

Quantum Entanglement

What is it, and why is it useful?

Laura Cui

March 2021

HMMO Education

Quantum computing

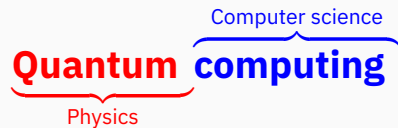
Quantum computing

Physics

Quantum **computing**

Computer science

Physics

The diagram features the words "Quantum" and "computing" in a bold, sans-serif font. "Quantum" is colored red, and "computing" is colored blue. A red horizontal curly brace is positioned beneath "Quantum", with the word "Physics" centered below it in a smaller red font. A blue horizontal curly brace is positioned beneath "computing", with the words "Computer science" centered above it in a smaller blue font. The two braces overlap, visually representing the intersection of the two fields.

- ⚛ **Quantum computing** is the application of quantum mechanical phenomena to perform computations
- ⚛ Information or data can be stored as the state of a physical system
- ⚛ The operation of a quantum computer is tied to the underlying physics

Why quantum computing?

- ⚛ Certain quantum effects can't be simulated classically
- ⚛ Quantum computers are believed to be capable of solving some problems much faster than classical computers
- ⚛ Example: factoring large integers

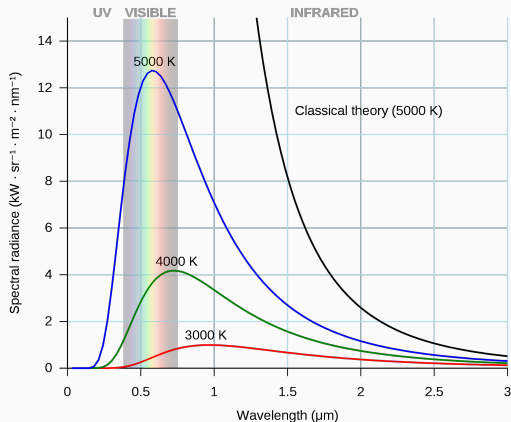
Quantum mechanics

The history of modern physics

- ⦿ By early 1900's most of physics was thought to be solved
- ⦿ Newtonian mechanics and Maxwell's equations seemed to accurately describe matter and light
- ⦿ In 1900, Lord Kelvin proclaimed "there is nothing new to be discovered in physics. All that remains is more and more precise measurement."

Inconsistencies c. 1900

- ⚛ Ultraviolet catastrophe: infinite amount of energy predicted in thermal radiation since classical distribution $B \propto \frac{1}{\lambda^4}$



Inconsistencies c. 1900 (cont'd.)

- ⚗ Photoelectric effect: electrons are released when shining light onto metal
 - Kinetic energies depend only on the wavelength of light and not the intensity
- ⚗ In 1900 Max Planck proposed the correct distribution for thermal radiation

$$B \propto \frac{\nu^3}{e^{h\nu/k_B T} - 1}, \quad \nu = c/\lambda$$

- ⚗ Suggests energy quantity/scale $h\nu$
- ⚗ In 1905 Albert Einstein proposed that $E = h\nu$ be taken literally to explain the photoelectric effect

Development of quantum mechanics

- ⊗ Initial opposition to quantization of physics, including from Planck
- ⊗ Additional experiments confirmed quantization of other quantities, e.g. angular momentum of electrons
- ⊗ Various "quantization rules" and *ad-hoc* theories used until development of quantum formalism by Erwin Schrödinger and Werner Heisenberg in 1925

Postulates of quantum mechanics

1. An isolated physical system is associated with a **state space** complex vector space with an inner product. At any point in time, the system is described by its **state vector**, a vector in this space which represents the wavefunction.

Postulates of quantum mechanics (cont'd.)

1. An **isolated** physical system is associated with a **state space** complex vector space with an inner product. At any point in time, the system is described by its **state vector**, a vector in this space, a vector in this space which represents the wavefunction.

Postulates of quantum mechanics (cont'd.)

