Intro to Quantum Computations and Quantum Complexity

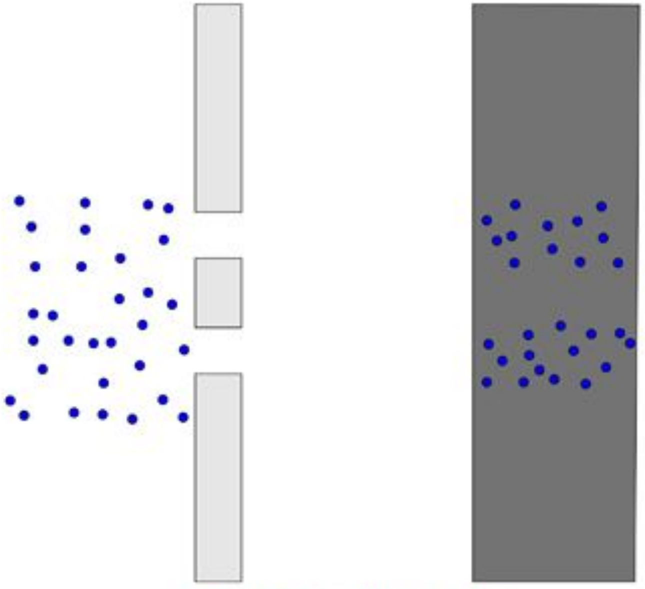
Orestis Chardouvelis

Contents

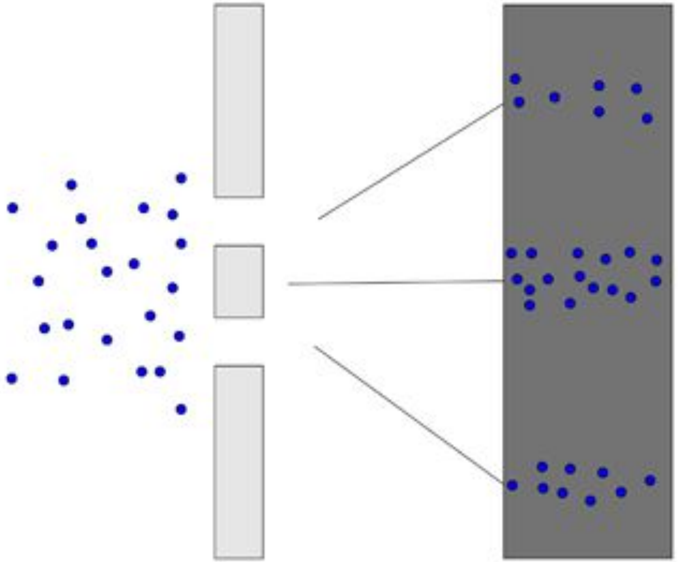
Contents

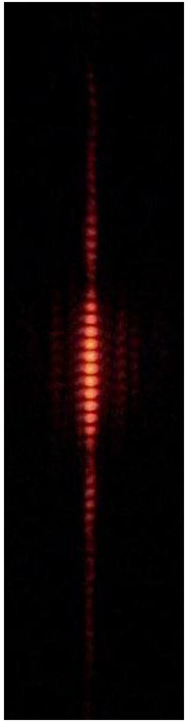
Quantum Physics

- The Double Slit Experiment



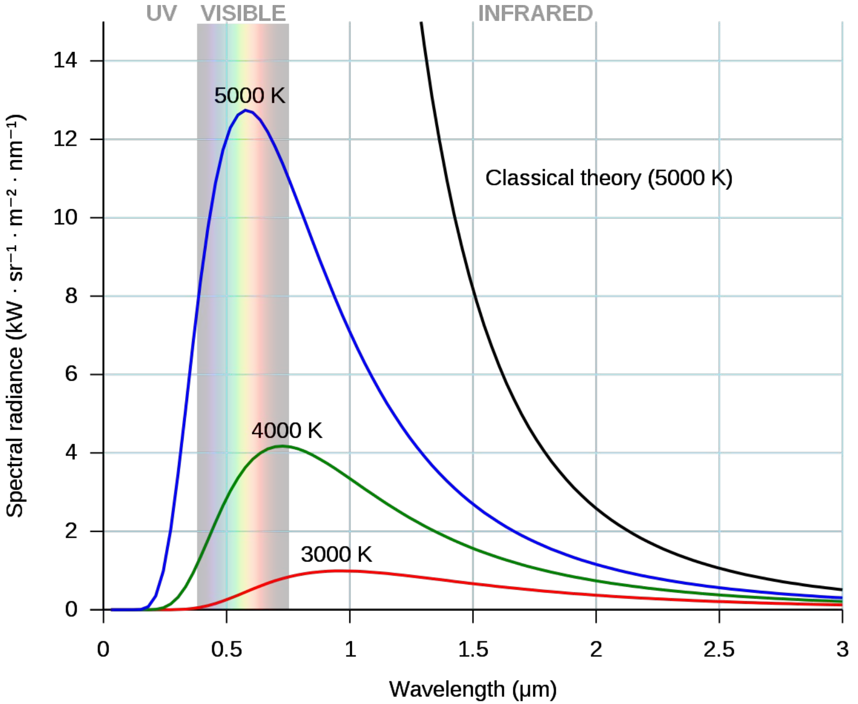
The pattern you get from particles.



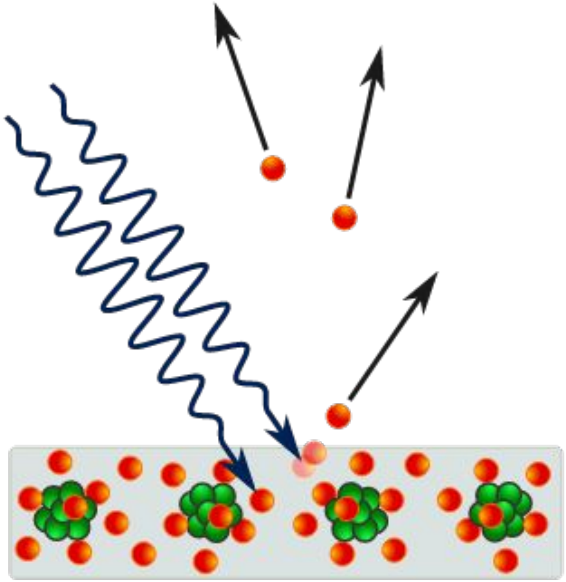


Quantum Physics

- Ultraviolet Catastrophe



- Photoelectric Effect



Quantum Mechanics

$|0\rangle$: photon having gone through the top slit

$|1\rangle$: photon having gone through the bottom slit

Photon can go through both:

$$\alpha |0\rangle + \beta |1\rangle$$

Classical vs Quantum

Quantum: generalization of classical probability theory

- amplitudes α,β
- $|\alpha|^2 + |\beta|^2 = 1$
- α,β can be negative
- α,β can be complex ($e^{i\theta}$, θ is phase shift)

Classical vs Quantum

Classical

- $\alpha + \beta = 1$
- $S \cdot \begin{pmatrix} a \\ b \end{pmatrix}$, S a stochastic matrix
- Classical probabilities are positive and will always add
- Operations preserve L_1 norm

Quantum

- $|\alpha|^2 + |\beta|^2 = 1$
- $U \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, U a unitary matrix
- Multiple paths to the same final answer can cause cancelations
- Operations preserve L_2 norm

Operations

- phase shifts
- bit flips
- Hadamard transformation

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Operations

- Generally, for some unitary U:

$$|0\rangle \rightarrow U_{00}|0\rangle + U_{01}|1\rangle$$
$$|1\rangle \rightarrow U_{10}|0\rangle + U_{11}|1\rangle$$

