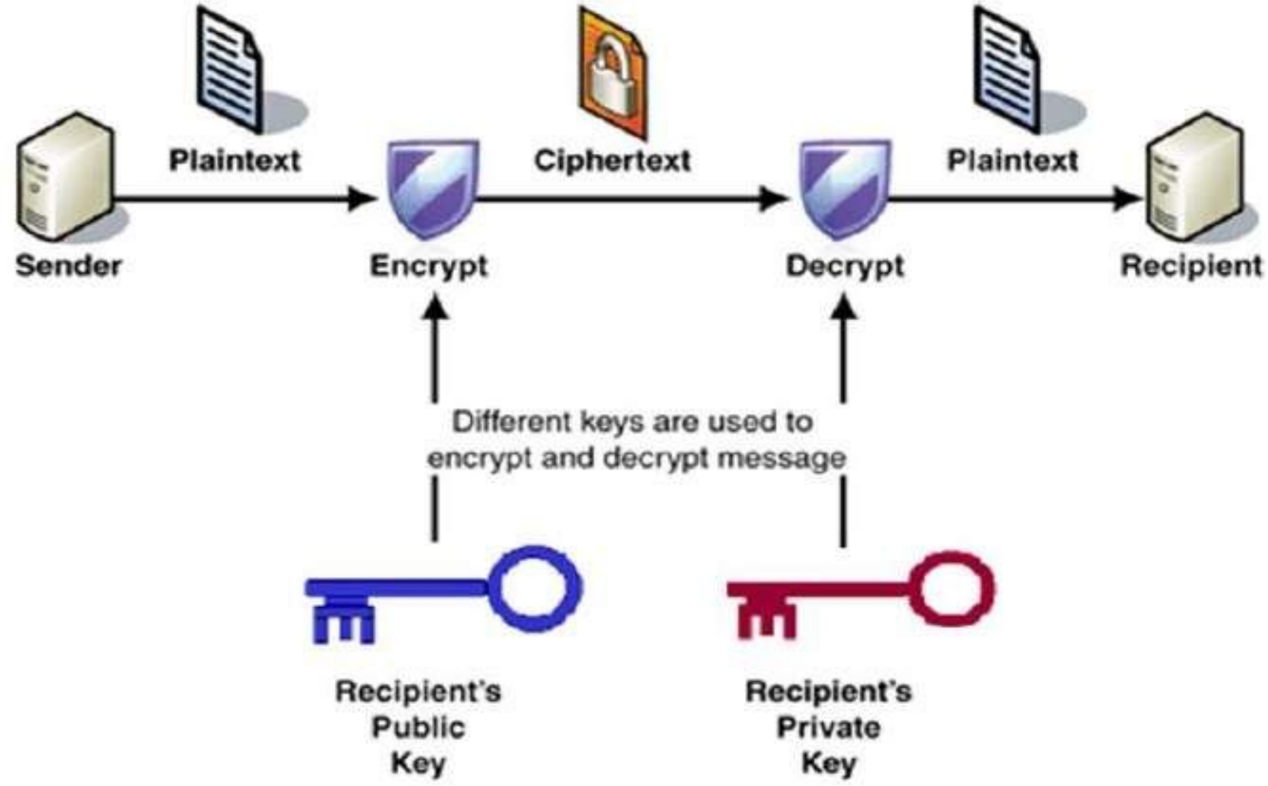
Classical Cryptography Concepts + Vocab

- Algorithms developed to
  - Maintain secrecy and privacy of data being transmitted
  - Authenticate data being received
- Plaintext vs. ciphertext
  - Plaintext = original message
  - Ciphertext = message altered through cipher
- Cipher
  - Algo itself which transforms plaintext so that it can’t be easily read
    - Transformation, substitution, etc.
- Encipher/Encode
  - Plaintext ⇒ ciphertext using cipher + key
- Decipher/Decode
  - Ciphertext ⇒ plaintext using cipher + key

Classical Crypt - Public Key

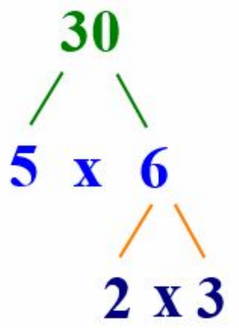
- Public key (Asymmetric cryptography)
  - Uses both public and private keys
    - Public key → can be shared with anyone
    - Private key → kept secret
  - Either key → used for encryption & opposite key → used for decryption
- Example scenario
  - Sender (Alice) & Receiver (Bob)
  - Alice get’s Bob’s public key
  - Plaintext encrypted with public key algo → converted to ciphertext
  - Ciphertext sent to Bob → Bob decrypts ciphertext with his private key to read message