1. An isolated physical system is associated with a **state space complex vector space** with an **inner product**. At any point in time, the system is described by its **state vector**, a vector in this space, a vector in this space which represents the wavefunction.

Postulates of quantum mechanics (cont'd.)

- ⊗ Analogous to Euclidean vector spaces, e.g. \mathbb{R}^2
- ⊗ A set of vectors S **spans** a vector space V if V is equal to the set of all **linear combinations** of elements of S
 - Does $\left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$ span \mathbb{R}^2 ? What about $\left\{ \begin{bmatrix} 2 \\ -1 \end{bmatrix}, \begin{bmatrix} -4 \\ 2 \end{bmatrix} \right\}$?
- ⊗ A **basis** B of a vector space V is a minimum spanning set of V
 - Notice $|B| = \dim V$

Postulates of quantum mechanics (cont'd.)

- ⊗ The **inner product** of two vectors \vec{a} and \vec{b} defines "how much of \vec{a} is in \vec{b} "
 - The inner product for \mathbb{R}^2 is just the dot product $\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2$
- ⊗ For any vector \vec{a} , $|\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}}$
- ⊗ Two vectors \vec{a} and \vec{b} are **orthogonal** if $\vec{a} \cdot \vec{b} = 0$
- ⊗ If two vectors $\vec{a}, \vec{a}' \in \mathbb{R}^2$ are orthogonal, then any vector $\vec{b} \in \mathbb{R}^2$ can be written as $\vec{b} = \frac{\vec{b} \cdot \vec{a}}{|\vec{a}|} \vec{a} + \frac{\vec{b} \cdot \vec{a}'}{|\vec{a}'|} \vec{a}'$
 - Example: the vector $\begin{bmatrix} 4 \\ 2 \end{bmatrix}$ can be written as $3 \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

Postulates of quantum mechanics (cont'd.)

- ⊗ In quantum mechanics the coefficients can be *complex* numbers
- ⊗ Quantum state vectors often written as **kets**, i.e. $|\psi\rangle$
- ⊗ If a two-level system is spanned by a set $\{|\psi_1\rangle, |\psi_2\rangle\}$, then any state $|\psi\rangle$ can be written as a sum $\{c_1 |\psi_1\rangle + c_2 |\psi_2\rangle\}$
- ⊗ Example: in Schrödinger's thought experiment, a cat is placed in a box, and nuclear radiation is released with some probability
 - The cat's state is given by $c_1 |\text{dead}\rangle + c_2 |\text{alive}\rangle$ for some complex c_1, c_2

Postulates of quantum mechanics (cont'd.)

- ⊗ The inner product of two states $|a\rangle = \{a_1 |\psi_1\rangle + a_2 |\psi_2\rangle$ and $|b\rangle = \{b_1 |\psi_1\rangle + b_2 |\psi_2\rangle$ is given by $\langle a|b\rangle = a_1^* b_1 + a_2^* b_2$
- ⊗ Notice $\langle a|b\rangle = \langle b|a\rangle^*$ for any two states $|a\rangle, |b\rangle$
- ⊗ $\langle a|a\rangle = |a_1|^2 + |a_2|^2$ is always real and non-negative

Postulates of quantum mechanics (cont'd.)

2. The evolution of a closed quantum system is given by a unitary transformation.

2. The evolution of a **closed** quantum system is given by a unitary transformation.

Postulates of quantum mechanics (cont'd.)

2. The evolution of a closed quantum system is given by a **unitary transformation**.

Postulates of quantum mechanics (cont'd.)

