Week 1: **The history of Q:** Overview of this course and review of linear algebra, basics of quantum mechanics, quantum bits and mixed states

Early History of Q: important milestones

EPR (Eistein-Podolsky-Rosen) 1935: “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?”

Bell 1964: Inequality to compare classical theory and quantum mechanics

Clauser-Horne-Shimony-Holt (CHSH) 1969: Another Inequality

Aspect, Granger and Roger 1982: Experimental violation of CHSH inequality

Bennett and Brassard 1984: Quantum Key Distribution using non-orthogonal states

Benioff 1990: Turing Machine using Quantum Mechanics

Manin 1990: Idea of Quantum Computation

Ekert 1991: QKD using singlet pairs

Feynmann 1992 & 1995: Quantum Computation and Quantum Simulations

Bennett et al. 1993: Quantum teleportation

Shor 1994: Quantum Factoring algorithm

Grover 1996: Quantum Search algorithm

Google 2019: Quantum Supremacy Demonstration

One quantum bit (qubit)

Quantum bit is a two-level system, which can be described by a complex vector (it lives in a Hilbert space (denoted by C^2), but let's not worry about the rigorous mathematical definition), labeled by a symbol ψ, usually we write it as

$|\vec{v}|^2 = 1$

quantum state

classical 0 or 1

a wave fcn $|\psi\rangle = \vec{v} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

For convenience and as a convention, we will normalize the complex vector to have unit norm (total probability over distribution $|\alpha|^2$ and $|\beta|^2$ is one):

$\boxed{|\alpha|^2 + |\beta|^2 = 1}$

$$\boxed{\langle\psi|}\cdot\boxed{|\psi\rangle} = \langle\psi|\psi\rangle = \vec{v}^* \cdot \vec{v} = \boxed{\begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}} \cdot \boxed{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}} = |\alpha|^2 + |\beta|^2 = 1$$

Since it is a two-component vector, it has two basis vectors, corresponding to (by our choice):

$$|\uparrow\rangle = |0\rangle = \boxed{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} \quad |\downarrow\rangle = \boxed{|1\rangle} = \boxed{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} \quad \text{so} \quad |\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle = \alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum gates or operators act on quantum states (their dimensions should match), so they behave like a matrix, e.g. the NOT or X gate:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{which flips up to down} \quad X|\uparrow\rangle = X\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\downarrow\rangle$$

Getting used to bra-ket notations

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

We use a ‘**ket**’ notation for ψ, whose ‘dual row vector’ is denoted by a ‘**bra**’ notation $\langle\psi| = (|\psi\rangle)^\dagger = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$

The inner product results in a number:

$$\langle\psi|\cdot|\psi\rangle = \langle\psi|\psi\rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 + |\beta|^2$$

→ off diags ⇒ $\boxed{\text{coherence}}$ fringes

The outer product results in a matrix (also called ‘density matrix’), also an operator:

$$\rho_\psi \equiv |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}\begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} = \boxed{\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}}$$

diagonal elements represent probability distribution

The trace of this density matrix is actually the norm square

$$\mathrm{Tr}(\rho_\psi) \equiv \mathrm{Tr}(|\psi\rangle\langle\psi|) = \mathrm{Tr}\left[\begin{pmatrix} \alpha \\ \beta \end{pmatrix}\begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}\right] \overset{\text{multiply}}{=} \mathrm{Tr}\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \overset{\text{sum of diagonal}}{=} |\alpha|^2+|\beta|^2 = 1$$

Interestingly, using the ‘cyclic’ property of the trace, we have (i.e. trace of outer product = inner product):

Tr(AB) = Tr(BA) cyclic property

$$\mathrm{Tr}(|\psi\rangle\langle\psi|) = \mathrm{Tr}(\langle\psi|\cdot|\psi\rangle) = \langle\psi|\psi\rangle = 1 = \underbrace{|\alpha|^2}_{\text{prob@0}} + \underbrace{|\beta|^2}_{\text{prob@1}}$$

Bloch sphere picture of a qubit

Given the normalization $|\alpha|^2 + |\beta|^2 = 1$ we can choose to parametrize α & β