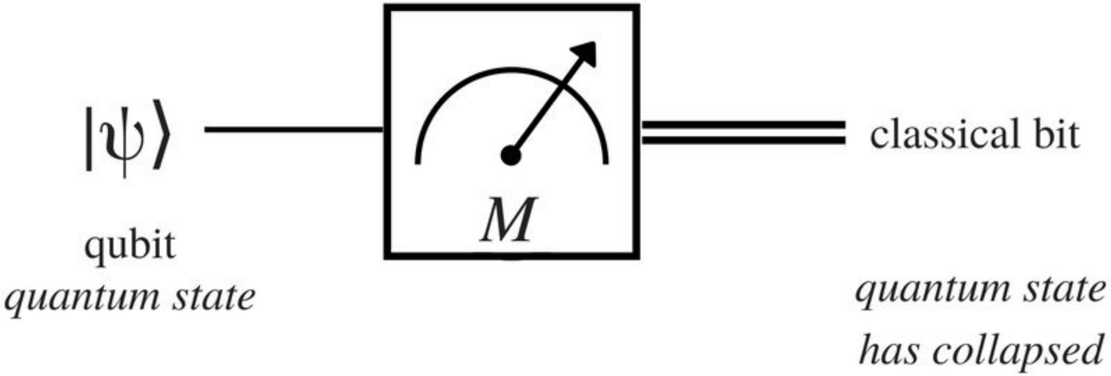
$$U = \begin{pmatrix} U_{00} & U_{10} \\ U_{10} & U_{11} \end{pmatrix}$$

- To preserve normalization,

$$U^\dagger U = I$$

$$U^\dagger = \begin{pmatrix} U_{00}^* & U_{01}^* \\ U_{10}^* & U_{11}^* \end{pmatrix}$$

Measurements



Contents

Quantum States

- B: a finite set of classical basis states

  B={top slit, bottom slit}

  B={0,...,n-1}
- A quantum state is a unit vector in $C^{|B|}$
- Only |B| complex numbers needed (amplitudes)

Quantum States

Syntax

- column vector ϕ with the "ket" symbol $|\phi\rangle$
- row vector $\phi^\dagger$ with the "bra" symbol $\langle\phi|$
- inner product with the "bra-ket" notation $\phi \cdot \psi = \langle\phi|\psi\rangle$

For B = {0,...,n-1}

- computational basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

- superposition

$$|\phi\rangle = \phi_0 |0\rangle + \phi_1 |1\rangle + \cdots + \phi_{n-1} |n-1\rangle .$$

Operations

Quantum Operations

Unitary Transformations

- $|\phi\rangle \mapsto U|\phi\rangle$.
- the state remains a unit vector

Measurements

quantum state
$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

- with probability $|\alpha|^2$: observe 0 and state collapses to $|0\rangle$
- with probability $|\beta|^2$: observe 1 and state collapses to $|1\rangle$

Joint Systems

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \bigotimes \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{bmatrix}$$

Consider two qubits

$$|\phi_0\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle$$
$$|\phi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$

- B = {0, 1} $\otimes$ {0, 1}
- computational basis: $|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle$
- Joint system:

$$\begin{aligned} |\phi_0\rangle |\phi_1\rangle &= (\alpha_0 |0\rangle + \beta_0 |1\rangle)(\alpha_1 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\alpha_1 |00\rangle + \alpha_0\beta_1 |01\rangle + \beta_0\alpha_1 |10\rangle + \beta_0\beta_1 |11\rangle \end{aligned}$$

Entanglement

A system of two qubits $|\varphi\rangle$ is entangled when it cannot be written as a tensor product of qubits $|\varphi_0\rangle$ and $|\varphi_1\rangle$.

e.g $$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Partial Measurement

- Joint System: $|\varphi\rangle = |\varphi_0\rangle\ |\varphi_1\rangle$

with probability $|\alpha_0|^2$: observe 0 and state collapses to $|0\rangle|\varphi_1\rangle$

with probability $|\beta_0|^2$: observe 1 and state collapses to $|1\rangle|\varphi_1\rangle$

- Entangled state: $|\psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle$

with probability $\|\psi_{00}\|^2 + \|\psi_{01}\|^2$: observe 0 and state collapses to $\dfrac{\psi_{00}|00\rangle + \psi_{01}|01\rangle}{\sqrt{\|\psi_{00}\|^2 + \|\psi_{01}\|^2}}$

with probability $\|\psi_{10}\|^2 + \|\psi_{11}\|^2$: observe 1 and state collapses to $\dfrac{\psi_{10}|10\rangle + \psi_{11}|11\rangle}{\sqrt{\|\psi_{10}\|^2 + \|\psi_{11}\|^2}}$

