Computation using Quantum Mechanics

Aly Ibrahim

McGill University

August 8, 2020

CLASSICAL v. QUANTUM

Classical Computer

Maxwell's Equations	Condensed Matter (Solid State)

Classical Computer

Circuits: Ohm's Law + Kirchoff's Laws ***AC, Resistance, Inductor, Capacitor***	**Electronics: Transistors** ***Switch***
Maxwell's Equations	**Condensed Matter (Solid State)**

Classical Computer

Digital Abstraction: Boolean Algebra

AND, OR, NOT

Circuits: Ohm's Law + Kirchoff's Laws

AC, Resistance, Inductor, Capacitor

Electronics: Transistors

Switch

Maxwell's Equations

Condensed Matter (Solid State)

Quantum Mechanics by Example

Time-independent 1-D Schrödinger Equation is

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$

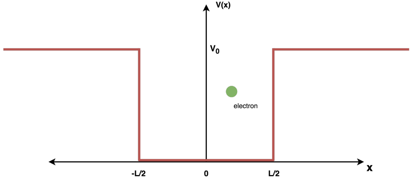
Quantum Mechanics by Example

Time-independent 1-D Schrödinger Equation is

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$

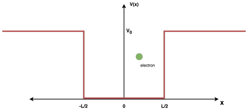
where
$\hbar$ is Plank's constant / 2π
m is the mass of the particle
ψ is a complex valued wavefunction
$V(x)$ is the potential energy at point x
E is the total energy of the particle.

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$

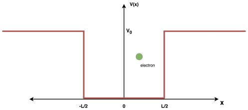


$$\psi = \begin{cases} \psi_l, & \text{if } x \leqslant -L/2 \\ \psi_m, & \text{if } -L/2 \leqslant x \leqslant L/2 \\ \psi_r, & \text{if } x \geqslant L/2 \end{cases}$$

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$

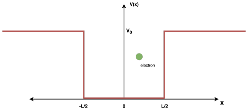


$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



$$-\frac{\hbar^2}{2m}\frac{d^2\psi_m}{dx^2} = E\psi_m$$

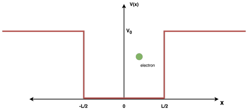
$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



$$-\frac{\hbar^2}{2m}\frac{d^2\psi_m}{dx^2} = E\psi_m$$

Let $k = \frac{\sqrt{2mE}}{\hbar}$, we get $\frac{d^2\psi_m}{dx^2} = -k^2\psi_m$

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$

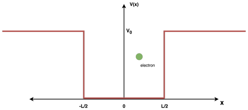


$$-\frac{\hbar^2}{2m}\frac{d^2\psi_m}{dx^2} = E\psi_m$$

Let $k = \frac{\sqrt{2mE}}{\hbar}$, we get $\frac{d^2\psi_m}{dx^2} = -k^2\psi_m$

So $\psi_m = A\cos(kx) + B\sin(kx)$

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$

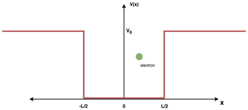


$$-\frac{\hbar^2}{2m}\frac{d^2\psi_m}{dx^2} = E\psi_m$$

Let $k = \frac{\sqrt{2mE}}{\hbar}$, we get $\frac{d^2\psi_m}{dx^2} = -k^2\psi_m$

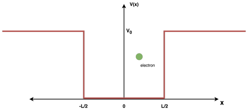
So $\psi_m = A\cos(kx) + B\sin(kx)$ for any $k \in \mathbb{R}$.

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



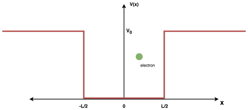
If $V_0 > E$,

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



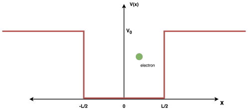
If $V_0 > E$, letting $\kappa = \frac{\sqrt{2m(V_0 - E)}}{\hbar}$, gives us $\frac{d^2\psi_l}{dx^2} = \kappa^2\psi_l$

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



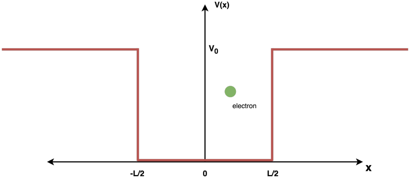
If $V_0 > E$, letting $\kappa = \frac{\sqrt{2m(V_0 - E)}}{\hbar}$, gives us $\frac{d^2\psi_l}{dx^2} = \kappa^2\psi_l$
So $\psi_l = Ce^{-\kappa x} + De^{\kappa x}$.

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



If $V_0 > E$, letting $\kappa = \frac{\sqrt{2m(V_0 - E)}}{\hbar}$, gives us $\frac{d^2\psi_l}{dx^2} = \kappa^2\psi_l$
So $\psi_l = Ce^{-\kappa x} + De^{\kappa x}$. Similarly, $\psi_r = Ee^{-\kappa x} + Fe^{\kappa x}$

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V(x)\psi = E\psi$$



$$\psi = \begin{cases} \psi_l = Ce^{-\kappa x} + De^{\kappa x}, & \text{if } x \leqslant -L/2 \\ \psi_m = A\cos(kx) + B\sin(kx), & \text{if } -L/2 \leqslant x \leqslant L/2 \\ \psi_r = Ee^{-\kappa x} + Fe^{\kappa x}, & \text{if } x \geqslant L/2 \end{cases}$$

$$\psi = \begin{cases} \psi_l = De^{\kappa x}, & \text{if } x \leqslant -L/2 \\ \psi_m = A\cos(kx) + B\sin(kx), & \text{if } -L/2 \leqslant x \leqslant L/2 \\ \psi_r = Ee^{-\kappa x}, & \text{if } x \geqslant L/2 \end{cases}$$

$$\psi = \begin{cases} \psi_l = De^{\kappa x}, & \text{if } x \leqslant -L/2 \\ \psi_m = A\cos(kx) + B\sin(kx), & \text{if } -L/2 \leqslant x \leqslant L/2 \\ \psi_r = Ee^{-\kappa x}, & \text{if } x \geqslant L/2 \end{cases}$$

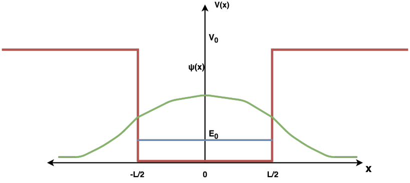
$\psi_l(\frac{-L}{2}) = \psi_m(\frac{-L}{2})$,
$\psi_m(\frac{L}{2}) = \psi_r(\frac{L}{2})$,
$\frac{\psi_l}{dx}(\frac{-L}{2}) = \frac{\psi_m}{dx}(\frac{-L}{2})$,
and $\frac{\psi_m}{dx}(\frac{L}{2}) = \frac{\psi_r}{dx}(\frac{L}{2})$.

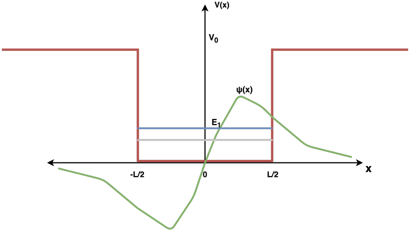
$\kappa = k \tan(\frac{kL}{2})$ (symmetric) or $\kappa = -k \cot(\frac{kL}{2})$ (asymmetric).

$\kappa = k \tan(\frac{kL}{2})$ (symmetric) or $\kappa = -k \cot(\frac{kL}{2})$ (asymmetric). These constraints restrict k, κ and hence the energies E_i to be discrete values $E_0, E_1, E_2, \ldots$.

$\kappa = k\tan(\frac{kL}{2})$ (symmetric) or $\kappa = -k\cot(\frac{kL}{2})$ (asymmetric). These constraints restrict k, κ and hence the energies E_i to be discrete values $E_0, E_1, E_2, \ldots$. We can make E_0 logical zero bit, and any $E_{i\geqslant 1}$ to be logical one bit.

$\kappa = k\tan(\frac{kL}{2})$ (symmetric) or $\kappa = -k\cot(\frac{kL}{2})$ (asymmetric). These constraints restrict k, κ and hence the energies E_i to be discrete values $E_0, E_1, E_2, \ldots$. We can make E_0 logical zero bit, and any $E_{i\geqslant 1}$ to be logical one bit.





Quantum Computer

Quantum Mechanics

Quantum Computer

- Energy Levels in Harmonic Oscillators
- Location of Single Optical Photon in 2 Cavities
- Polarization of Photons
- Nuclear spin state of an ion in a magnetic field
- Spin of a Nucleus

- Laser pulses
- Magnetic fields
- Electric fields
- Beam splitters
- Phase shifters

Quantum Mechanics

Quantum Computer

Quantum Gates and Circuits

Toffoli, Hadamard, Controlled NOT, X, Z, S, T

- Energy Levels in Harmonic Oscillators
- Location of Single Optical Photon in 2 Cavities
- Polarization of Photons
- Nuclear spin state of an ion in a magnetic field
- Spin of a Nucleus

- Laser pulses
- Magnetic fields
- Electric fields
- Beam splitters
- Phase shifters

Quantum Mechanics

QUANTUM DYNAMICS

Mathematical Modelling

$$\left[-\frac{\hbar^2}{2m}\frac{d^2}{dx^2}+V(x)\right]\psi(x)=E\psi(x) \implies H\left|\psi\right\rangle = E\left|\psi\right\rangle$$

Mathematical Modelling

$$\left[-\frac{\hbar^2}{2m}\frac{d^2}{dx^2}+V(x)\right]\psi(x)=E\psi(x) \implies H\left|\psi\right\rangle = E\left|\psi\right\rangle$$

Definition (Hilbert Space)

A complete complex inner product vector space.