$e^{i\chi}$ $\qquad\qquad$ $e^{i\chi}$

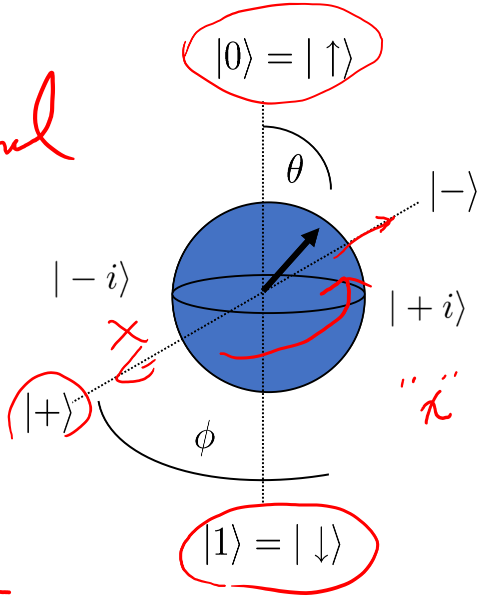
$$\alpha = \cos(\theta/2), \ \beta = e^{i\phi}\sin(\theta/2)$$

α & β are complex in general

Evaluate the density matrix

$$\rho_\psi \equiv |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

$$= \begin{pmatrix} \cos^2(\theta/2) = (1+\cos\theta)/2 & \sin(\theta/2)\cos(\theta/2)e^{-i\phi} = \sin\theta e^{-i\phi}/2 \\ \sin(\theta/2)\cos(\theta/2)e^{i\phi} & \sin^2(\theta/2) = (1-\cos\theta)/2 \end{pmatrix}$$



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

"x": $\theta = \frac{\pi}{2}$, $\phi = 0$, $\alpha = \frac{1}{\sqrt{2}}$, $\beta = \frac{1}{\sqrt{2}}$

"$-x$": $\phi = \pi$, $\beta = -\frac{1}{\sqrt{2}}$

If we define $\quad r_x = \sin\theta\cos\phi, \ r_y = \sin\theta\sin\phi, \ r_z = \cos\theta$

Then

$$\begin{array}{cccc} & I & X & Y & Z \end{array}$$

$$\rho_\psi = \frac{1}{2}\begin{pmatrix} 1 + r_z & r_x - ir_y \\ r_x + ir_y & 1 - r_z \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{r_x}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{r_y}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + \frac{r_z}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$= (I + \vec{r}\cdot\vec{\sigma})/2, \quad \vec{\sigma} \equiv (X, Y, Z)$$

$\vec{r}\cdot\vec{\sigma} = r_x \sigma_x + r_y \sigma_y + r_z \sigma_z$

$\qquad\qquad\qquad\ X \qquad\ \ Y \qquad\ \ Z$

[Pauli matrices]

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$|\vec{r}| = 1 : \ \text{pure states}$

Properties of Pauli matrices

$$\rho_\psi = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}), \quad \vec{\sigma} \equiv (X, Y, Z) \qquad X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Square to identity, anticommute & cyclic in commutator

$$X^2 = Y^2 = Z^2 = I$$

$$\{X, Y\} \equiv XY + YX = 0 = \{Y, Z\} = \{Z, X\}$$

$$[X, Y] \equiv XY - YX = iZ, \; [Y, Z] = iX, \; [Z, X] = iY$$

commutator

$S = \frac{\sigma}{2}$

$XY = -YX$

$[S_x, S_y] = i\epsilon_{xyz} S_z$

$X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

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

- They are related to spin angular momentum operators, i.e. they generate rotation of the qubit around respective axes

$$R_x(\varphi) \equiv e^{-i\varphi\frac{X}{2}} \qquad R_y(\varphi) \equiv e^{-i\varphi\frac{Y}{2}} \qquad R_z(\varphi) \equiv e^{-i\varphi\frac{Z}{2}}$$

$$R_{\hat{n}}(\varphi) \equiv e^{-i\frac{\varphi}{2}\hat{n}\cdot\vec{\sigma}} = \cos(\varphi/2)I - i\sin(\varphi/2)\hat{n}\cdot\vec{\sigma}$$ w.r.t. direction n

"Euler formula" $e^{i\theta} = \cos\theta + i\sin\theta$

(physical meaning: rotation)

- X, Y, Z are themselves rotation by 180 degrees (e.g. X flips up to down); Note they are Hermitian $X^\dagger = X$ and traceless $Tr(X)=Tr(Y)=Tr(Z)=0$.