- ⊗ Given the state of the system $|\psi\rangle$ at some time t_0 , the state of the system at any other time t can be given as $|\psi'\rangle U(t) |\psi\rangle$, such that $\langle\psi|\psi\rangle = \langle\psi'|\psi'\rangle$ for all t
- ⊗ U must be a **linear operator**, so for any $|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle$,
 $U|\psi\rangle = c_1 U|\psi_1\rangle + c_2 U|\psi_2\rangle$
- ⊗ Is $U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ a valid transformation? What about $U = \begin{bmatrix} i & 0 \\ 1 & 0 \end{bmatrix}$?
- ⊗ Note U can represent the natural evolution of the system or manipulations by a scientist

3. Quantum measurements project the system onto an orthonormal basis of possible outcomes.

3. Quantum measurements project the system onto an **orthonormal basis** of possible outcomes.

Postulates of quantum mechanics (cont'd.)

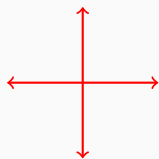
- ⊗ A system whose state is given by $|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle$ will be observed in the $|\psi_1\rangle$ state with probability $\frac{|\langle\psi|\psi_1\rangle|^2}{\langle\psi|\psi\rangle} = \frac{|c_1|^2}{|c_1|^2 + |c_2|^2}$, and in the $|\psi_2\rangle$ state with probability $\frac{|\langle\psi|\psi_2\rangle|^2}{\langle\psi|\psi\rangle} = \frac{|c_2|^2}{|c_1|^2 + |c_2|^2}$
- By convention we set $|c_1|^2 + |c_2|^2 = 1$
 - Can't directly measure c_1 and c_2
- ⊗ Example: if Schrödinger's cat is in the state $|\psi_{\text{cat}}\rangle = \frac{1}{2} |\text{dead}\rangle + \frac{\sqrt{3}}{2} |\text{alive}\rangle$, there is a $\frac{1}{4}$ chance of observing it dead and $3/4$ chance of observing it alive when we open the box

- ⊗ In addition to pure quantum states, we can also consider *classical* probabilistic ensembles of different states or **mixed states**
- ⊗ Example: a coin toss lands on either heads or tails with probability $1/2$
- ⊗ Behave differently from superpositions when measured in different bases

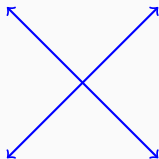
- ⊗ Polarizing filters project photons along either the X or Y axes, allowing only photons along the X axis to pass through
- ⊗ If the initial beam is unpolarized, a photon's initial state can be represented as $\frac{1}{\sqrt{2}} |x\rangle + \frac{1}{\sqrt{2}} |y\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1/\sqrt{2} \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$
- ⊗ Photons are projected onto the state $|x\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and pass through with probability $1/2$

Photon polarization (cont'd.)

- ⊗ If the polarized beam is passed through another filter rotated by 45° , photons are projected onto $|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$ and pass through with probability $1/2$
- ⊗ If the outgoing beam is passed through yet another filter rotated by 90° , photons are projected onto $|y\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and pass through with probability $1/2$
- ⊗ The final output beam is orthogonal to the original polarized beam!



$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$



$$\left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$$

Photon polarization (cont'd.)

- ⊗ Note if a beam polarized in the $|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$ direction is passed through another filter offset by 45° , all of the photons will pass through
- ⊗ A mixed state can be prepared by combining a beam passed through the first filter with a beam passed through a filter rotated by 90°
 - Any given photon is either in the state $|x\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ or $|y\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ with probability $1/2$
 - If this beam is passed through a filter offset by 45° , only $1/2$ of the photons will pass through!

- ⊗ Classical bits can take on the values 0 or 1
- ⊗ Quantum bits or **qubits** can be in any superposition of $|0\rangle$ and $|1\rangle$
- ⊗ A general qubit state is given by $a|0\rangle + b|1\rangle$, where a and b are complex
 - Suggests a single qubit can store more information than a classical bit

- ⊛ Often interested in systems with multiple components
- ⊛ **Composite systems** are associated with a vector space represented by the tensor product of its component vector spaces
 - If we have two classical coins, the outcome is one of $\{HH, HT, TH, TT\}$
 - If we have two cats in boxes Mittens and Nora, the state of the system is spanned by the basis $\{|\text{alive}\rangle_M \otimes |\text{alive}\rangle_N, |\text{alive}\rangle_M \otimes |\text{dead}\rangle_N, |\text{dead}\rangle_M \otimes |\text{alive}\rangle_N, |\text{dead}\rangle_M \otimes |\text{dead}\rangle_N\}$
 - The state of a two-qubit system AB is spanned by the basis $\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}$, or $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