Definition (Dirac Notation)

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^{\dagger}$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.

The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.

The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.

The norm is denoted by $||v||^2 = \langle v|v\rangle$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.

The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.

The norm is denoted by $||v||^2 = \langle v|v\rangle$.

An operator A is a linear map $A : \mathcal{H} \rightarrow \mathcal{H}$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.

The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.

The norm is denoted by $||v||^2 = \langle v|v\rangle$.

An operator A is a linear map $A : \mathcal{H} \to \mathcal{H}$.

The Lie Bracket for $\mathcal{H}$ is $[A, B] = AB - BA$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.

The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.

The norm is denoted by $||v||^2 = \langle v|v\rangle$.

An operator A is a linear map $A : \mathcal{H} \to \mathcal{H}$.

The Lie Bracket for $\mathcal{H}$ is $[A, B] = AB - BA$.

Hermitian operators, H, are operators that obey $H = H^\dagger$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.
The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.
The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.
The norm is denoted by $||v||^2 = \langle v|v\rangle$.
An operator A is a linear map $A : \mathcal{H} \to \mathcal{H}$.
The Lie Bracket for $\mathcal{H}$ is $[A, B] = AB - BA$.
Hermitian operators, H, are operators that obey $H = H^\dagger$.
Projectors are Hermitian operators, P, obeying $P^2 = P$.

Definition (Dirac Notation)

A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$.

The complex conjugate is then called a bra: $\langle v| = |v\rangle^\dagger$.

The inner product is denoted by the bra-c-ket $\langle u|v\rangle$.

The norm is denoted by $||v||^2 = \langle v|v\rangle$.

An operator A is a linear map $A : \mathcal{H} \rightarrow \mathcal{H}$.

The Lie Bracket for $\mathcal{H}$ is $[A, B] = AB - BA$.

Hermitian operators, H, are operators that obey $H = H^\dagger$.

Projectors are Hermitian operators, P, obeying $P^2 = P$.

Unitary operators, U, obeying $UU^\dagger = U^\dagger U = I$.

Postulate (Quantum States)

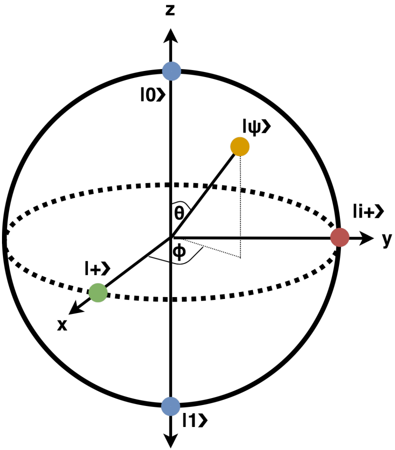
A closed quantum system is represented by a Hilbert space, $\mathcal{H}$, known as a state space, which is fully described by a state vector, $|\psi\rangle \in \mathcal{H}$ with $\|\psi\| = 1$.

Postulate (Quantum States)

A closed quantum system is represented by a Hilbert space, $\mathcal{H}$, known as a state space, which is fully described by a state vector, $|\psi\rangle \in \mathcal{H}$ with $||\psi|| = 1$.

Definition (Quantum Bits (Qubits))

A qubit is the simplest quantum system and is represented by a 2-dimensional Hilbert space $\mathcal{H}$. A canonical basis spanning $\mathcal{H}$ is $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Making any arbitrary state vector $|\psi\rangle \in \mathcal{H}$ be written as $\alpha |0\rangle + \beta |1\rangle$, where $\alpha, \beta \in \mathbb{C}$ are called probability amplitudes constrained that $|\alpha|^2 + |\beta|^2 = 1$.

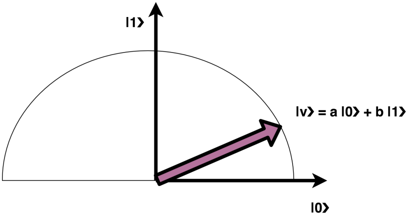

z
|0❯
|ψ❯
θ
|i+❯
y
ϕ
|+❯
x
|1❯

Definition (Superposition)

If $\alpha \neq 0$ and $\beta \neq 0$ then we say $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is in a superposition of logical zero $|0\rangle$ and logical one $|1\rangle$.

Definition (Superposition)

If $\alpha \neq 0$ and $\beta \neq 0$ then we say $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ is in a superposition of logical zero $|0\rangle$ and logical one $|1\rangle$.

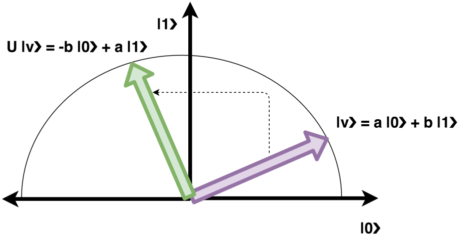


Postulate (Quantum Evolution)

A closed quantum system, $|\psi_{t=0}\rangle$, evolves according a unitary operator U (for time T) to reach the (new) state $|\psi_{t=T}\rangle$ written as $|\psi_{t=T}\rangle = U|\psi_{t=0}\rangle$.

Postulate (Quantum Evolution)

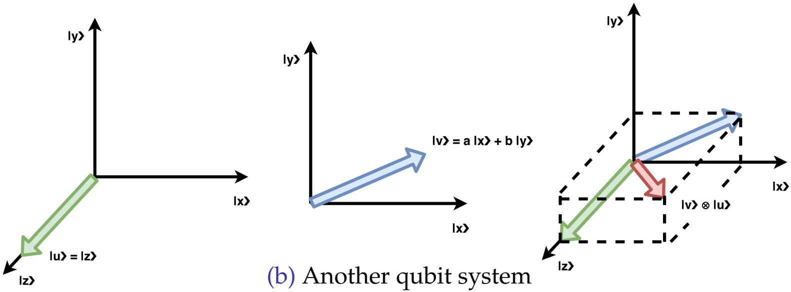
A closed quantum system, $|\psi_{t=0}\rangle$, evolves according a unitary operator U (for time T) to reach the (new) state $|\psi_{t=T}\rangle$ written as $|\psi_{t=T}\rangle = U\,|\psi_{t=0}\rangle$.



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

Postulate (Quantum state composition)

The state space representing a composition of multiple (possibly interacting) closed quantum systems is defined by the tensor product of the state spaces of the individual quantum systems, and is written as the product state $|\psi_1\rangle \otimes |\psi_2\rangle$*, where* $|\psi_1\rangle \in \mathcal{H}_1$ *and* $|\psi_2\rangle \in \mathcal{H}_2$ *and dimension* $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ *is the product of their dimensions.*



(a) A qubit system $|u\rangle$.

(b) Another qubit system $|v\rangle$.

(c) A composition of both systems $|v\rangle \otimes |u\rangle$.

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} x & y \\ z & l \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} x & y \\ z & l \end{pmatrix} & b \begin{pmatrix} x & y \\ z & l \end{pmatrix} \\ c \begin{pmatrix} x & y \\ z & l \end{pmatrix} & d \begin{pmatrix} x & y \\ z & l \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ax & ay & bx & by \\ az & al & bz & bl \\ cx & cy & dx & dy \\ cz & cl & dz & dl \end{pmatrix}$$

Definition (Quantum Entanglement)

We say a quantum state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is entangled if it cannot be decomposed/factored into a tensor product of constituents of the sub-systems $\mathcal{H}_1$ and $\mathcal{H}_2$, namely $\forall\ |\psi_1\rangle \in \mathcal{H}_1, |\psi_2\rangle \in \mathcal{H}_2$

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$$

Table: The four Bell Basis states represent the simplest maximally entangled two qubit systems

Symbol	Expansion in Tensor Product of Canonical Basis
$\|\Phi^+\rangle$	$\frac{1}{\sqrt{2}}\left(\|00\rangle_{AB} + \|11\rangle_{AB}\right)$
$\|\Phi^-\rangle$	$\frac{1}{\sqrt{2}}\left(\|00\rangle_{AB} - \|11\rangle_{AB}\right)$
$\|\Psi^+\rangle$	$\frac{1}{\sqrt{2}}\left(\|01\rangle_{AB} + \|10\rangle_{AB}\right)$
$\|\Psi^-\rangle$	$\frac{1}{\sqrt{2}}\left(\|01\rangle_{AB} - \|10\rangle_{AB}\right)$

Table: The four Bell Basis states represent the simplest maximally entangled two qubit systems

Symbol	Expansion in Tensor Product of Canonical Basis
$\|\Phi^+\rangle$	$\frac{1}{\sqrt{2}}\left(\|00\rangle_{AB} + \|11\rangle_{AB}\right)$
$\|\Phi^-\rangle$	$\frac{1}{\sqrt{2}}\left(\|00\rangle_{AB} - \|11\rangle_{AB}\right)$
$\|\Psi^+\rangle$	$\frac{1}{\sqrt{2}}\left(\|01\rangle_{AB} + \|10\rangle_{AB}\right)$
$\|\Psi^-\rangle$	$\frac{1}{\sqrt{2}}\left(\|01\rangle_{AB} - \|10\rangle_{AB}\right)$