Partial Measurement

Example:

Entangled state: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Measuring first qubit:

- with probability 1/2: observe 0 and state collapses to $|0\rangle|0\rangle$
- with probability 1/2: observe 1 and state collapses to $|1\rangle|1\rangle$

Measuring second qubit: same result

Phase Changes

- Overall phase changes don't matter
  - there's no quantum operation to distinguish $|\psi\rangle$ from $a|\psi\rangle$, $|a|^2=1$
- Partial phase changes matter

example:

$$x = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \quad y = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\-1\end{pmatrix} \quad z = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

- U (y) = U (-x) = - U (x)

- H x = $(1,0)^T = |0\rangle$
- H z = $(0,1)^T = |1\rangle$

No-cloning

- No quantum procedure transforms $|\varphi\rangle \rightarrow |\varphi\rangle|\varphi\rangle$ for all φ.

- (weakened) There is no unitary transformation such that
  $U\,|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$ for all φ.

Proof. Suppose we have such a U. Then using $U^\dagger U = I$ we have for any ψ, ϕ

$$\begin{aligned} \langle\psi|\phi\rangle &= \langle 0|0\rangle \langle\psi|\phi\rangle \\ &= \langle\psi| \langle 0|\phi\rangle |0\rangle \\ &= \langle\psi| \langle 0|U^\dagger U\phi\rangle |0\rangle \\ &= \langle\psi| \langle\psi|\phi\rangle |\phi\rangle \\ &= |\langle\psi|\phi\rangle|^2. \end{aligned}$$

Thus taking ψ, ϕ neither orthogonal nor equal we reach a contradiction. $\square$

No-cloning

- No quantum procedure transforms |φ⟩→ |φ⟩|φ⟩ for all φ.

- (weakened) There is no unitary transformation such that U |φ⟩|0⟩= |φ⟩|φ⟩ for all φ.

Proof. Suppose we have such a U. Then using $U^\dagger U = I$ we have for any ψ, ϕ

$$\begin{aligned}\langle\psi|\phi\rangle &= \langle 0|0\rangle\,\langle\psi|\phi\rangle \\ &= \langle\psi|\,\langle 0|\phi\rangle\,|0\rangle \\ &= \langle\psi|\,\langle 0|U^\dagger U\phi\rangle\,|0\rangle \\ &= \langle\psi|\,\langle\psi|\phi\rangle\,|\phi\rangle \\ &= |\langle\psi|\phi\rangle|^2.\end{aligned}$$

Thus taking ψ, ϕ neither orthogonal nor equal we reach a contradiction. □

Limitation or Cryptographic Guarantee?

Quantum Systems for Classical Problems

Classical problems with quantum systems:

- classical function $f: \{0,1\}^n \rightarrow \{0,1\}^n$
- unitary transformation U: $U|x\rangle \rightarrow |f(x)\rangle$
- need to transform every classical function f into a bijective function

Reversible Computation

i.e. XOR: $(a,b) \rightarrow (c = a \oplus b)$

information is lost

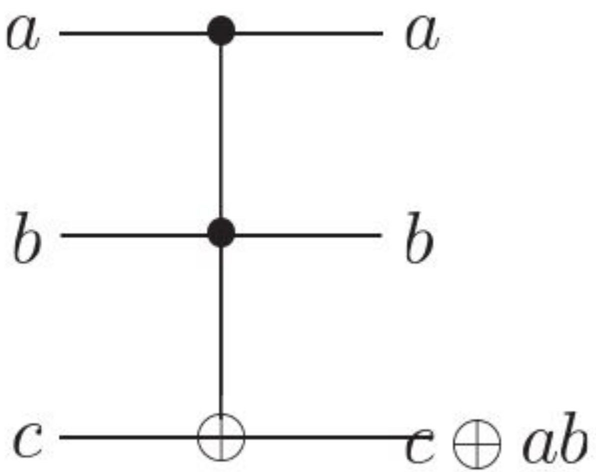
Landauer's Principle: Energy must be expended to lose information (and there is a particular conversion from amount of information lost to amount of energy that must be expended)