Classical Crypt - Public Key



Classical Crypt - Prime Factorization

- What are the algorithms used for classical crypt?
- Prime factorization → public key encryption
  - Multiply 2 large primes together → encrypts message
  - To decrypt → need to break the big number into its prime factors
- No shortcut → trial and error
  - Large numbers initially → hard to break the message because hard to decrypt back into its original prime factors

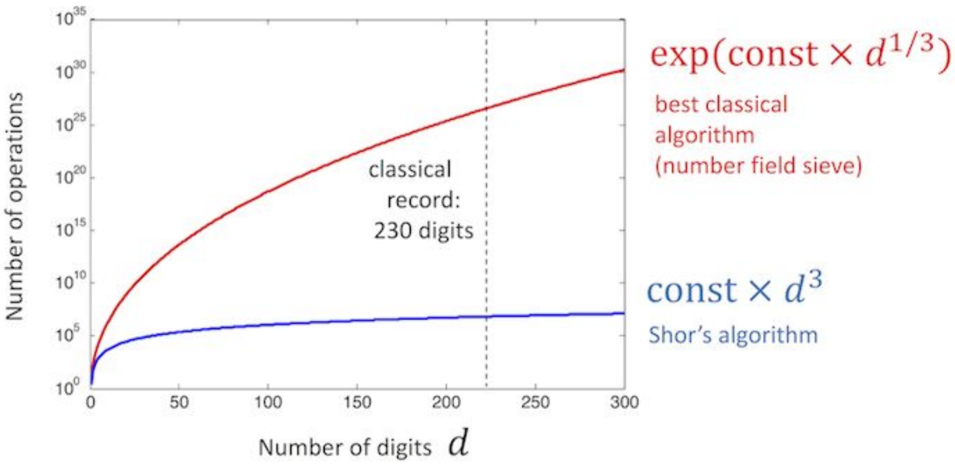


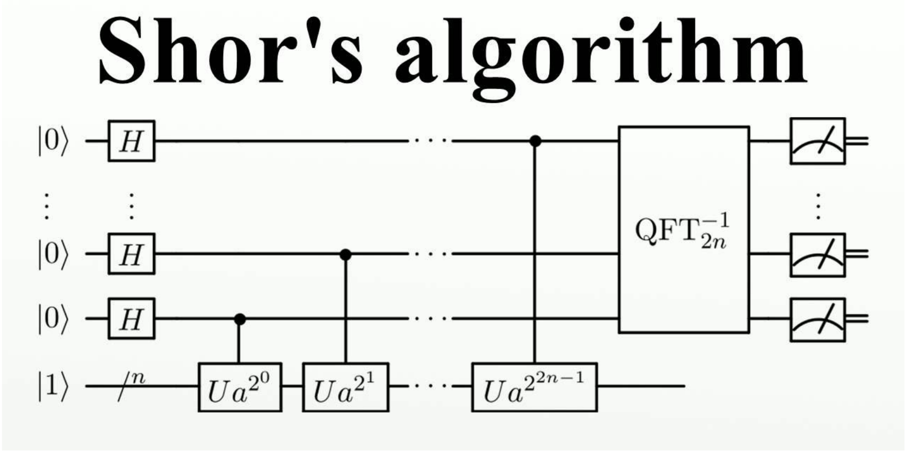
RSA - A Quantum Algorithm

- ➢ Standard cryptographic algo
- ➢ Used for Internet
- ➢ Public key encryption, uses prime factorization technique

Shor's Quantum Algorithm

- Solves problem of trying to find prime factors for very large number efficiently
- Can be run on both classical and quantum computers
  - Runs very slow on classical comp
  - Very fast on quantum comp