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \xi\,|1\rangle) =$$
$$\alpha\gamma\,|00\rangle + \alpha\xi\,|01\rangle + \beta\gamma\,|10\rangle + \beta\xi\,|11\rangle$$

Definition (No-Cloning Theorem)

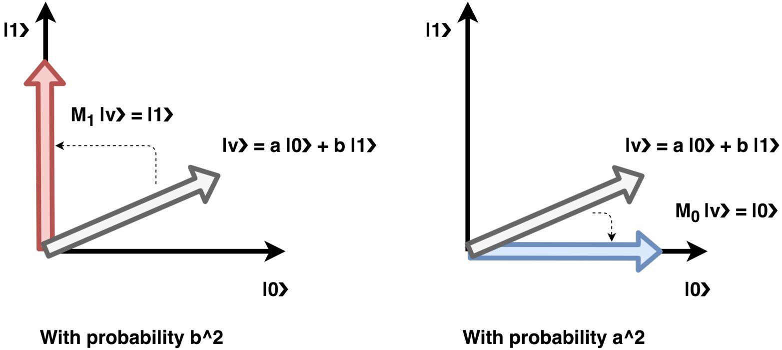
Creating an identical copy of an arbitrary unknown quantum state without destroying the original is impossible.

Postulate (Quantum Measurement)

An open quantum system, $|\psi_{\text{Pre}}\rangle$, interacts with the rest of the world in non-unitary evolution. Let us model this external system interacting with our quantum system by a collection of measurement operators (for our purposes these will be projectors) $\{M_b\}$ where b represents the measurement outcome and $\sum_b M_b^\dagger M_b = I$. The result of this interaction is the collapse of $|\psi_{\text{Pre}}\rangle$ to

$$|\psi_{\text{Post}}\rangle = \frac{M_b |\psi_{\text{Pre}}\rangle}{\sqrt{\langle\psi_{\text{Pre}}| M_b^\dagger M_b |\psi_{\text{Pre}}\rangle}}$$

for a specific b, where the probability for any particular b, $Pr[b] = \langle\psi_{\text{Pre}}| M_b^\dagger M_b |\psi_{\text{Pre}}\rangle$


|1❯
M1 |v❯ = |1❯
|v❯ = a |0❯ + b |1❯
|0❯
With probability b^2
|1❯
|v❯ = a |0❯ + b |1❯
M0 |v❯ = |0❯
|0❯
With probability a^2

In quantum mechanics Hermitian operators are associated with observables.

In quantum mechanics Hermitian operators are associated with observables. The eigenvalues of a Hermitian operator are the possible measured values of the observables.

In quantum mechanics Hermitian operators are associated with observables. The eigenvalues of a Hermitian operator are the possible measured values of the observables. A Hermitian operator, H, has eigenvectors $|v_i\rangle \in \mathcal{H}$ each with real eigenvalue λ_i.

In quantum mechanics Hermitian operators are associated with observables. The eigenvalues of a Hermitian operator are the possible measured values of the observables. A Hermitian operator, H, has eigenvectors $|v_i\rangle \in \mathcal{H}$ each with real eigenvalue λ_i. The eigenvectors are orthonormal and they span $\mathcal{H}$.

In quantum mechanics Hermitian operators are associated with observables. The eigenvalues of a Hermitian operator are the possible measured values of the observables. A Hermitian operator, H, has eigenvectors $|v_i\rangle \in \mathcal{H}$ each with real eigenvalue λ_i. The eigenvectors are orthonormal and they span $\mathcal{H}$. The eigenvalue is the observed physical quantity, and the corresponding eigenvector is the state of the system after measurement.

Definition (Heisenberg Uncertainty Principle)

Let A, B be two Hermitian operators (aka. observables). Then the following inequality always holds:

$$(\Delta A)^2(\Delta B)^2 \geqslant \left(\langle\Psi| \frac{1}{2i}[A, B] |\Psi\rangle \right)^2$$

Definition (Heisenberg Uncertainty Principle)

Let A, B be two Hermitian operators (aka. observables). Then the following inequality always holds:

$$(\Delta A)^2(\Delta B)^2 \geqslant \left(\langle\Psi| \frac{1}{2i}[A, B] |\Psi\rangle \right)^2$$

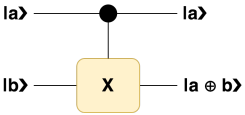
example: $\Delta x \Delta p \geqslant \frac{\hbar}{2}$

QUANTUM COMPUTATION

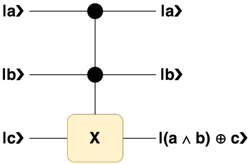
Quantum Gates

Pauli-X / NOT	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
Pauli-Y / Rotation by π around y-axis	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto i \begin{pmatrix} -\beta \\ \alpha \end{pmatrix}$
Pauli-Z / Rotation by π around z-axis	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$
Hadamard H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$
$S = \sqrt{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ i\beta \end{pmatrix}$
$T = \sqrt{S}$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ e^{i\pi/4}\beta \end{pmatrix}$

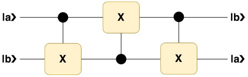
Quantum Gates



(a) Controlled NOT



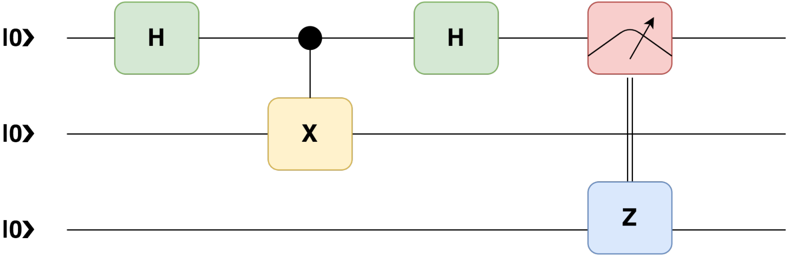
(b) Toffoli

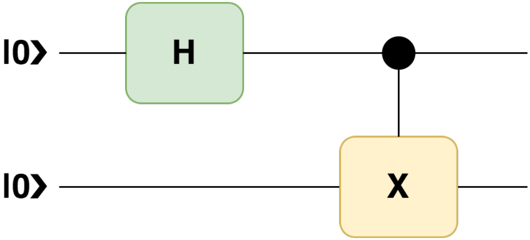


(c) Swap

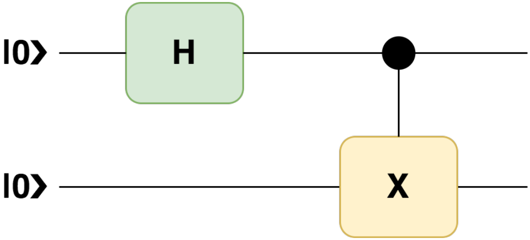
Universal Quantum Gate Sets

- CNOT and all single qubit gates.
- Toffoli, Hadamard, and S gates.
- CNOT, Hadamard, and T gates.

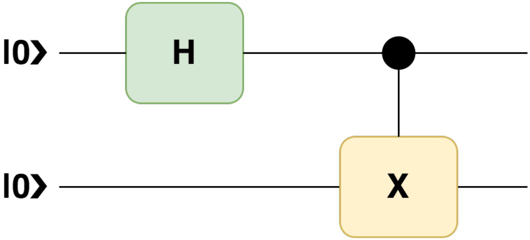

|0❯
|0❯
|0❯
H
X
H
Z



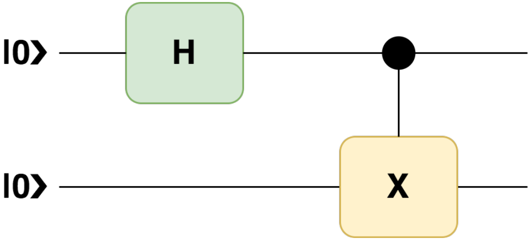
$|0,0\rangle$



$$|0,0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle$$



$$|0,0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle+|10\rangle}{\sqrt{2}}$$



$$|0,0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle+|10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

Quantum Fourier Transformation

DFT: $y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$. Time $O(N \log N)$

QFT: $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$. Time $O(\log^2 N)$

Quantum Fourier Transformation

DFT: $y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$. Time $O(N \log N)$

QFT: $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$. Time $O(\log^2 N)$

$$\begin{pmatrix} y_0 \\ y_1 \\ \dots \\ y_k \\ \dots \\ y_{N-1} \end{pmatrix}, \begin{pmatrix} x_0 \\ x_1 \\ \dots \\ \dots \\ \dots \\ x_{N-1} \end{pmatrix}$$

i is the imaginary number.