- cheat: $(a,b) \rightarrow (a,\ c = a \oplus b)$

Reversible Computation

Toffoli Gate

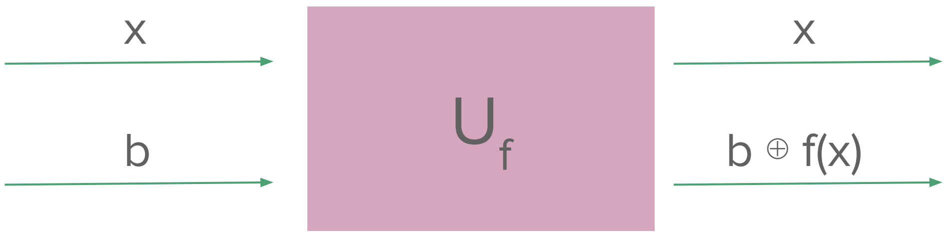
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Reversible Computation

Make $f: \{0,1\}^n \rightarrow \{0,1\}$ with auxiliary input

- $g(x,b) = (x, b \oplus f(x))$
  - it is its own inverse
  - its bijective



Reversible Computation

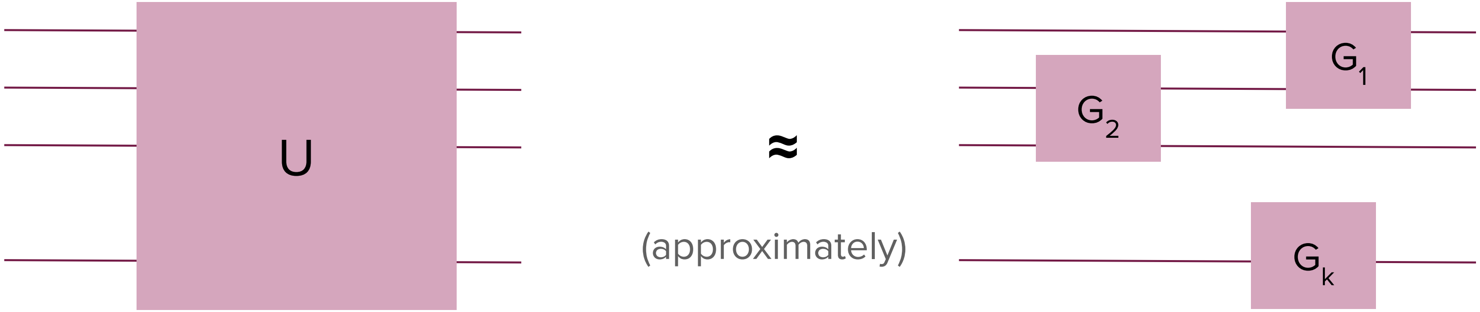
- efficient transformation from f to g
- every step reversible

- Suppose f: $\{0,1\}^n \rightarrow \{0,1\}$ is implemented by a circuit of s classical NAND gates. Then g can be implemented with ~2s Toffoli gates.

$$(x, 1^s, b) \rightarrow \boxed{h(x, 1^s), b} \rightarrow (x, w_1(x), \ldots, w_s(x), b) \rightarrow$$
$$\boxed{h'(x, w_1(x), \ldots, w_s(x)), b \oplus w_s(x)} \rightarrow (x, 1^s, b \oplus f(x))$$

Quantum Circuits

- classical: A finite set of gates S is universal if for any function f: $\{0,1\}^n \rightarrow \{0,1\}$, there exists a circuit with gates in S that computes f, i.e {NAND}, {AND, NOT}
- quantum: A finite set of unitaries S is universal if for every unitary U, there exists a circuit made up of unitaries from S that computes U
  - countably many ways to stitch unitaries from S
  - uncountably many unitary transformations