The Power of Shor's Algo in Quantum World

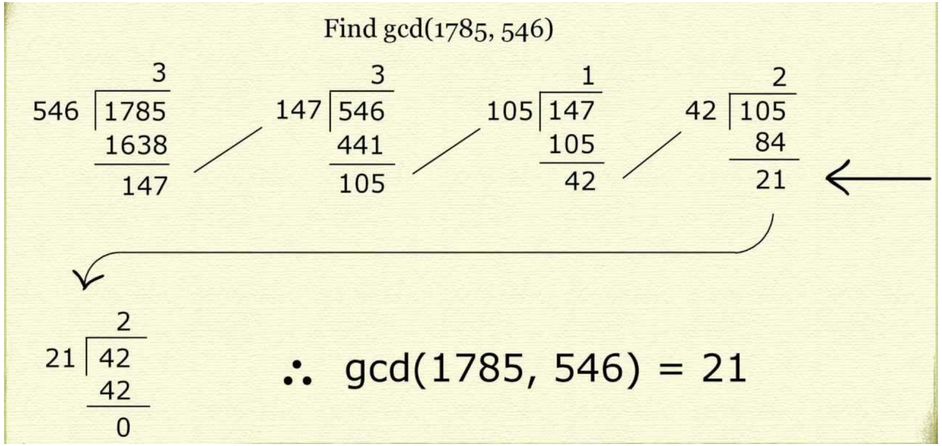
- Can decrypt message for very large prime numbers using Shor's algo
  - Thus, can afford to use big numbers for quantum cryptography in future
  - Hackers will need to break laws of quantum physics to compute the prime numbers

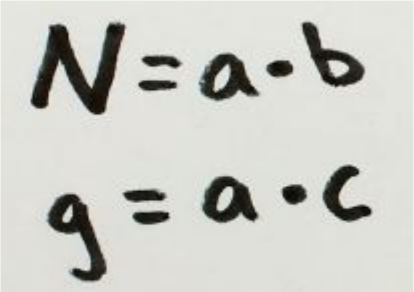
Shor's Quantum Algorithm (Cont.)

- The Algorithm -
  - Original number (N)
  - Random guess (g) which could be a factor
  - Transform (g) into a better guess which will likely be a factor of (N)
- Doesn't actually use quantum mechanics inside algo BUT works more efficient on quantum comp

Need to Check if "g" Shares Common Factor With "N"

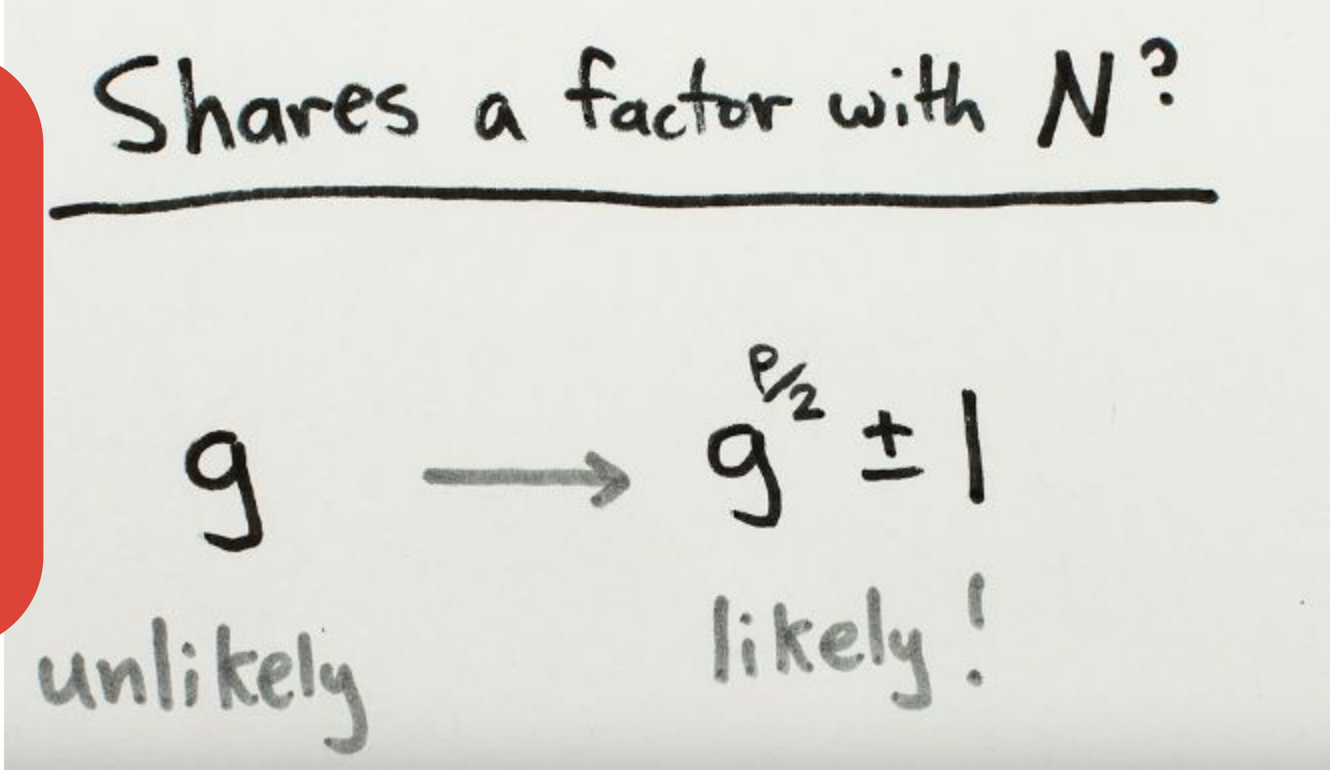
- When picking g
  - Don't need g to be an actual factor of N
  - INSTEAD → g just needs to share a factor with N (>=1 factors shared)
- Euclid's algorithm → Ex – **<u>divide N by g to get a → build factors of N → part of Number Theory</u>**