$$f(t) = \text{constant} \rightarrow \text{QFT}(f(t)) = \delta(0)$$

$$f(t) = \text{constant} \rightarrow \text{QFT}(f(t)) = \delta(0)$$

$$f(t) = \sin(f_0 \cdot t) \rightarrow \text{QFT}(f(t)) = \delta(f_0), \text{ for some frequency } f_0.$$

$$f(t) = \text{constant} \rightarrow \text{QFT}(f(t)) = \delta(0)$$

$$f(t) = \sin(f_0 \cdot t) \rightarrow \text{QFT}(f(t)) = \delta(f_0), \text{ for some frequency } f_0.$$

$$f(t) = \delta(t_0) \rightarrow \text{QFT}(f(t)) = \sin(t_0 f), \text{ for some time instant } t_0.$$

$$f(t) = \text{constant} \to \text{QFT}(f(t)) = \delta(0)$$

$$f(t) = \sin(f_0 \cdot t) \to \text{QFT}(f(t)) = \delta(f_0), \text{ for some frequency } f_0.$$

$$f(t) = \delta(t_0) \to \text{QFT}(f(t)) = \sin(t_0 f), \text{ for some time instant } t_0.$$

Differentiation in time domain $\frac{df(t)}{dt}$ becomes multiplication by frequency $i2\pi f$.

$$f(t) = \text{constant} \rightarrow \text{QFT}(f(t)) = \delta(0)$$

$$f(t) = \sin(f_0 \cdot t) \rightarrow \text{QFT}(f(t)) = \delta(f_0), \text{ for some frequency } f_0.$$

$$f(t) = \delta(t_0) \rightarrow \text{QFT}(f(t)) = \sin(t_0 f), \text{ for some time instant } t_0.$$

Differentiation in time domain $\frac{df(t)}{dt}$ becomes multiplication by frequency $i2\pi f$.
Convolution in time is multiplication in frequency:
$\text{QFT}(x * y) = \text{QFT}(x) \cdot \text{QFT}(y)$

Let $N = 2^n$, $|j\rangle = |j_1, j_2, .., j_n\rangle$, and $0.j_1 j_2 ... j_n = j/2^n$. Then

$$|j\rangle \to \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^{n/2}} |k\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} e^{2\pi i j(\sum_{l=1}^{n} k_l 2^{-l})} |k_1 ... k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_1=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right]$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n} |1\rangle\right)..\left(|0\rangle + e^{2\pi i 0.j_1..j_n} |1\rangle\right)}{2^{n/2}}$$

$$\text{Let } R_k \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i(2\pi/2^k)} \end{pmatrix}, R_1 = Z, R_2 = S \text{ and } R_3 = T$$

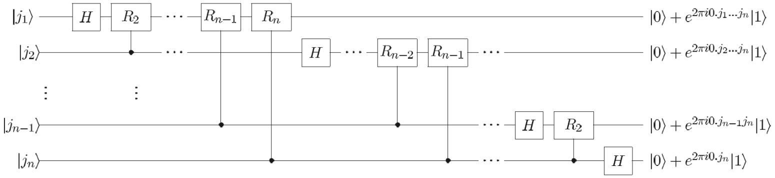


Image source from Mike and Ike.

QUANTUM ALGORITHMS

DEUTSCH'S ALGORITHM

Deutsch's Algorithm

Consider All functions $f : \{0,1\} \rightarrow \{0,1\}$:

Function #1: $f(x) = 0$ (the constant zero function)

Function #2: $f(x) = 1$ (the constant one function)

Function #3: $f(x) = x$ (the identity function)

Function #4: $f(x) = \overline{x}$ (the inverse function)

Deutsch's Algorithm

Consider All functions $f : \{0,1\} \to \{0,1\}$:

Function #1: $f(x) = 0$ (the constant zero function)

Function #2: $f(x) = 1$ (the constant one function)

Function #3: $f(x) = x$ (the identity function)

Function #4: $f(x) = \overline{x}$ (the inverse function)

Functions #1 and #2 are constant functions, functions #3 and #4 are called balanced functions.

Deutsch's Algorithm (cont.)

Imagine I pick one of the 4 functions, f, uniformly at random. How many queries do you need to determine if f is constant or balanced?

Deutsch's Algorithm (cont.)

Imagine I pick one of the 4 functions, f, uniformly at random. How many queries do you need to determine if f is constant or balanced?

Classically you would need 2 calls ($f(0)$ and $f(1)$).

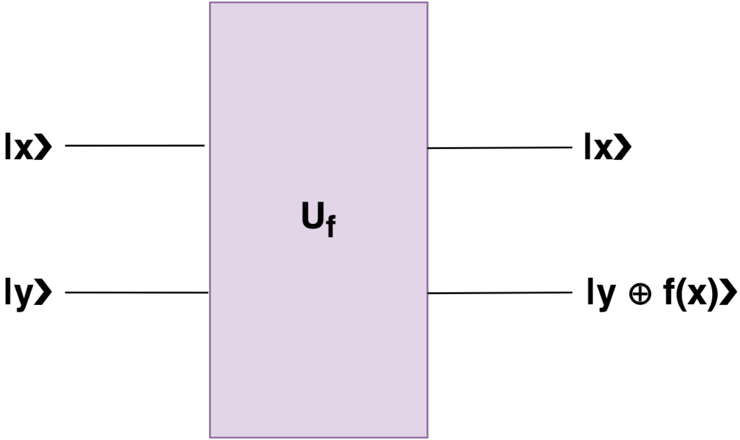
Deutsch's Algorithm (cont.)

Imagine I pick one of the 4 functions, f, uniformly at random. How many queries do you need to determine if f is constant or balanced?

Classically you would need 2 calls ($f(0)$ and $f(1)$).

Quantumly you would need only 1 call!

Quantum-izing a Function



Deutsch's Algorithm

Recall $H|0\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Deutsch's Algorithm

Recall $H|0\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

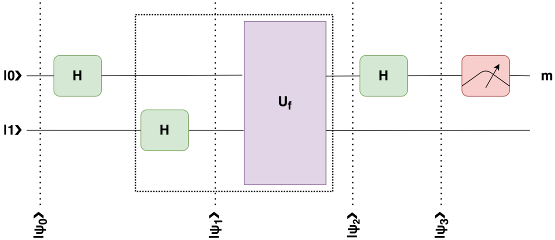
Furthermore, $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, which is a kind of Fourier Transform.

Deutsch's Algorithm

Recall $H|0\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Furthermore, $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, which is a kind of Fourier Transform.
Finally we denote by $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$.

Deutsch's Algorithm (cont.)

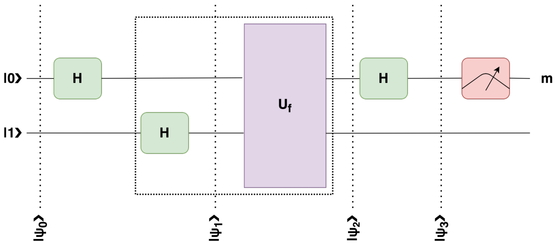


$$|\psi_0\rangle = |0,1\rangle$$

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

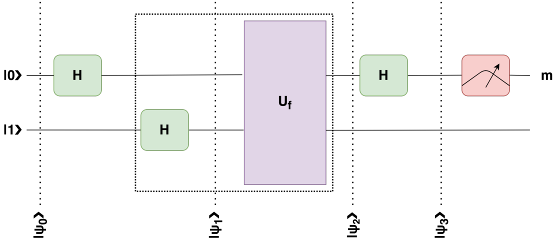
$$|\psi_2\rangle = |+\rangle \otimes \left(\frac{|0 \oplus f(+)\rangle - |1 \oplus f(+)\rangle}{\sqrt{2}}\right)$$

Deutsch's Algorithm (cont.)



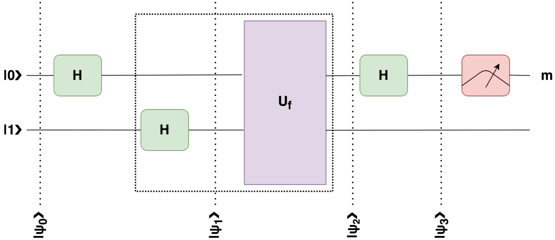
$$|\psi_2\rangle = |+\rangle \otimes \left(\frac{|0 \oplus f(+)\rangle - |1 \oplus f(+)\rangle}{\sqrt{2}} \right)$$

Deutsch's Algorithm (cont.)



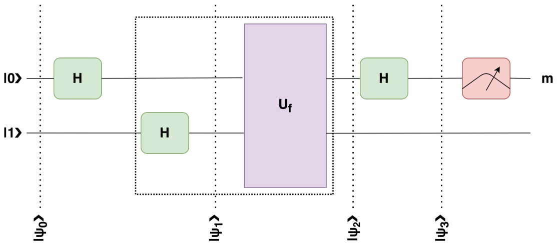
$$|\psi_2\rangle = |+\rangle \otimes \left(\frac{|0 \oplus f(+)\rangle - |1 \oplus f(+)\rangle}{\sqrt{2}} \right) = |+\rangle \otimes \left(\frac{|f(+)\rangle - |\overline{f(+)}\rangle}{\sqrt{2}} \right)$$

Deutsch's Algorithm (cont.)



$$|\psi_2\rangle = |+\rangle \otimes \left(\frac{|0 \oplus f(+)\rangle - |1 \oplus f(+)\rangle}{\sqrt{2}} \right) = |+\rangle \otimes \left(\frac{|f(+)\rangle - |\overline{f(+)}\rangle}{\sqrt{2}} \right) = (-1)^{f(+)} |+\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Deutsch's Algorithm (cont.)



$$|\psi_2\rangle = |+\rangle \otimes \left(\frac{|0 \oplus f(+)\rangle - |1 \oplus f(+)\rangle}{\sqrt{2}}\right) = |+\rangle \otimes \left(\frac{|f(+)\rangle - |\overline{f(+)}\rangle}{\sqrt{2}}\right) =$$
$$(-1)^{f(+)}\,|+\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

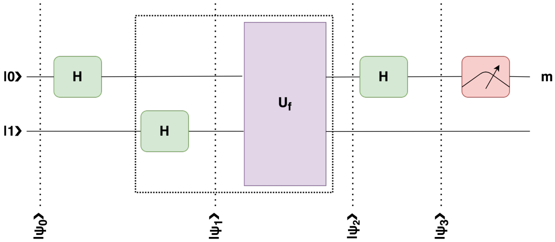
Deutsch's Algorithm (cont.)

$$|\psi_2\rangle = \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

If f was constant then $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle = \pm(|0\rangle + |1\rangle)$

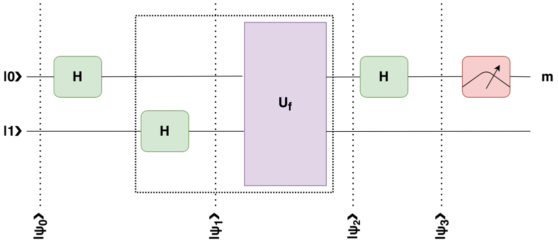
If f was balanced then $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle = \pm(|0\rangle - |1\rangle)$

Deutsch's Algorithm (cont.)