- ⊗ The outcomes of two coin flips is always independent, i.e. landing on heads for one doesn't affect the probability of landing on heads for the other
- ⊗ Two components of a composite quantum system are **entangled** if the distribution of their measurement outcomes is *not* independent
- ⊗ Example: is the state $|\psi\rangle_{MN} = |\text{alive}\rangle_M \otimes |\text{alive}\rangle_N$ entangled?
 - No, no matter which cat we check first, we always find that both are alive

Entanglement (cont'd.).

Which of the following qubit states are entangled?

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{8}} |00\rangle + \frac{\sqrt{3}}{\sqrt{8}} |01\rangle + \frac{1}{\sqrt{8}} |10\rangle + \frac{\sqrt{3}}{\sqrt{8}} |11\rangle$$

- Not entangled, regardless of the outcome of A we always have 1/4 chance of measuring B in the $|0\rangle$ state and 3/4 chance of the $|1\rangle$ state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

- Entangled, if we measure A in the $|0\rangle$ state we will always measure B in the $|0\rangle$ state, and vice versa
- Example of a **maximally entangled state**, also one of the **Bell states**

Entanglement (cont'd.)

- ⊗ Equivalent definition: a two-system state is entangled if the composite state cannot be factored
 - $\frac{1}{\sqrt{8}}|00\rangle + \frac{\sqrt{3}}{\sqrt{8}}|01\rangle + \frac{1}{\sqrt{8}}|10\rangle + \frac{\sqrt{3}}{\sqrt{8}}|11\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle_A + \frac{1}{\sqrt{2}}|1\rangle_A\right) \left(\frac{1}{2}|0\rangle_B + \frac{\sqrt{3}}{2}|1\rangle_B\right)$
- ⊗ Entanglement is generated by interactions between the two subsystems
- ⊗ States can be prepared using an **entangling gate** such as CNOT ("controlled NOT"), which flips the second qubit if the first qubit is 1

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{CNOT} \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)|0\rangle_B = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Entanglement (cont'd.)

- ⊗ A pair of qubits which are maximally entangled is also known as an **EPR pair** (short for Einstein–Podolsky–Rosen)
- ⊗ Bell states $\{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$ form alternative basis for two-qubit system
- ⊗ Is it possible for Alice to send Bob two bits of classical information by sending only one qubit?
 - Yes, if Alice and Bob share an EPR pair beforehand
 - Known as **superdense coding**

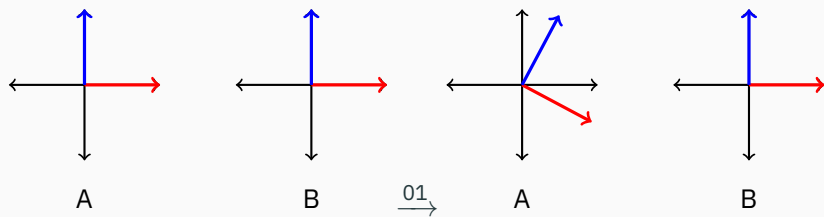
- ⚛ Quantum game theory allows for strategies which take advantage of effects such as quantum operations or entanglement
- ⚛ Players may improve their chances of winning without directly communicating if they share entangled qubits

Quantum game theory (cont'd.)