$R_z(\pi) = e^{-i\pi\frac{Z}{2}} = 0 - i\sin\frac{\pi}{2} Z = -iZ$

Pure states vs. mixed states

$$\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}), \quad \vec{\sigma} \equiv (X, Y, Z)$$

- We used the density matrix of a general pure state (a projector) $\rho_\psi \equiv |\psi\rangle\langle\psi|$ and thus there is a constraint that $|\vec{r}| = \sqrt{r_x^2 + r_y^2 + r_z^2} = 1$

$$\rho_\psi^2 = |\psi\rangle\underbrace{\langle\psi|\cdot|\psi\rangle}_{0}\langle\psi| = \overbrace{|\psi\rangle\langle\psi|}^{=\rho_\psi} \to \mathrm{Tr}(\rho_\psi^2) = 1$$ sometimes referred to as purity $\Rightarrow$ Purity = 1

Pure state

Pure state

$\rho \to \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ Some basis

mixed state

$\rho \to \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix}$

- For general ~~ρ~~ A, can directly calculate (exercise)

$(\vec{r}\cdot\vec{\sigma})^2 = |\vec{r}|^2 \mathbb{1}$

$$\rho^2 = \frac{1}{4}(I + \vec{r}\cdot\vec{\sigma})^2 = \frac{1}{4}(I + 2\vec{r}\cdot\vec{\sigma} + |\vec{r}|^2 I) \Rightarrow \mathrm{Tr}(\rho^2) = (1 + |\vec{r}|^2)/2 \leq 1$$

$\mathrm{Tr}(\rho^2) < 1$ for mixed states

If |r|<1, then ρ does **not** represent the density matrix of a pure state, it is a **mixed state**! In other words, eigenvalues of ρ are both nonzero & less than one (rank-two in contrast to rank-one for the pure state)

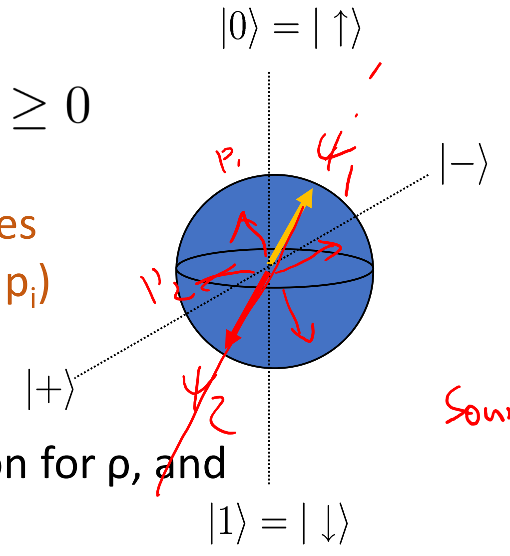
How do we get mixed states?

by mixing pure state

- One can simply diagonalize ρ and obtain two eigenvalues p_1 & p_2 and eigenvectors (eigenstates) ψ_1 & ψ_2 then

$$\rho = p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2|, \text{ with } p_1 + p_2 = 1, p_i \geq 0$$

Mixed states can come from statistical mixture of pure states (imagine a source randomly emit states ψ_i with probability p_i)



Source $\begin{cases} p_1 \rightsquigarrow \psi_1 \\ p_2 \rightsquigarrow \psi_2 \end{cases}$

- In the above example, we have the '**spectral**' decomposition for ρ, and ψ_1 & ψ_2 are orthonormal eigenstates

$$\langle\psi_i|\psi_j\rangle = \delta_{ij}$$

In general, there **infinite** ways of decomposing a mixed state (with more than two components), thus we have a statistical ensemble:

$$\rho = \sum_{i=1}^{n} q_j\rho_j, \quad \text{with } \sum_j q_j = 1, \quad \rho_j \geq 0 \,\&\, \mathrm{Tr}(\rho_j) = 1$$