$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f \text{ constant} \\ \pm|1\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f \text{ balanced} \end{cases}$$

Deutsch's Algorithm (cont.)



$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f \text{ constant} \\ \pm|1\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f \text{ balanced} \end{cases}$$

If $m = 0$ after measurement we conclude that f was constant, otherwise we say it was balanced.

Deutsch-Jozsa Algorithm

Consider All functions $f : \{0,1\}^n \rightarrow \{0,1\}$, where a balanced function is one where half inputs go to zero, while constant function all inputs go to either zero or one. This is a Promise problem.

Classically you would need

Deutsch-Jozsa Algorithm

Consider All functions $f : \{0,1\}^n \to \{0,1\}$, where a balanced function is one where half inputs go to zero, while constant function all inputs go to either zero or one. This is a Promise problem.

Classically you would need $\frac{2^n}{2} + 1 = 2^{n-1} + 1$ **calls.**

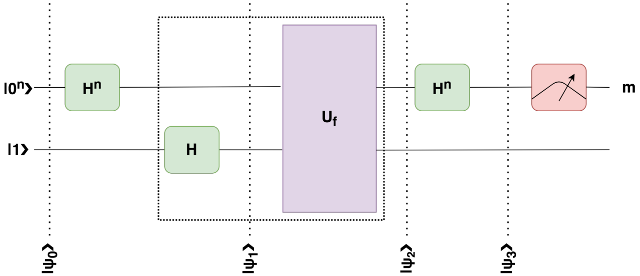
Deutsch-Jozsa Algorithm

Consider All functions $f : \{0,1\}^n \to \{0,1\}$, where a balanced function is one where half inputs go to zero, while constant function all inputs go to either zero or one. This is a Promise problem.

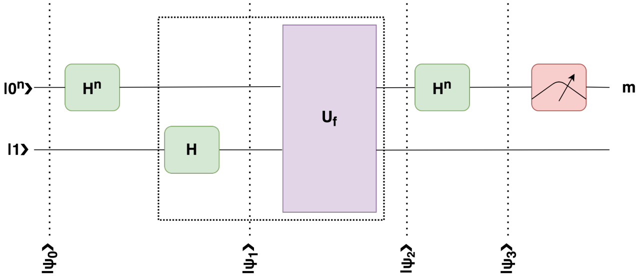
Classically you would need $\frac{2^n}{2} + 1 = 2^{n-1} + 1$ **calls.**

Quantumly you still need only 1 call! That is an exponential speedup.

Deutsch-Jozsa Algorithm



Deutsch-Jozsa Algorithm



Try to follow the same analysis as a homework.

GROVER'S ALGORITHM

Grover's Algorithm

Given an unordered array of m elements, find a particular element.

Grover's Algorithm

Given an unordered array of m elements, find a particular element.

Classically, in the worst case, this takes m queries and on average, we will find the desired element in $\frac{m}{2}$ queries.

Grover's Algorithm

Given an unordered array of m elements, find a particular element.

Classically, in the worst case, this takes m queries and on average, we will find the desired element in $\frac{m}{2}$ queries.
Quantumly, we can find the element in $\sqrt{m}$ queries.

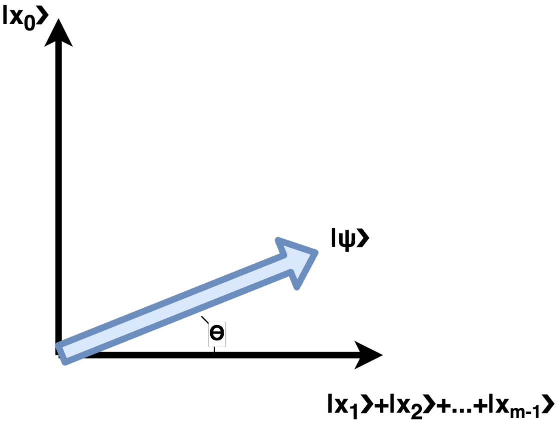
Grover's Algorithm (cont.)

Imagine we find a function $f : \{0,1\}^n \rightarrow \{0,1\}$ with exactly one x_0 representing the index of the desired element s.t.

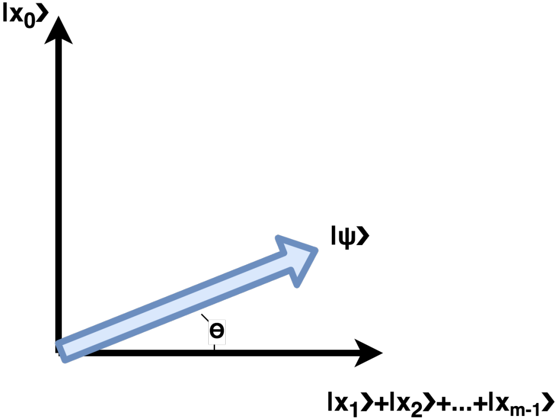
$$f(x) = \begin{cases} 1, & \text{if } x = x_0 \\ 0, & \text{otherwise} \end{cases}$$

Quantum-izing f gives us the unitary $U_f \left|x, y\right\rangle \rightarrow \left|x, f(x) \oplus y\right\rangle$ where $x \in \{0,1\}^n$ and $y \in \{0,1\}$.

Grover's Algorithm (cont.)

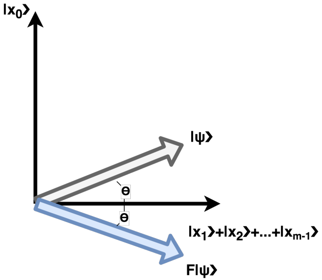


Grover's Algorithm (cont.)

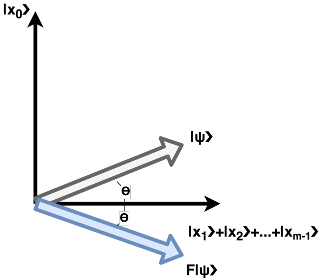


Recall number qubits n equals $\log(m)$, where m is number of elements in array.

Grover's Algorithm (cont.)

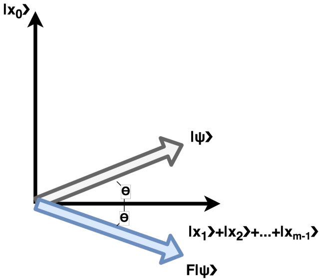


Grover's Algorithm (cont.)



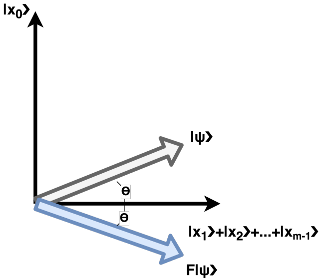
$$U_f(I^{\otimes n} \otimes H)\,|x, 1\rangle$$

Grover's Algorithm (cont.)