Need to Check if "X" Shares Common Factor With "N"

- Euclid's algo is still inefficient for large numbers
- Transform g to a number which will share a factor with N



Shor's Algorithm (Cont.)

$$\underline{N, g}$$

$$g^{p} = m \cdot N + 1$$

$$g^{p} - 1 = m \cdot N$$

$$\underbrace{\left(g^{p/2}+1\right)}_{\text{something}} \cdot \underbrace{\left(g^{p/2}-1\right)}_{\text{something}} = m \cdot N$$

$$\underbrace{\left(g^{p/2}+1\right)}_{a \cdot \text{factor}} \underbrace{\left(g^{p/2}-1\right)}_{b \cdot \text{factor}} = m \cdot N$$

$$7^{4/2} + 1 = 50 \not\rightarrow 15 \rightarrow 5$$

$$7^{4/2} - 1 = 48 \not\rightarrow 15 \rightarrow 3$$

Can find factors of g^(p/2)+1 & g^(p/2)-1 with EUCLID'S ALGORITHM!!!
Even though 50 and 48 aren't factors of 15 → share common factors with 15 which can be determined by applying Euclid's with gcd(50, 15) AND gcd(48, 15)

Examples

$\underline{7,\ 15}$

$$7^2 = 3 \cdot 15 + 4$$
$$7^3 = 22 \cdot 15 + 13$$
$$7^4 = 160 \cdot 15 + 1$$

$\underline{42,\ 13}$

$$42^2 = 135 \cdot 13 + 9$$
$$42^3 = 5699 \cdot 13 + 1$$

Need to Check if "g" Shares Common Factor With "N"

Reasoning for g^(p/2) + 1

- ➢ 2 #s A, B with no common factors
- ➢ If A is multiplied with itself enough times = m * B + 1

why $g^{p/2} \pm 1$?

$A, B \longrightarrow \underbrace{A \cdot A \cdot A \cdot A \cdot \ldots \cdot A}_{\text{enough times}} = \text{something} \cdot B + 1$

(no common factors)

i.e.

$A^p = m \cdot B + 1$

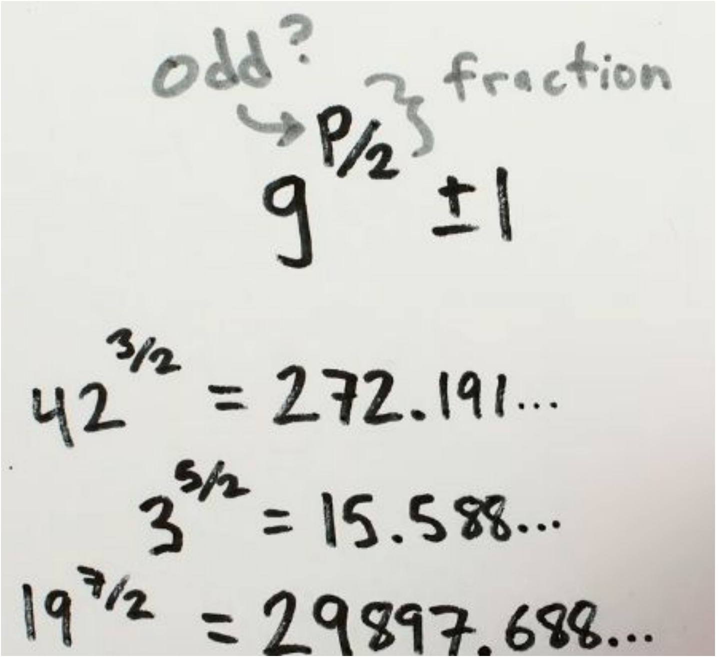
Some Problems of Shor's Algorithm

- 3 central problems ⇒ hard to implement on quantum computer

$$\underbrace{\left(g^{P/2}+1\right)}_{a\cdot N}\underbrace{\left(g^{P/2}-1\right)}_{\text{factor of } m} = m\cdot N$$