Basic quantum mechanical rules

- (I) Quantum states can have superposition

We have seen that a qubit can be a 'superposition' of up and down, with respective weights or more precisely, amplitudes

$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$ e.g. a Q coin: α 

$+\ \beta$ 

But how do you put it in such a superposition (e.g. if we begin with up)? **Ans**. By using quantum gates (e.g. the **Hadamard gate** *H*)

$$H|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} ; \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

But how are quantum gates implemented? One key approach is to let quantum states evolve (under the so-called Hamiltonian), and the evolution gives rise to the action of a quantum gate

Basic quantum mechanical rules

- (II) Evolution is Linear and Unitary

→ Hamiltonian

The 'driver' of the evolution is the Hamiltonian (unfortunately has same symbol H as the Hadamard). How it drives the evolution is:

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle$$

(Schrödinger's equation and h-bar is the reduced Planck constant)

verify

$\frac{d}{dt}\left(e^{-\frac{i}{\hbar}Ht} |\psi(0)\rangle \right) = -\frac{i}{\hbar} H \underbrace{e^{-\frac{i}{\hbar}Ht}|\psi(0)\rangle}_{|\psi(t)\rangle}$

Don't worry, we won't dwell on how to solve it (this is what do we in PHY251 or PHY308). But there is a formal solution:

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar}\hat{H}t}|\psi(0)\rangle$$

➔ We have a gate! $U_H(t) \equiv e^{-\frac{i}{\hbar}\hat{H}t}$

Hadamard

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

- Unitarity: $U_H U_H^\dagger = U_H^\dagger U_H = 1$
- Linearity: $U_H(a|\psi\rangle + b|\phi\rangle) = a\left(U_H|\psi\rangle\right) + b\left(U_H|\phi\rangle\right)$

Basic quantum mechanical rules

- (III) Strong **measurement** projects wavefunction; outcome is often probabilistic

This is one mystical part of quantum mechanics, but is easy to illustrate with a quantum coin. Suppose we measure in the 'classical' or 'computational' basis to reveal ***up*** or ***down*** on a Q coin:

$$\begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}$$

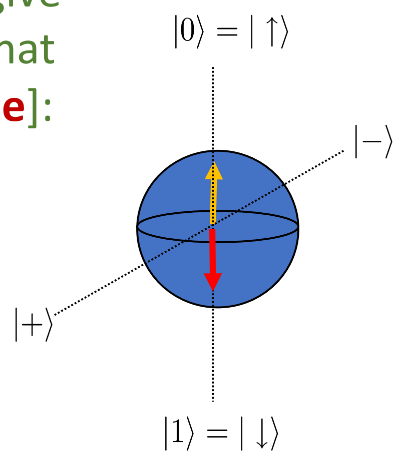
α  $+\ \beta$ 

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

➔ You obtain an outcome **randomly**. Sometimes it's up (we will give a score of +1) and sometimes it's down (we give a score of -1). What we know is that it occurs according to some distribution [**Born rule**]:

$$P_\uparrow = |\alpha|^2 = |\langle\uparrow|\psi\rangle|^2 \qquad \sigma_z = +1$$

$$P_\downarrow = |\beta|^2 = |\langle\downarrow|\psi\rangle|^2 \qquad \sigma_z = -1$$



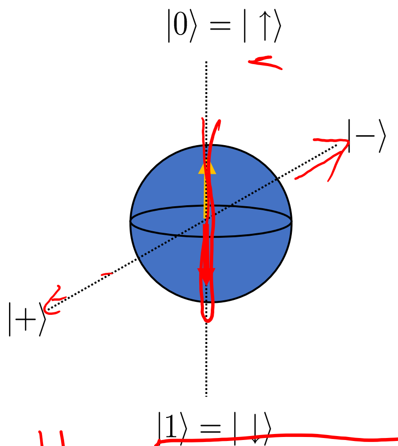
Basic quantum mechanical rules

- Strong measurement projects wavefunction; outcome is often probabilistic

Now we frame the understanding into the **standard QM language**:

$$P_\uparrow = |\alpha|^2 = |\langle\uparrow|\psi\rangle|^2 \qquad \sigma_z = +1$$

$$P_\downarrow = |\beta|^2 = |\langle\downarrow|\psi\rangle|^2 \qquad \sigma_z = -1$$