Quantum Universal Gate Sets

- $\{\text{Toffoli}, H, \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}\}$
- $\{CNOT, H, \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}\}$
- $\{\text{Toffoli}, CNOT, H, P\}$

$CNOT : (a, b) \to (a, a \oplus b)$

$P = \begin{pmatrix} 1 & \\ & i \end{pmatrix}$

Clifford gates: generated by $\{P, H, CNOT\}$

Classical vs Quantum Algorithms

Quantum Algorithm	Complexity	Classical Algorithm Complexity
Deutsch-Jozsa	constant	$\Theta(2^n)$
Simon's Problem	$O(n)$	$\Theta(2^{n/2})$
Grover Search	$\Theta(N^{1/2})$	$\Theta(N)$
Shor's Algorithm	$O(\log^3 N)$	subexponential

Contents

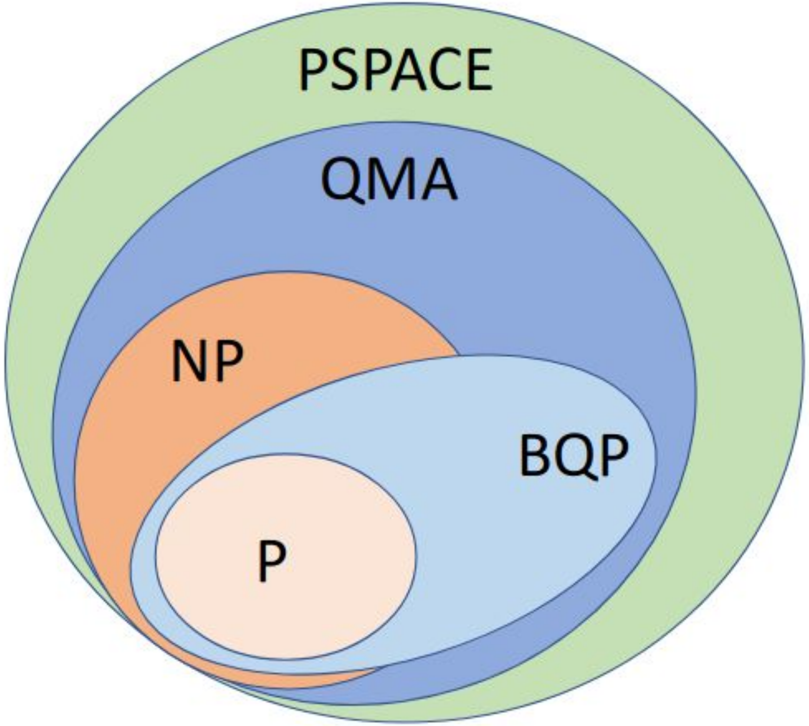
- Quantum Physics Intuition
- A Mathematical Model for Quantum Mechanics
- **Quantum Complexity**

Computational Complexity

How hard is it to solve a problem

How hard is it to verify a problem

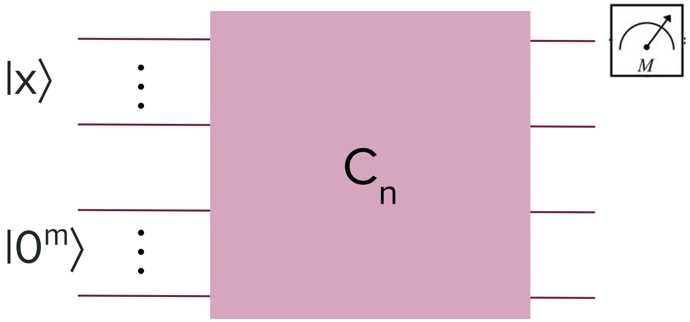
Quantum Complexity



BQP

- A language L is in Bounded-Error Quantum Polynomial Time (BQP) if there exists a universal family of polynomial size quantum circuits C_n such that for each x of length n:
  - If $x \in L \Rightarrow \Pr[C_n \text{ accepts } x] \geq 2/3$
  - If $x \notin L \Rightarrow \Pr[C_n \text{ accepts } x] \leq 1/3$