Problem #1 - neither #s produced by algo will be useful for finding factors through Euclidean algo

Some Problems of Shor's Algorithm



Problem #2 - number p is odd ⇒ fraction will not be an integer
⇒ number will not be an integer, only want int

Some Problems of Shor's Algorithm

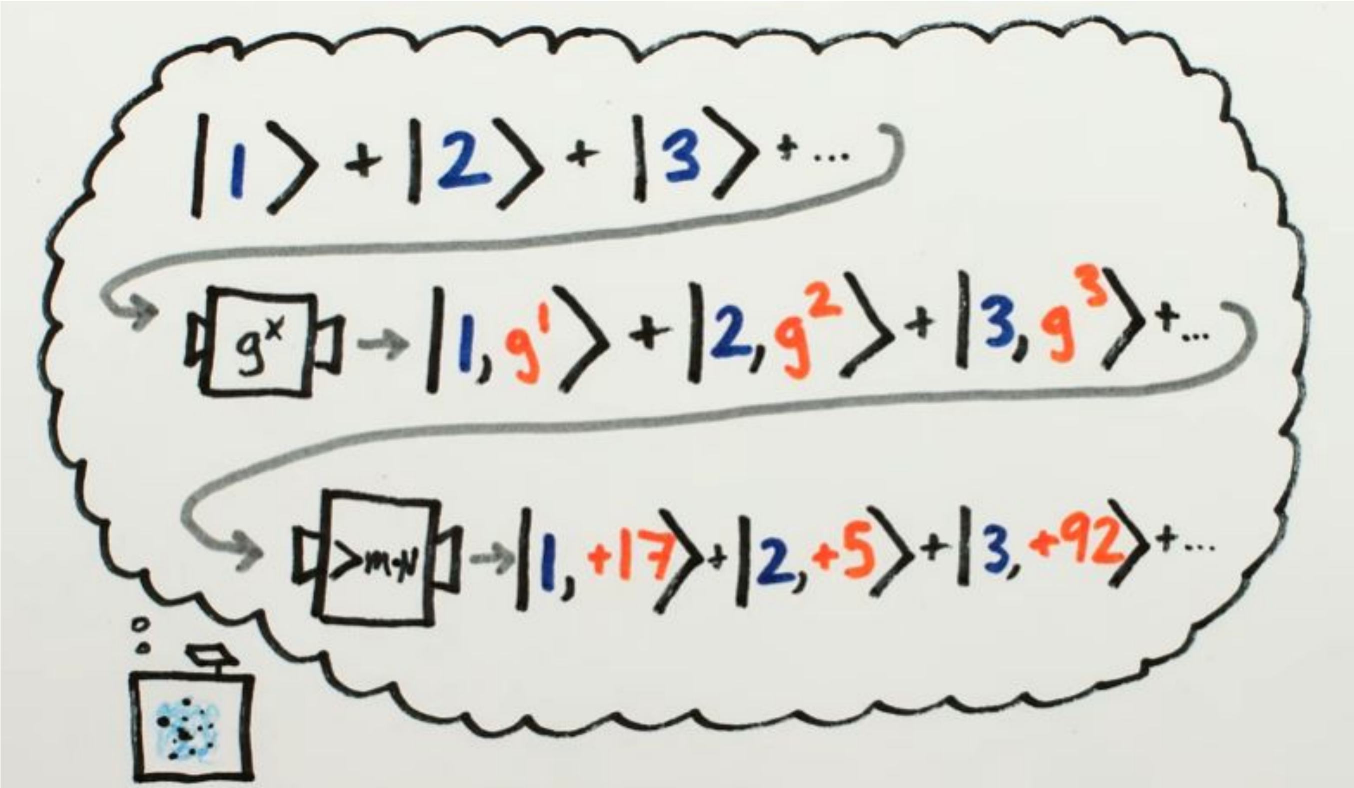
Problem #3 - Finding "p" ⇒ classical computer → take a lot of time vs. quantum computer will harness quantum mechanics

Solution - quantum superposition → calculate all poss answers simultaneously

Output → all wrong answers are destructively interfere & are removed singling out 1 correct answer

Essence of Shor's Algo = translates problem into quantum form so output has wrong answers destructively interfering and 1 right answer through superposition ⇒ find "p"