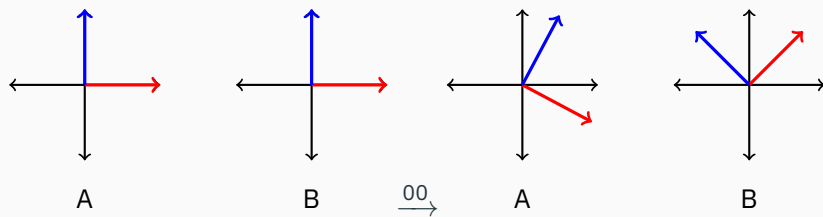
- ⚛ Alice and Bob play a game where they each receive a challenge bit and must send another bit in response; they win if the challenge string was 00 and the sum of the response bits is odd, or if the challenge string was anything else and the sum of the response bits is even
- ⚛ What is the best probability of winning they can get playing classically?
- ⚛ If Alice and Bob are allowed to share an EPR pair, what is their maximum probability of winning?

- ⊗ Solution: Alice agrees to rotate her state by -22.5° if she receives a 0 and 22.5° if she receives a 1
- ⊗ Bob rotates his state by 45° if he receives a 0 and 0° if he receives a 1
- ⊗ States are offset by 67.5° if the challenge string is 00 and 22.5° otherwise
 - They win with probability $\cos(22.5^\circ)^2 \approx 0.85$ no matter the challenge string

Quantum game theory (cont'd.)



Quantum game theory (cont'd.)



Magic squares game

- ⊗ Alice and Bob are asked to fill in one row and one column of a 3×3 square, respectively, with 0's and 1's such that Alice places an even number of 1's and Bob places an odd number of 1's
- ⊗ They win if their entries do not conflict with each other
- ⊗ What is the best probability of winning they can get playing classically?

Magic squares game (cont'd.)

- ⚛ Not possible to fill in a 3×3 square so that all rows have an even number of 1's and all columns have an odd number of 1's
- ⚛ If Alice and Bob agree on a particular square beforehand, the best they can do is $\frac{8}{9}$ if the row and column to fill in are randomly chosen

0	0	0
0	1	1
1	0	?

Magic squares game (cont'd.)

- ⊗ Alice and Bob can always win if they share two EPR pairs
- ⊗ Each of the qubits can be measured in the $Z = \{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\}$, $X = \{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}\}$ or $Y = \{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}\}$ basis
- ⊗ Let $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ correspond to 0 and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$ correspond to 1

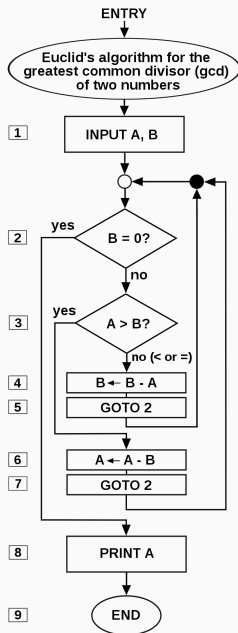
$1 + Z_2$	$Z_1 + 1$	$Z_1 + Z_2$
$X_1 + 1$	$1 + X_2$	$X_1 + X_2$
$1 + X_1 + Z_2$	$1 + Z_1 + X_2$	$Y_1 + Y_2$

Computation theory

What is a computer?

- ⚛ Computers are machines which can be programmed to perform a task by following a set of rules or instructions
- ⚛ These sets of instructions are known as **algorithms**

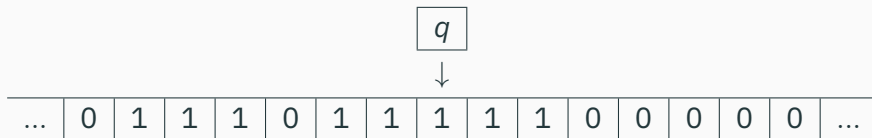
What is a computer? (cont'd.)



- ⚛ Study of what problems can be solved by computers and how efficiently or two what degree
- ⚛ **Computability** is the ability to effectively solve a problem
- ⚛ **Computational complexity** is a measure of how difficult a problem is to solve

- ⚛ **Models** provide a concrete framework for how instructions can be executed
- ⚛ **Turing machines** are the most common model used in classical computation
 - Consists of an infinite tape of symbols, a cursor, an internal state, and a set of instructions
 - May rewrite the cursor position, move forwards or back, or halt depending on the current state and the symbol at the cursor position
 - Can reproduce any classical algorithm

Models of computation (cont'd.)