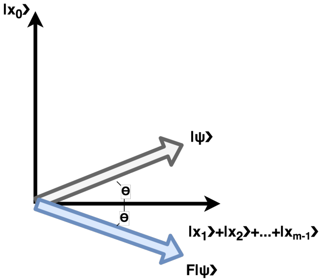
$$U_f(I^{\otimes n} \otimes H)\,|x,1\rangle = U_f\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{2}\right)$$

Grover's Algorithm (cont.)



$$U_f(I^{\otimes n} \otimes H)\left|x,1\right\rangle = U_f\left|x\right\rangle\left(\frac{|0\rangle - |1\rangle}{2}\right) = \left|x\right\rangle\left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{2}\right)$$

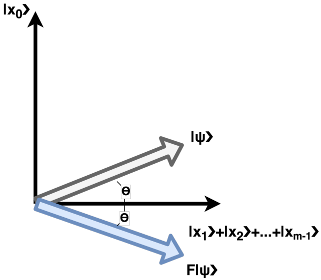
Grover's Algorithm (cont.)



$$U_f(I^{\otimes n} \otimes H)\,|x,1\rangle = U_f\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{2}\right) = |x\rangle \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{2}\right) =$$

$$(-1)^{f(x)}\,|x,-\rangle.$$

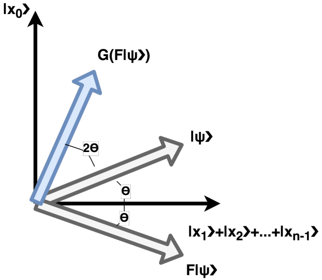
Grover's Algorithm (cont.)



$$U_f(I^{\otimes n} \otimes H)\,|x,1\rangle = U_f\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{2}\right) = |x\rangle\left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{2}\right) = (-1)^{f(x)}\,|x,-\rangle.$$

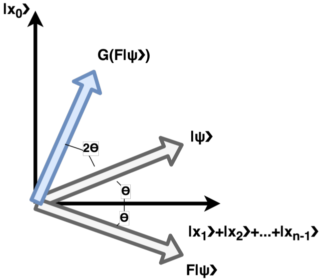
$$\cos(\theta) = \langle\psi|x_1 x_2 .. x_{m-1}\rangle = \sqrt{\frac{m-1}{m}}.$$

Grover's Algorithm (cont.)



$$[(-\mathbf{I}+\mathbf{2A})\otimes I](-1)^{f(x)}\,|x,-\rangle$$

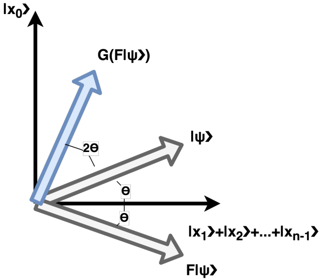
Grover's Algorithm (cont.)



$$[(-\mathbf{I}+\mathbf{2A})\otimes I](-1)^{f(x)}\,|x,-\rangle$$

where A is the average matrix $A_{i,j} = \frac{1}{2^n}$

Grover's Algorithm (cont.)



$$[(-\mathbf{I}+\mathbf{2A})\otimes I](-1)^{f(x)}\,|x,-\rangle$$

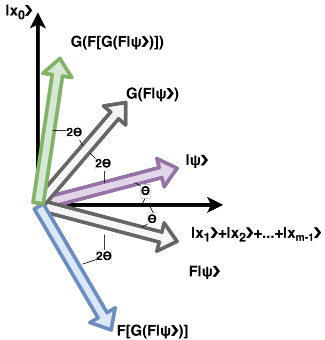
where A is the average matrix $A_{i,j}=\frac{1}{2^n}$ $A=|\psi\rangle\langle\psi|$.

Grover's Algorithm (cont.)

$G = (-I + 2\,|\psi\rangle\langle\psi|)$ means:

Grover's Algorithm (cont.)

$G = (-I + 2|\psi\rangle\langle\psi|)$ means:



Grover's Algorithm (cont.)

Why $-I+2A=A+(A-I)$?

If you have numbers 4, 9, 17.

Grover's Algorithm (cont.)

Why $-I + 2A = A + (A - I)$?

If you have numbers 4, 9, 17. Their average is 10.

Grover's Algorithm (cont.)

Why $-I + 2A = A + (A - I)$?

If you have numbers 4, 9, 17. Their average is 10.
If we take element 4 which was six points below average, we get

Grover's Algorithm (cont.)

Why $-I + 2A = A + (A - I)$?

If you have numbers 4, 9, 17. Their average is 10.
If we take element 4 which was six points below average, we get 10 + (10-4) = 16

Grover's Algorithm (cont.)

Why $-I + 2A = A + (A - I)$?

If you have numbers 4, 9, 17. Their average is 10.
If we take element 4 which was six points below average, we get 10 + (10-4) = 16 , which is six points above average.

Grover's Algorithm Summary

$$\left[\left(H^{\otimes n} (2 \left| 0^n \right\rangle \left\langle 0^n \right| - I^{\otimes n}) H^{\otimes n} \otimes I \right) U_f (I^{\otimes n} \otimes H)) \right]^{\sqrt{n}} (H^{\otimes n} \otimes I) \left| 0^{\otimes n}, 1 \right\rangle$$

$$\left[\left((2 \left| \psi \right\rangle \left\langle \psi \right| - I^{\otimes n}) \otimes I \right) U_f (I^{\otimes n} \otimes H)) \right]^{\sqrt{n}} (H^{\otimes n} \otimes I) \left| 0^{\otimes n}, 1 \right\rangle$$

Grover's Algorithm Summary

$$\left[\left(H^{\otimes n}(2\left|0^n\right\rangle\left\langle 0^n\right| - I^{\otimes n})H^{\otimes n} \otimes I\right) U_f (I^{\otimes n} \otimes H)\right)\right]^{\sqrt{n}} (H^{\otimes n} \otimes I)\left|0^{\otimes n}, 1\right\rangle$$

$$\left[\left((2\left|\psi\right\rangle\left\langle\psi\right| - I^{\otimes n}) \otimes I\right) U_f (I^{\otimes n} \otimes H)\right)\right]^{\sqrt{n}} (H^{\otimes n} \otimes I)\left|0^{\otimes n}, 1\right\rangle$$

$\cos(\theta) = \sqrt{(m-1)/m}$, so $\sin(\theta) \approx \theta = \sqrt{1/m}$,

Grover's Algorithm Summary

$$\left[\left(H^{\otimes n}(2\left|0^n\right\rangle\left\langle 0^n\right| - I^{\otimes n})H^{\otimes n} \otimes I\right)U_f(I^{\otimes n} \otimes H))\right]^{\sqrt{n}} (H^{\otimes n} \otimes I)\left|0^{\otimes n}, 1\right\rangle$$

$$\left[\left((2\left|\psi\right\rangle\left\langle\psi\right| - I^{\otimes n}) \otimes I\right)U_f(I^{\otimes n} \otimes H))\right]^{\sqrt{n}} (H^{\otimes n} \otimes I)\left|0^{\otimes n}, 1\right\rangle$$

$\cos(\theta) = \sqrt{(m-1)/m}$, so $\sin(\theta) \approx \theta = \sqrt{1/m}$, then time complexity is $\frac{\pi}{2} \cdot \frac{1}{2\theta} = \frac{\pi}{2 \cdot 2}\sqrt{m} = O(\sqrt{m})$

SIMON'S ALGORITHM

Simon's Algorithm

Suppose we are given $f : \{0,1\}^n \to \{0,1\}^n$ and promised that $\exists$ a period $c \in \{0,1\}^n$ s.t. $\forall x, y \in \{0,1\}^n, f(x) = f(y)$ iff $x = y \oplus c$.

Simon's Algorithm

Suppose we are given $f : \{0,1\}^n \rightarrow \{0,1\}^n$ and promised that $\exists$ a period $c \in \{0,1\}^n$ s.t. $\forall x, y \in \{0,1\}^n, f(x) = f(y)$ iff $x = y \oplus c$.

Find c.

Simon's Algorithm (cont.)

Observe: if $c = 0^n$ then f is one-to-one. Otherwise, f is two-to-one, namely $f(x_1) = y = f(x_2)$ when $x_1 = x_2 \oplus c$

Simon's Algorithm (cont.)

Observe: if $c = 0^n$ then f is one-to-one. Otherwise, f is two-to-one, namely $f(x_1) = y = f(x_2)$ when $x_1 = x_2 \oplus c$

Classically we need

Simon's Algorithm (cont.)

Observe: if $c = 0^n$ then f is one-to-one. Otherwise, f is two-to-one, namely $f(x_1) = y = f(x_2)$ when $x_1 = x_2 \oplus c$

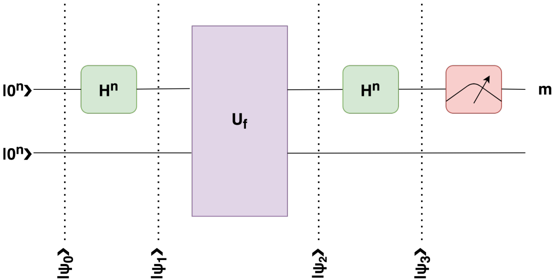
Classically we need $\frac{2^n}{2} + 1$ evaluations to find the period c.

Simon's Algorithm (cont.)

Observe: if $c = 0^n$ then f is one-to-one. Otherwise, f is two-to-one, namely $f(x_1) = y = f(x_2)$ when $x_1 = x_2 \oplus c$

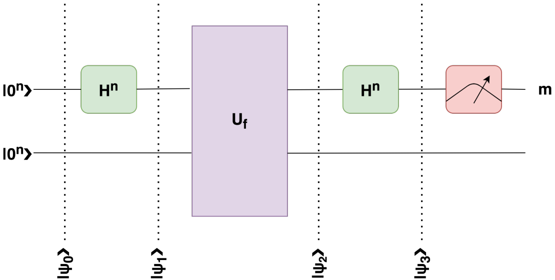
Classically we need $\frac{2^n}{2} + 1$ evaluations to find the period c. Quantum-ly?