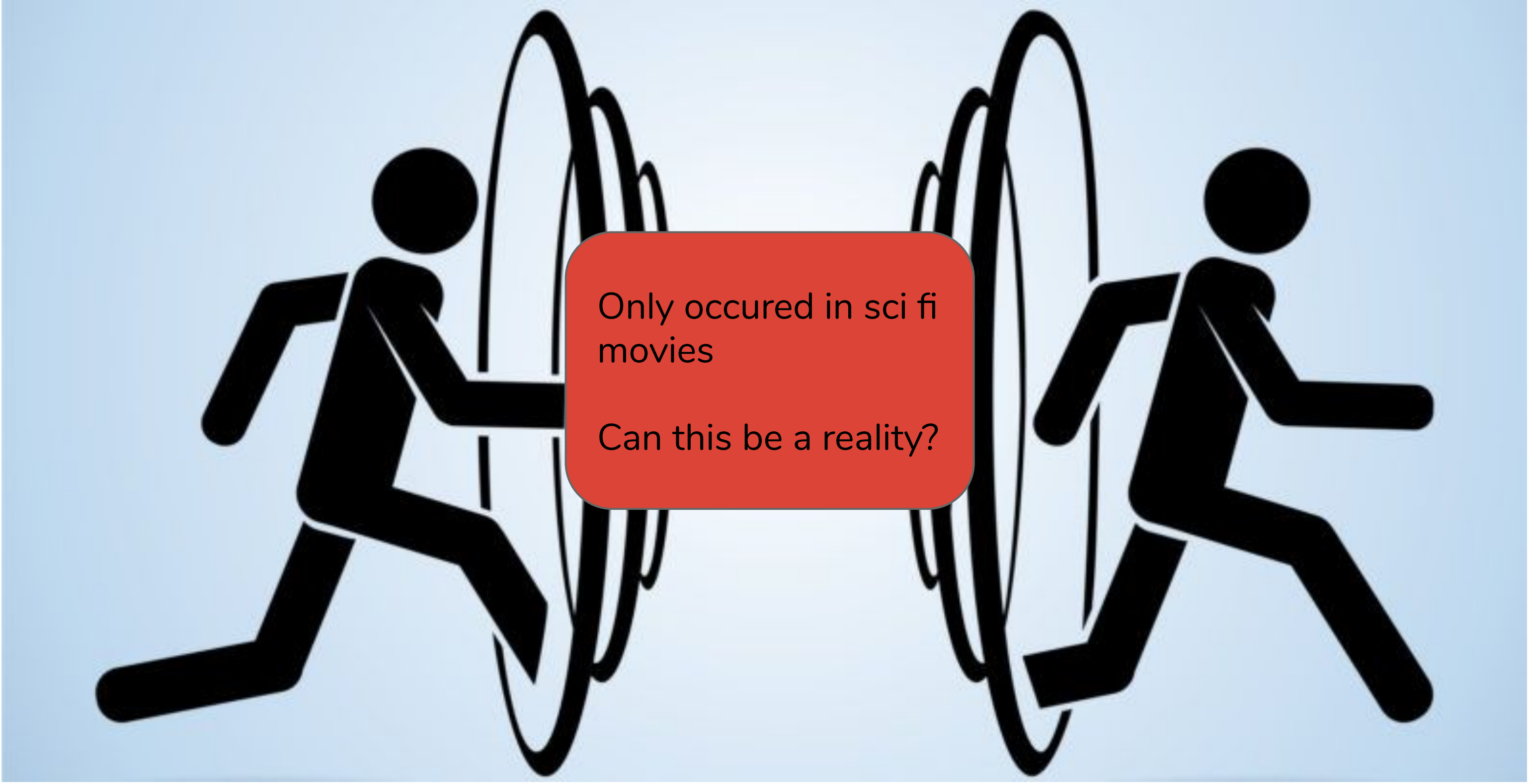
Solution of Problem #3 Diagrammatically



Send in a superposition of #s → superposition of all possible powers guess can be raised to → superposition of how much bigger each of the guesses raised to a power are

Quantum Computing-Communication

Teleportation



Only occured in sci fi movies

Can this be a reality?