- ⦿ What does it mean for a function to be computable?
- ⦿ Often interested in functions on the natural numbers, which can be enumerated
- ⦿ The **Church-Turing thesis** states that a function on the natural numbers can be calculated iff it can be computed by a Turing machine

Halting problem

- ⊛ Given an arbitrary program with integer input, is there a general algorithm to determine whether the program terminates?
- ⊛ Turing showed in 1936 that no such algorithm can be implemented on a Turing machine

Halting problem (cont'd.)

- ⊛ Since programs can be described by a finite set of instructions, they can be assigned a unique identifying positive integer i
- ⊛ All instructions consist of four entries: the internal state, the symbol at the current cursor position, what to write at the current cursor position, and whether to move left or right
- ⊛ Consider the representation $2^a 3^b 5^c \dots$ where a, b, c are the first, second, and third entries in the instructions

Halting problem (cont'd.)

- ⊛ Consider a function $h(i, x)$ which evaluates to 1 if program i halts on input x , and 0 otherwise
- ⊛ If $h(i, x)$ is computable for all i, x , we can represent it as a Turing machine program identified by a positive integer A
- ⊛ Consider a function $f(x)$ which returns 0 if $h(x, x) = 0$ and otherwise is undefined
 - Can be implemented by a program B which returns 0 if $h(x, x) = 0$ and otherwise loops forever

Halting problem (cont'd.)

- ⊛ What does $f(B)$ evaluate to?
- ⊛ If $f(B) = 0$, then $h(B, B) = 0$, which means that the program B does not halt on input B , which is a contradiction
- ⊛ If $f(B)$ is undefined, then $h(B, B) = 1$, which means that the program B halts on input B , which is also a contradiction

- ⦿ Often interested in quantifying how difficult a problem is
- ⦿ **Computational complexity** measures how the required time or memory resources scale with the size of the problem
- ⦿ An algorithm is said to be **efficient** if the resources required scale at most polynomial in the size of the problem

Complexity classes (cont'd.)

- ⦿ **P** is the class of all problems which can be solved by a deterministic Turing machine in polynomial time
- ⦿ **NP** is the class of all problems whose solutions can be *verified* by a deterministic Turing machine in polynomial time
- ⦿ **BPP** is the class of all problems which can be solved by a *probabilistic* Turing machine in polynomial time, with at most $1/3$ chance of error
- ⦿ Known that $P = NP \Rightarrow P = BPP$, so at least one of $P \neq NP$ and $P = BPP$ is true
 - Commonly believed that $P = BPP$

Quantum complexity theory

- ⊗ Any classical algorithm can also be computed on a quantum computer
- ⊗ P is a subset of **BQP**, the class of problems which can be solved by a quantum computer in polynomial time, with at most $1/3$ chance of error for any input
- ⊗ BQP is commonly believed to be more powerful than P
- ⊗ **Quantum supremacy** describes goal of implementing a quantum program which significantly outperforms classical computing technology

- ⚛ **Interactive proof systems** consist of a **prover** who demonstrate the validity of a password or string to a **verifier**
- ⚛ **MIP*** denotes multiprover interactive proof systems with entanglement
- ⚛ **RE** is the class of all problems whose solutions can be verified by a Turing machine and thus are no harder than the halting problem
- ⚛ Result published in 2020 uses quantum games to show that demonstrating entanglement is equivalent to proving computability of a problem

- ⦿ Noisy intermediate-scale quantum (NISQ) devices may be available soon
- ⦿ Google quantum supremacy announcement in October 2019
- ⦿ Quantum cryptography and secure communication applications
 - Quantum key distribution implementations have been demonstrated on distances of over 300 miles

Conclusion

- ⚛ Quantum computing is still a developing field
- ⚛ Remains to be seen whether all-purpose quantum computers will ever exist
- ⚛ Demonstrates important connections between different fields