Simon's Algorithm (cont.)



$$|\psi_0\rangle = |0^n, 0^n\rangle$$

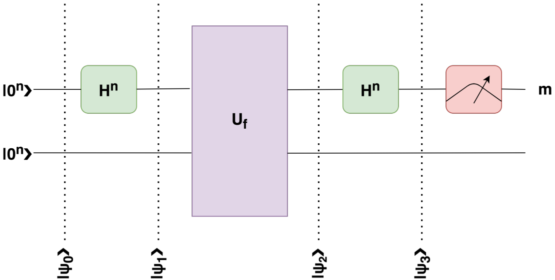
Simon's Algorithm (cont.)



$$|\psi_0\rangle = |0^n, 0^n\rangle \qquad |\psi_1\rangle = \frac{\sum_{x\in\{0,1\}^n} |x, 0^n\rangle}{\sqrt{2^n}}$$

$$|\psi_2\rangle = \frac{\sum_{x\in\{0,1\}^n} |x, f(x)\rangle}{\sqrt{2^n}}$$

Simon's Algorithm (cont.)



$$|\psi_0\rangle = |0^n, 0^n\rangle \qquad |\psi_1\rangle = \frac{\sum_{x\in\{0,1\}^n} |x, 0^n\rangle}{\sqrt{2^n}}$$

$$|\psi_2\rangle = \frac{\sum_{x\in\{0,1\}^n} |x, f(x)\rangle}{\sqrt{2^n}} \qquad |\psi_3\rangle = \frac{\sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{\langle z,x\rangle} |z, f(x)\rangle}{\sqrt{2^n}}$$

Simon's Algorithm (cont.)

$$|\psi_3\rangle = \sum_{x\in\{0,1\}^n} \left[\frac{\sum_{z\in\{0,1\}^n} (-1)^{\langle z,x\rangle} |z, f(x)\rangle}{\sqrt{2^n}} \right]$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & 1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ 1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & -1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{pmatrix}$$

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

Simon's Algorithm (cont.)

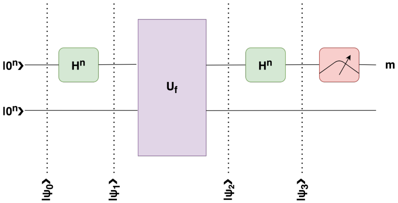
Notice that we are promised that $|z, f(x)\rangle = |z, f(x \oplus c)\rangle$. Then in $|\psi_3\rangle = \frac{\sum_{z\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{\langle z,x\rangle}|z,f(x)\rangle}{\sqrt{2^n}}$, the coefficient of $|z, f(x)\rangle$ is

$$\frac{(-1)^{\langle z,x\rangle} + (-1)^{\langle z,x\oplus c\rangle}}{2} = \frac{(-1)^{\langle z,x\rangle} + (-1)^{\langle z,x\rangle\oplus\langle z,c\rangle}}{2}$$

$$\frac{(-1)^{\langle z,x\rangle} + (-1)^{\langle z,x\rangle}(-1)^{\langle z,c\rangle}}{2} = (-1)^{\langle z,x\rangle}\frac{(1 + (-1)^{\langle z,c\rangle})}{2}$$

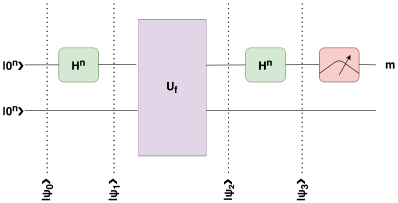
if $\langle z, c\rangle = 1$ then the coefficient is 0 (destructive interference).
If $\langle z, c\rangle = 0$ it will be ± 1. (recall inner product is mod 2)

Simon's Algorithm (cont.)



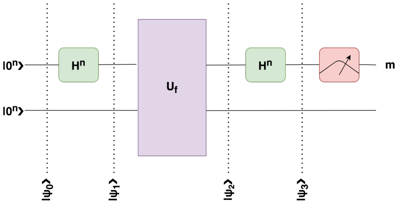
Measuring at the end will collapse our n-qubits into one of the states with $\langle z, c \rangle = 0$.

Simon's Algorithm (cont.)



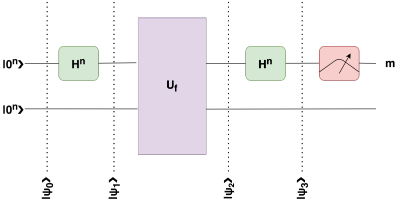
Measuring at the end will collapse our n-qubits into one of the states with $\langle z, c\rangle = 0$. So $m = z$.

Simon's Algorithm (cont.)



Measuring at the end will collapse our n-qubits into one of the states with $\langle z, c\rangle = 0$. So $m = z$. Thus $\langle m, c\rangle = 0$ is a linear equation.

Simon's Algorithm (cont.)



Measuring at the end will collapse our n-qubits into one of the states with $\langle z, c \rangle = 0$. So $m = z$. Thus $\langle m, c \rangle = 0$ is a linear equation. Since c has n-bits, we run Simon's $O(n)$ times, get $O(n)$ equations in n unknowns, and solve them classically.

SHOR'S ALGORITHM

Shor's Algorithm

Given an n-bit number N (2^n possible such numbers).

Shor's Algorithm

Given an n-bit number N (2^n possible such numbers). We can check if N is prime in polynomial time in n classically.

Shor's Algorithm

Given an n-bit number N (2^n possible such numbers). We can check if N is prime in polynomial time in n classically. If N is composite ($N = x \cdot y$), then finding x and y classically requires exponential time in n.

Shor's Algorithm

Given an n-bit number N (2^n possible such numbers). We can check if N is prime in polynomial time in n classically. If N is composite ($N = x \cdot y$), then finding x and y classically requires exponential time in n. Quantum-ly it is also polynomial time in n.

Recall GCD

The Greatest Common Divisor can be efficiently computed using Euclid's Algorithm.

Recall GCD

The Greatest Common Divisor can be efficiently computed using Euclid's Algorithm. Moreover, it can be used to find reduced fractions.

Recall GCD

The Greatest Common Divisor can be efficiently computed using Euclid's Algorithm. Moreover, it can be used to find reduced fractions.

e.g.: $\gcd(42, 56) = 14$, then $\frac{42}{56} = \frac{3 \cdot 14}{4 \cdot 14} = \frac{3}{4}$.

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\ p$ s.t

$$g^p = (m \cdot N) + 1$$

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\ p$ s.t

$$g^p = (m \cdot N) + 1$$

p is the order of the element g. And every coprime to N has a finite order.

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\ p$ s.t

$$g^p = (m \cdot N) + 1$$

p is the order of the element g. And every coprime to N has a finite order. Finding p is as hard as factoring.

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\, p$ s.t

$$g^p = (m \cdot N) + 1$$

p is the order of the element g. And every coprime to N has a finite order. Finding p is as hard as factoring.

e.g. g=7, N=15,

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\, p$ s.t

$$g^p = (m \cdot N) + 1$$

p is the order of the element g. And every coprime to N has a finite order. Finding p is as hard as factoring.

e.g. g=7, N=15, $g^2 = 3 \cdot N + 4$,

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\ p$ s.t

$$g^p = (m \cdot N) + 1$$

p is the order of the element g. And every coprime to N has a finite order. Finding p is as hard as factoring.

e.g. g=7, N=15, $g^2 = 3 \cdot N + 4$, $g^3 = 22 \cdot N + 13$,

More Number Theory

For any element $1 < g < N$, with $\gcd(g, N) = 1$, $\exists\, p$ s.t

$$g^p = (m \cdot N) + 1$$

p is the order of the element g. And every coprime to N has a finite order. Finding p is as hard as factoring.

e.g. g=7, N=15, $g^2 = 3 \cdot N + 4$, $g^3 = 22 \cdot N + 13$, but $g^4 = 160 \cdot N + 1$.

Using Order Finding to Factor

However, assume you found p.

Using Order Finding to Factor

However, assume you found p. Then we can rearrange $g^p = (m \cdot N) + 1$ to:

Using Order Finding to Factor

However, assume you found p. Then we can rearrange $g^p = (m \cdot N) + 1$ to:

$$
\begin{aligned}
g^p - 1 &= m \cdot N \\
(g^{p/2} - 1)(g^{p/2} + 1) &= m \cdot N
\end{aligned}
$$

If $p/2$ is not a fraction

Using Order Finding to Factor

However, assume you found p. Then we can rearrange $g^p = (m \cdot N) + 1$ to:

$$g^p - 1 = m \cdot N$$
$$(g^{p/2} - 1)(g^{p/2} + 1) = m \cdot N$$

If $p/2$ is not a fraction , and neither $(g^{p/2} - 1)$ nor $(g^{p/2} + 1)$ equals N,

Using Order Finding to Factor

However, assume you found p. Then we can rearrange $g^p = (m \cdot N) + 1$ to:

$$g^p - 1 = m \cdot N$$
$$(g^{p/2} - 1)(g^{p/2} + 1) = m \cdot N$$

If $p/2$ is not a fraction , and neither $(g^{p/2} - 1)$ nor $(g^{p/2} + 1)$ equals N, then you found a factor of N which is either $(g^{p/2} - 1)$ or $(g^{p/2} + 1)$ or both (happens w/ 37.5%).

Using Order Finding to Factor

However, assume you found p. Then we can rearrange $g^p = (m \cdot N) + 1$ to:

$$g^p - 1 = m \cdot N$$
$$(g^{p/2} - 1)(g^{p/2} + 1) = m \cdot N$$

If $p/2$ is not a fraction , and neither $(g^{p/2} - 1)$ nor $(g^{p/2} + 1)$ equals N, then you found a factor of N which is either $(g^{p/2} - 1)$ or $(g^{p/2} + 1)$ or both (happens w/ 37.5%). (you can remove extra multiples of the factors using GCD.)