Observable

The notion of 'observables' is tightly related to the 'basis' of measurement, in this case is the Z operator (as the observable)

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

$$Z = (+1)|\uparrow\rangle\langle\uparrow| + (-1)|\downarrow\rangle\langle\downarrow| =$$

when you diagonalize

The 'eigenvalues' are what we 'read out' and the 'eigenstates' define the measurement basis. **The act of measurement will project the system randomly into one of the eigenstates of the observable**. The average 'score' represents the expected value of the observable over many repeated measurements.

$\alpha|\uparrow\rangle + \beta|\downarrow\rangle \xrightarrow{\text{measurement}}$ $\boxed{|\uparrow\rangle} \rightarrow |\uparrow\rangle$, $|\downarrow\rangle \rightarrow |\downarrow\rangle$

average score $= P_\uparrow(+1) + P_\downarrow(-1) = |\alpha|^2 - |\beta|^2 = \langle\psi|Z|\psi\rangle$

$$\langle\psi|Z|\psi\rangle = P_\uparrow\cdot(+1) + P_\downarrow\cdot(-1)$$

Do poll 2-1

- superposition
- $\boxed{\text{unitary}}$
- measurement

take a state into a superposition

Beyond one qubit---entanglement

The true quantum-ness comes at two qubits or more, where you can have 'entanglement'. Superposition also occurs at classical waves, but entanglement is "the characteristic feature of quantum mechanics" according to Schrödinger

We will also see the advantage of Dirac's 'bra-ket' notation.

For two qubits, there are four basis states (we omit 'tensor product' $\otimes$ notation)

$$|\uparrow\uparrow\rangle \equiv |\uparrow\rangle \otimes |\uparrow\rangle,\ |\uparrow\downarrow\rangle,\ |\downarrow\uparrow\rangle,\ |\downarrow\downarrow\rangle$$

There are entangled states (which cannot be written as a product form)

$$|\Phi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle),\quad |\Psi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$$

$\neq |A\rangle \otimes |B\rangle$ $\longrightarrow$ define "being entangled"

We will see later that they are useful resources for many quantum tasks.
Notation wise, it is cumbersome to write N-qubit states using vectors, as it requires 2^N components

$$|\uparrow\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\downarrow\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |\uparrow\rangle \otimes |\downarrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$|\uparrow\downarrow\uparrow\rangle$ $\Downarrow$ 8-component

Two-qubit gates

$$|\Phi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle), \quad |\Psi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$$

We now illustrate how to obtain one such entangled state from applying gates to the product state $|\uparrow\uparrow\rangle$; we introduce the CNOT (Controlled-NOT or Controlled-X) gate

$|\uparrow\rangle - \boxed{X} \rightarrow |\downarrow\rangle$

(comes from unitary evolution e^{-iHt})

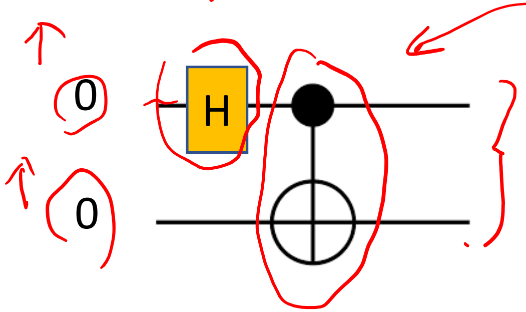
$$\mathrm{CNOT}_{12} = |\uparrow\rangle\langle\uparrow| \otimes I + |\downarrow\rangle\langle\downarrow| \otimes X = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

Then

superposition

$$|\uparrow\uparrow\rangle \xRightarrow{H_1} \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \otimes \underset{X}{|\uparrow\rangle} \xRightarrow{\mathrm{CNOT}_{12}} \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$$

In terms of a quantum circuit (which we introduce now), it can be represented as:



where we use 0 and 1 instead of up and down arrows, and we have introduced the diagram for the CNOT gate

measurement 1 & 2 $(\uparrow/\downarrow)$

two possible outcomes

① $\uparrow\uparrow$, $p=\frac{1}{2}$

② $\downarrow\downarrow$, $p=\frac{1}{2}$

Even if you never learn quantum mechanics before, you can still learn quantum information and computation provided you know matrices and vectors (linear algebra).