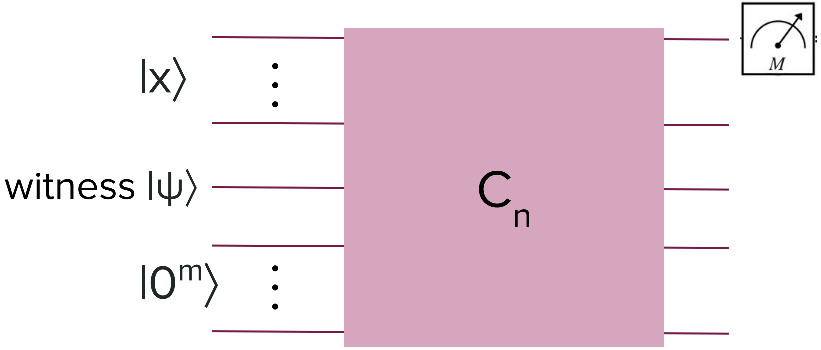
- Problems in BQP:
  - Factoring
  - Discrete Logarithm
  - Simulating Quantum Systems



QMA

- A language L is in Quantum Merlin-Arthur (QMA) if there exists a family of polynomial size quantum verifier circuits C_n such that for each x of length n:
  - If $x \in L \Rightarrow \exists\ |\psi\rangle$ $\Pr[C_n$ accepts $|x\rangle \otimes |\psi\rangle] \geq 2/3$
  - If $x \notin L \Rightarrow \forall |\psi\rangle$ $\Pr[C_n$ accepts $|x\rangle \otimes |\psi\rangle] \leq 1/3$

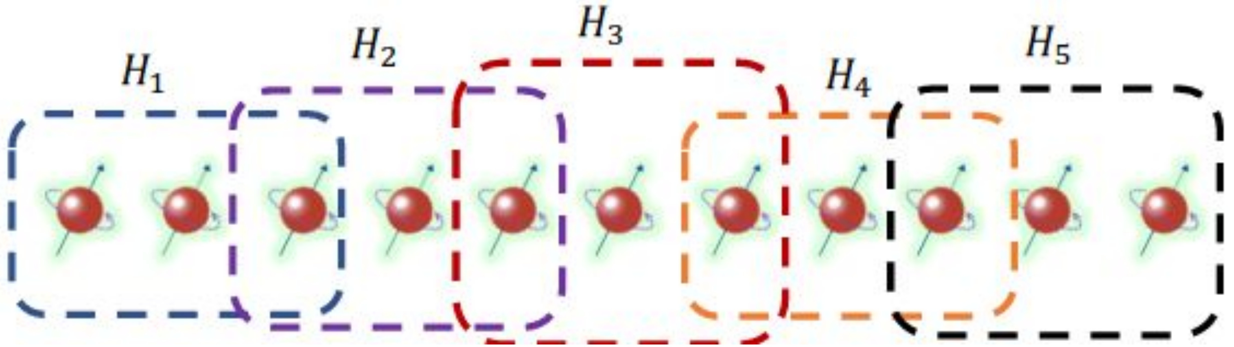
- Problems in QMA:
  - Local Hamiltonian Problem



Local Hamiltonian Problem

(k,α,β)-Local Hamiltonians problem (simplified): Given classical description of measurements $\{H_1, \ldots, H_n\}$ where each H_i acts on k qubits and has a two outcome measurement, decide whether there exists a quantum state $|\psi\rangle$ such that:

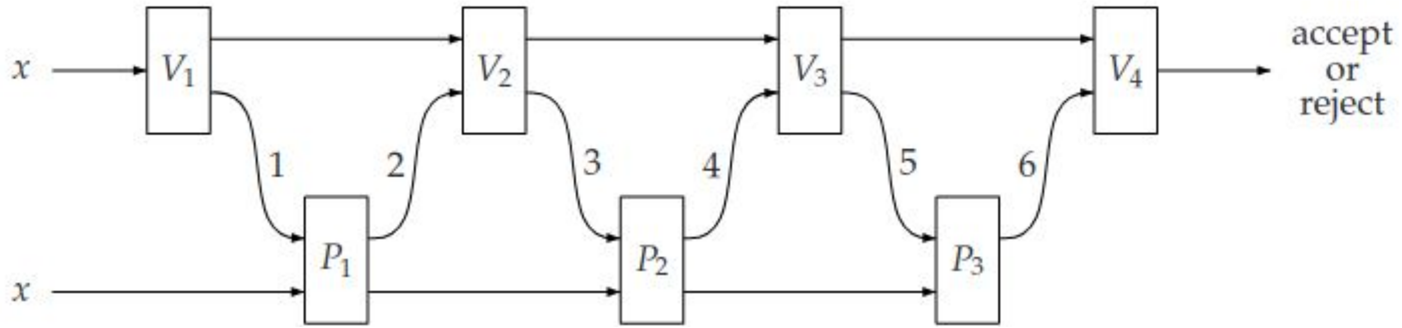
- $\sum_i$Pr[measuring $|\psi\rangle$ using H_i yields "Reject"] $\leq \alpha$ (YES case)
- $\sum_i$Pr[measuring $|\psi\rangle$ using H_i yields "Reject"] $\geq \beta$ (NO case)



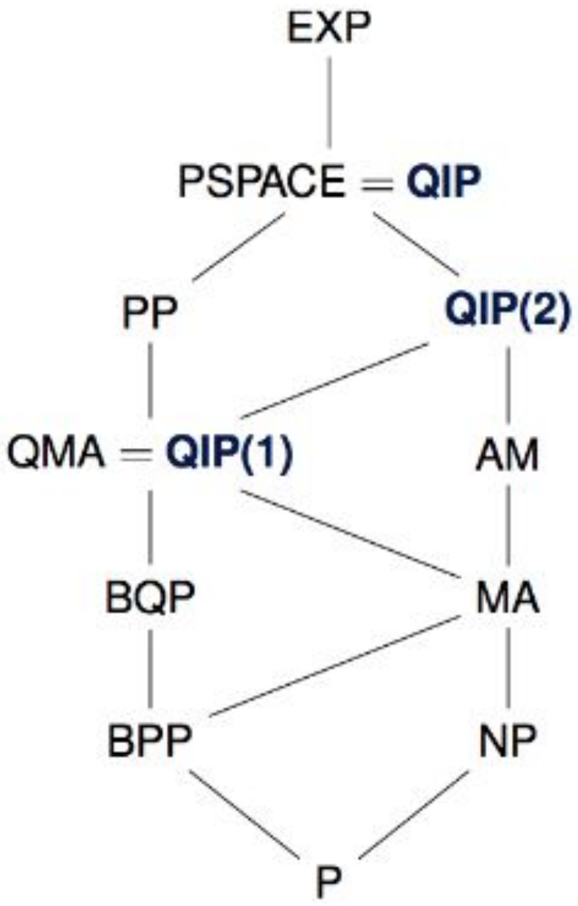
QIP

- A language L is in Quantum Interactive Proofs (QIP) if there exists a family of polynomial size quantum verifier circuits $V_{|x|}$ computable in poly(|x|) time such that for each x of length n:
  - If $x \in L \Rightarrow \exists$ P Pr[P persuades $V_{|x|}$ to accept] $\geq 2/3$
  - If $x \notin L \Rightarrow \forall$ P Pr[P persuades $V_{|x|}$ to accept] $\leq 1/3$

QIP(m)$_{m=6}$:



QIP



MIP*

Multi-Prover Interactive Proofs with Quantum Provers (MIP*) is the same as QIP, except that now the verifier can exchange messages with *many provers*, not just one. The provers cannot communicate with each other during the execution of the protocol, so the verifier can "cross-check" their assertions.

MIP* = RE

[Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen]

- Entangled states ➔ verifier doesn’t have to compute the question
- Different models for entanglement
  - tensor product model
  - commuting operator model of entanglement
- Calculate maximum winning percentage of nonlocal games
  - compute floor with algorithm using tensor product model
  - compute floor with algorithm using commuting operator model of entanglement
- Nonlocal game of halting problem

“That’s all Folks!”