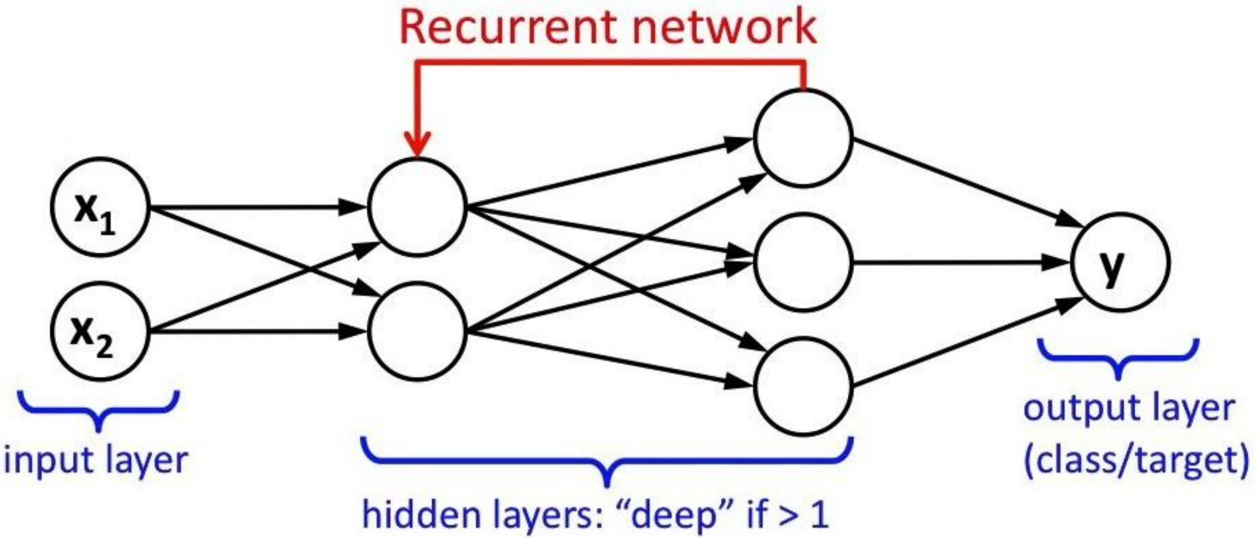
Entanglement - Teleportation

- “Spooky action a distance”
- Can be harnessed for teleportation
- Chinese scientists teleported packet of info to space
  - FARTHEST distance achieved - long distance comm
    - Eavesdropper can’t use this type of long distance system without alerting the other end
  - https://www.space.com/37506-quantum-teleportation-record-shattered.html
- Far from teleporting humans
  - Going from one place to the other
  - Same constituents transferred → exactly same person