Remember the three basic rules of QM and how to understand them in terms of linear algebra.

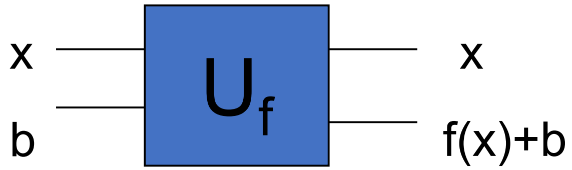
We are ready for the first quantum algorithm.

Balanced or constant? Deutsch algorithm

- Consider a function *f* mapping from one bit to one bit

  ➔ Four possibilities, classified into two categories:

x	f1(x)	f2(x)	f3(x)	f4(x)
0	0	1	1	0
1	0	1	0	1



constant — $f(1) = f(0)$

balanced — $f(1) = f(0) + 1$

+ (addition modulo 2):
1+1=0

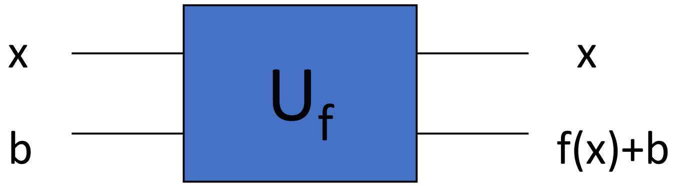
- Question: Is the function “balanced” or “constant”?

  Equivalently: $f(0) \oplus f(1) = ?$

  - Classical computers: need two function evaluations to determine
  - Quantum computers: need one evaluation

Useful observation/trick: `phase kickback'

- Suppose the effect of the circuit is to compute f(x) and add it to second register:



$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |f(x)+b\rangle$$

1   1+1=0

- If we send in $|x\rangle \otimes (|0\rangle - |1\rangle)$, ignoring normalization

$\sqrt{2}$ 0 $|0+1\rangle$

$$|x\rangle \otimes (|0\rangle - |1\rangle) \;\rightarrow |x\rangle \otimes (|f(x)\rangle - |f(x)+1\rangle)$$

$$= |x\rangle \otimes (-1)^{f(x)}(|0\rangle - |1\rangle)$$

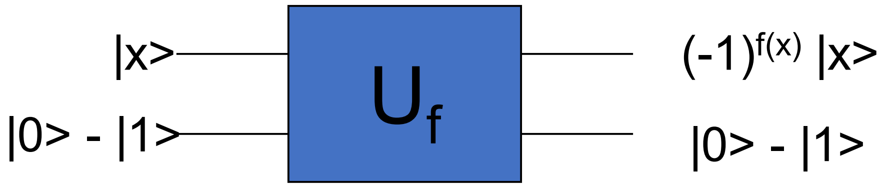
By linearity & superposition

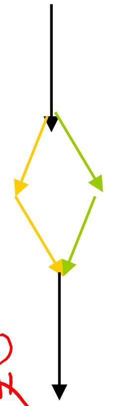
- Phase kickback:

e.g. $f(x)=0$ $f(x)=1$

$$|x\rangle \otimes (|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)}|x\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch algorithm: one function call

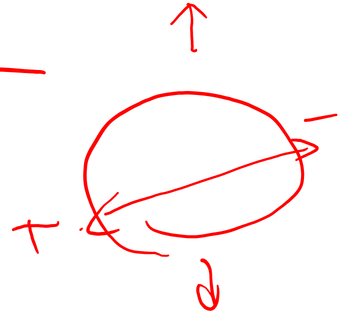




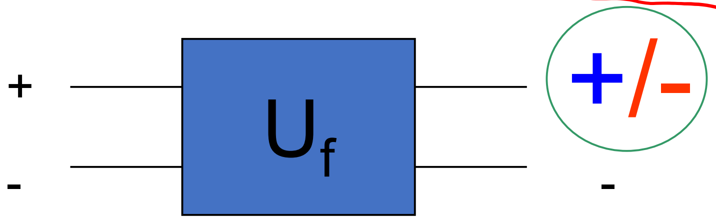
Quantum explores Parallel universes?