Sketch of Shor's Algorithm Idea

Pick random g satisfying $\gcd(g, N) = 1$

Sketch of Shor's Algorithm Idea

Pick random g satisfying $\gcd(g, N) = 1$
$\rightarrow$ create $U_g \left|x, 0\right\rangle = \left|x, g^x\right\rangle$

Sketch of Shor's Algorithm Idea

Pick random g satisfying $\gcd(g, N) = 1$
$\rightarrow$ create $U_g |x, 0\rangle = |x, g^x\rangle$
$\rightarrow$ create $U_N |x, g^x\rangle = |x, (g^x \mod N)\rangle$

Sketch of Shor's Algorithm Idea

Pick random g satisfying $\gcd(g, N) = 1$
$\rightarrow$ create $U_g \left|x, 0\right\rangle = \left|x, g^x\right\rangle$
$\rightarrow$ create $U_N \left|x, g^x\right\rangle = \left|x, (g^x \mod N)\right\rangle = \left|x, r\right\rangle$

Sketch of Shor's Algorithm Idea

Pick random g satisfying $\gcd(g, N) = 1$
$\rightarrow$ create $U_g |x, 0\rangle = |x, g^x\rangle$
$\rightarrow$ create $U_N |x, g^x\rangle = |x, (g^x \mod N)\rangle = |x, r\rangle$
$\rightarrow$ Feed $|x, 0\rangle = \sum_{q=0}^{N-1} |q, 0\rangle$ resulting in $\sum_{q=0}^{N-1} |q, r_q\rangle$

Easy Property of $g^p \equiv 1 \mod N$

$$g^{p'} = m \cdot N + r \implies g^{p'+p} = m' \cdot N + r$$

Easy Property of $g^p \equiv 1 \mod N$

$$g^{p'} = m \cdot N + r \implies g^{p'+p} = m' \cdot N + r$$

Notice $g^{p'+p} = g^{p'} \cdot g^p$.

Easy Property of $g^p \equiv 1 \mod N$

$$g^{p'} = m \cdot N + r \implies g^{p'+p} = m' \cdot N + r$$

Notice $g^{p'+p} = g^{p'} \cdot g^p$. Multiplying $g^{p'}$ by g^p, multiplies RHS by $1 \mod N$ because $g^p \equiv 1 \mod N$.

Sketch of Shor's Algorithm Idea

Pick random g
$\rightarrow$ create $U_g \left|x, 0\right\rangle = \left|x, g^x\right\rangle$
$\rightarrow$ create $U_N \left|x, g^x\right\rangle = \left|x, (g^x \mod N)\right\rangle = \left|x, r\right\rangle$
$\rightarrow$ Feed $\left|x, 0\right\rangle = \sum_{q=0}^{N-1} \left|q, 0\right\rangle$ resulting in $\sum_{q=0}^{N-1} \left|q, r_q\right\rangle$
$\rightarrow$ measure $\left|r\right\rangle$ reading say r_0, which gives a superposition of the first register $\sum_{q'} \left|q'\right\rangle$ with q' being all powers that share the same remainder.

Sketch of Shor's Algorithm Idea

$\rightarrow$ measure $|r\rangle$ reading say r_0, which gives a superposition of the first register $\sum_{q'} |q'\rangle$ with q' being all powers that share the same remainder.

Sketch of Shor's Algorithm Idea

$\rightarrow$ measure $|r\rangle$ reading say r_0, which gives a superposition of the first register $\sum_{q'} |q'\rangle$ with q' being all powers that share the same remainder.
We know from

$$g^{p'} = m \cdot N + r \implies g^{p'+p} = m' \cdot N + r$$

that all the q''s resulting from measuring this r_0 must be $q_0, q_0 + p, q_0 + 2p, q_0 + 3p, \ldots$ for some initial q_0.

Sketch of Shor's Algorithm Idea

$\rightarrow$ measure $|r\rangle$ reading say r_0, which gives a superposition of the first register $\sum_{q'} |q'\rangle$ with q' being all powers that share the same remainder.
We know from

$$g^{p'} = m \cdot N + r \implies g^{p'+p} = m' \cdot N + r$$

that all the q''s resulting from measuring this r_0 must be $q_0, q_0 + p, q_0 + 2p, q_0 + 3p, \ldots$ for some initial q_0. How do we find this frequency?

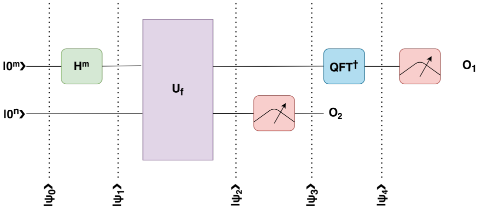
Sketch of Shor's Algorithm Idea

$\rightarrow$ measure $|r\rangle$ reading say r_0, which gives a superposition of the first register $\sum_{q'} |q'\rangle$ with q' being all powers that share the same remainder.
We know from

$$g^{p'} = m \cdot N + r \implies g^{p'+p} = m' \cdot N + r$$

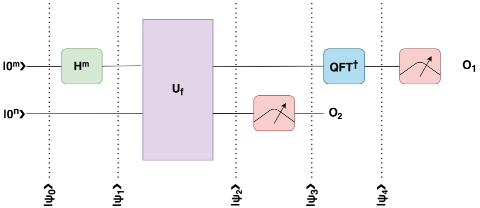
that all the q''s resulting from measuring this r_0 must be $q_0, q_0 + p, q_0 + 2p, q_0 + 3p, \ldots$ for some initial q_0. How do we find this frequency? QFT.

Shor's Algorithm (cont.)



$$|\psi_0\rangle = |0^m, 0^n\rangle$$

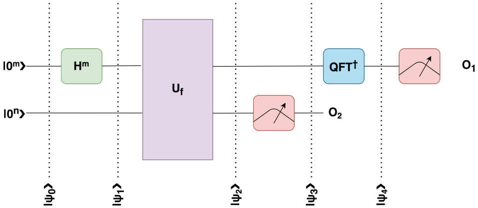
Shor's Algorithm (cont.)



$$|\psi_0\rangle = |0^m, 0^n\rangle \qquad |\psi_1\rangle = \frac{\sum_{q\in\{0,1\}^m} |q, 0^n\rangle}{\sqrt{2^m}}$$

$$|\psi_2\rangle = \frac{\sum_{q\in\{0,1\}^m} |q, g^q \bmod N\rangle}{\sqrt{2^m}}$$

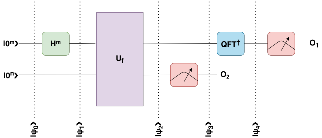
Shor's Algorithm (cont.)



Assuming $O_2 = g^v \bmod N$. $|\psi_3\rangle = \dfrac{\sum_{g^{q'} \equiv g^v \bmod N} |q', O_2\rangle}{\sqrt{2^m/r}}$

$= \dfrac{\sum_{j=0}^{(2^m/r)-1} |q_0 + j \cdot p, O_2\rangle}{\sqrt{2^m/r}}$ with $q_0 = \mathsf{min}_t \left[g^t \equiv a^v \bmod N \right]$

Shor's Algorithm (cont.)



The QFT† removes the offset q_0, and changes the period from $r \to 2^m/r$. Now measuring gives $O_1 = c \cdot 2^m/r$ for some c. Dividing by 2^m which we know, we get c/r which can be reduced to an irreducible fraction enabling us to extract r.

Full Shor's Algorithm

(1) Randomly pick $1 < g < N$. Compute $\text{GCD}(g, N)$. If $\text{GCD}(g, N) \neq 1$ then g is a factor return it.
(2) Find period of function $f_{a,N}(x)$ using previous circuit.
(3) If p is odd or $p^r \equiv -1 \bmod N$ then start over.
(4) Compute $\text{GCD}(g^{p/2} + 1, N)$ and $\text{GCD}(g^{p/2} - 1, N)$. At least one of these two GCDs is a factor if not both.

Introspection

Since this was basically a period finding problem, why didn't we use Simon's algorithm?

Introspection

Since this was basically a period finding problem, why didn't we use Simon's algorithm? Notice also that Shor's circuit is similar to Simon's except for the QFT instead of the second Hadamard.

Introspection

Since this was basically a period finding problem, why didn't we use Simon's algorithm? Notice also that Shor's circuit is similar to Simon's except for the QFT instead of the second Hadamard. The reason is that Simon's period finding problem was for two-to-one periodic functions.

Introspection

Since this was basically a period finding problem, why didn't we use Simon's algorithm? Notice also that Shor's circuit is similar to Simon's except for the QFT instead of the second Hadamard. The reason is that Simon's period finding problem was for two-to-one periodic functions. Here it was finding a period of a general periodic function, so we had to use the Fourier Transform (QFT for polytime(n)).

Introspection

Since this was basically a period finding problem, why didn't we use Simon's algorithm? Notice also that Shor's circuit is similar to Simon's except for the QFT instead of the second Hadamard. The reason is that Simon's period finding problem was for two-to-one periodic functions. Here it was finding a period of a general periodic function, so we had to use the Fourier Transform (QFT for polytime(n)). We deduce that Hadamard is a kind of Fourier transform of size-2.

That's All Folks!