https://www.youtube.com/watch?v=JMdO5KyjwAw

Quantum ML- Quantum Boltzmann Machine

Recurrent Neural Network

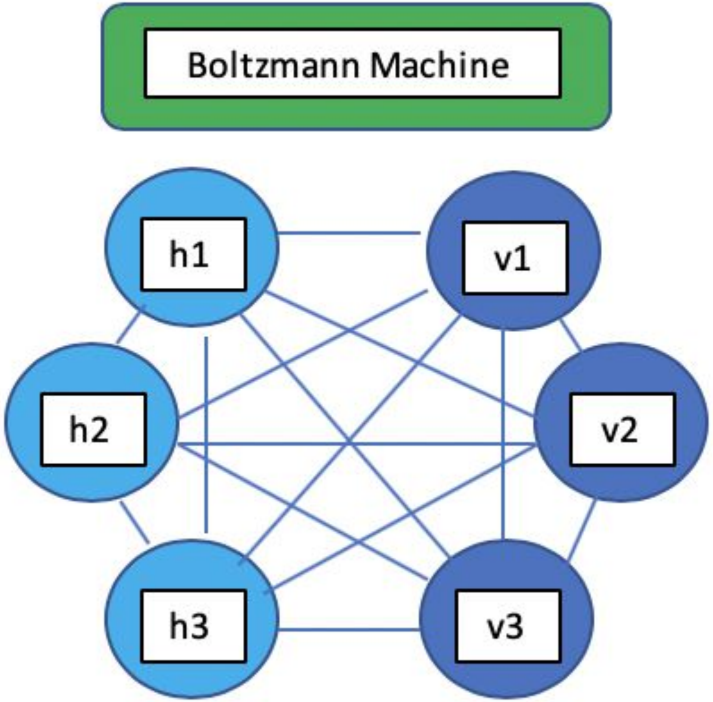


Looks at previous events in network to make conclusions for future layers

Boltzmann Machine

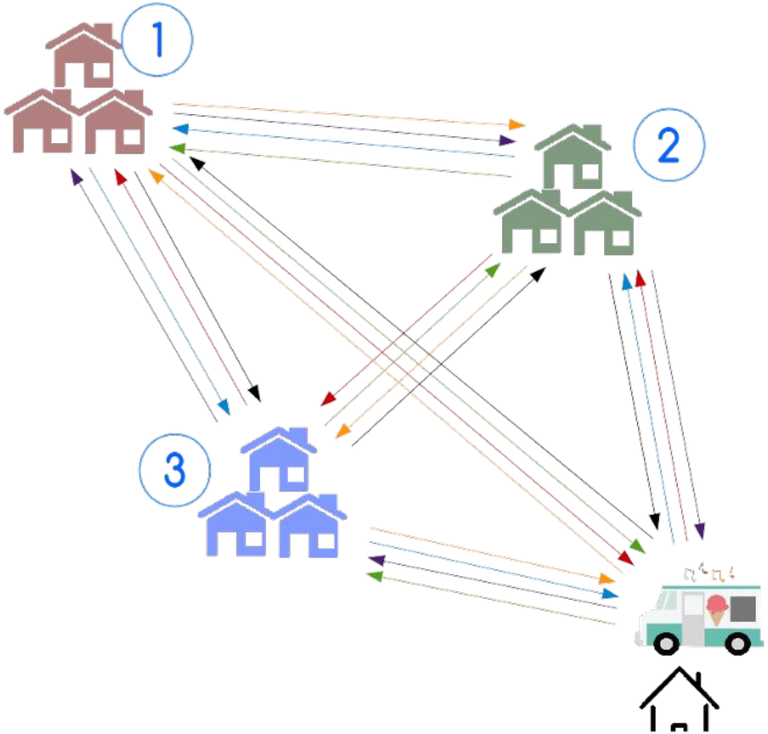
- Type of ML Recurrent neural network
  - Type of neural network which looks at previous outputs to determine current output
  - Neural network - use inputs and adjust weights to get output, where error approaches 0 after several iterations
- Stochastic vs Deterministic neural net
  - Deterministic/normal neural network
    - Output is unique/deterministic for fixed input
    - Introduce random variations into neural net
      - Can give stochastic weights or stochastic transfer function
      - Ex of stochastic transfer function ⇒ In Boltzmann machine, each neuron has "binary value" (fired or not fired) ⇒ chance of neuron firing depends on state of other neurons
    - Useful for optimization probs ⇒
  - Stochastic neural network
    - Output will be different/stochastic/random for fixed input

Boltzmann Machine



Analogy for Quantum Annealing

Problem Statement -
Ice cream business & need to sell ice cream by going to different neighborhoods → optimal route going through all neighborhoods ***(Traveling Salesman Problem)***



Solution-
Find shortest distance by comparing all poss paths → BUT inefficient if large # neighborhoods

Analogy for Quantum Annealing (cont.)

Actual Solution -

1. Encode solution into physical system
    a. Convert info of ice cream problem into physical system so **ground state = solution**
        i. Why ground state?
            1. Easier to go down the mountain vs. climbing → systems tend to ground state
    b. Physical systems → described by **Hamiltonian** function
        i. Can get energy of system, other quantum phys prop of system, etc.

Going back to Ice Cream Analogy -

1. Include constraints to problem (Ex - amt of max distance ice cream truck can travel before gas runs out, which roads truck is not allowed to use, etc.)
    a. If constraint is NOT satisfied → add terms to Hamiltonian (inc energy of system → farther from ground state = solution)
2. Ex - spin interaction changes based on distance traveled
    a. More distance traveled = more spin (more energy), less distance = less spin (less energy) = closer to ground state
3. Lowest energy state, ground state = solution through SIMULATION

Quantum Annealing

- ➢ Find minimum of a function
- ➢ Type of optimization problem → go through all possible solutions and find min = solution
- ➢ D-wave machine = quantum annealer which runs quantum comp algos
- ➢ **Application = Predicting financial crashes**
  - **Great for predicting financial issues for Wall Street & equilibrium needed to avoid such crashes**
    - **Ex - minimize cost of trading and minimize market risk ⇒ <u>optimizing the global min value through quantum annealing</u>**
      - **Able to identify right equilibrium and in turn predict financial crashes**

Quantum Boltzmann Machine

- Quantum annealing with boltzmann machine
- Boltzmann machine
  - Use binary variables
- **Run boltzmann machine on quantum annealing processor to get solution to optimization problems**
  - **Training the Boltzmann machine on quantum annealing processor will be more efficient**
  - **Applications → make better predictions of financial problems (financial forecasting), etc.**

Recap

ANALOGY

- Objective
  - Search for a briefcase lost in building (100 levels)
- Classical Computer
  - One person checks each floor of the building repetitively
- Supercomputer
  - A team of people search for briefcase at same time
- Quantum computer
  - 1 person is placed in every room of each level
    - Find briefcase **INSTANTLY**!

https://www.youtube.com/watch?v=IhHMJCUmq28

Hope You Had Fun Learning Quantum Computing + Quantum ML!