- Consider sending |0>+|1> in first register (and |0>-|1> in the second):

$$|0\rangle + |1\rangle \rightarrow \overset{0}{(-1)^{f(0)}}|0\rangle + \overset{1}{(-1)^{f(1)}}|1\rangle \rightarrow \begin{cases} \overset{f(1)=}{(-1)^{f(0)}}(|0\rangle + |1\rangle) & \text{constant} \\ (-1)^{f(0)}(|0\rangle - |1\rangle) & \text{balanced} \end{cases}$$



- Quantum computers: need one evaluation only and measure in +/- basis $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$



➔ Measure: + constant

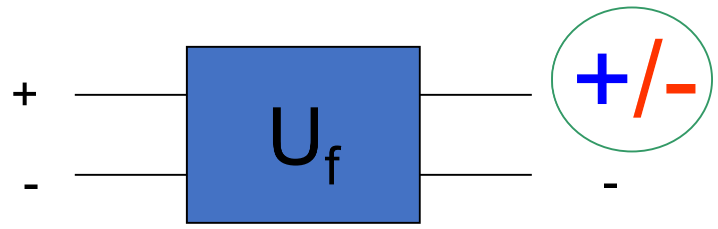
- balance

- First hint that quantum computer can be powerful!

Comment on input and readout

- Quantum computers: need one evaluation only and measure in +/- basis

$$|\pm\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$$

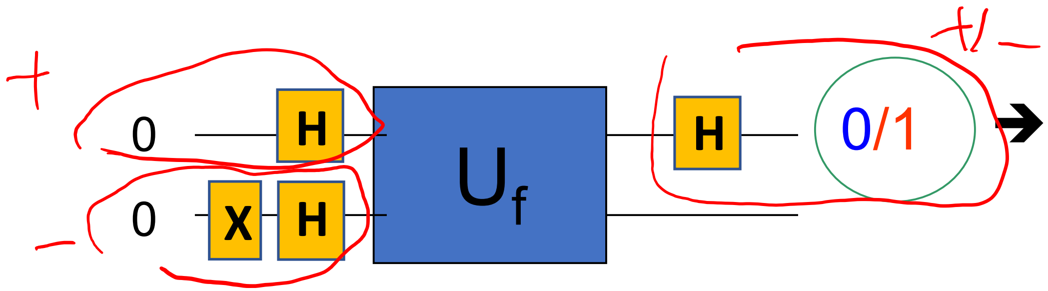


➔ Measure: + constant
- balanced

- Usually, qubits are initialized to 0 and measurement is in 0/1 basis

➔ Use X gate to flip 0 to 1

➔ Use Hadamard gate to transform between 0/1 and +/-



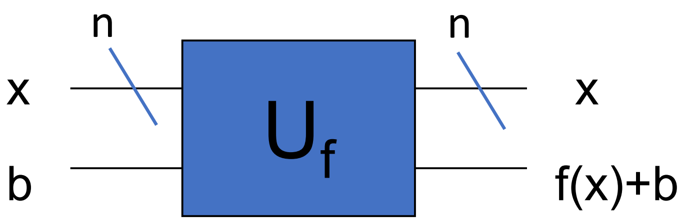
➔ Measure: 0 constant
1 balanced

Do poll 2-2

Got to here on Wed 8/26

Exercise: Deutsch-Josza Algorithm

Here we consider unknown function *f* that maps from n-bits to 1-bit. We are promised that f is either constant (f= the same value) or balanced (the latter means exactly half of inputs f(x)=1, and other half f(x)=0). This generalizes Deutsch's problem from one bit to n bits.



$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |f(x)+b\rangle$$

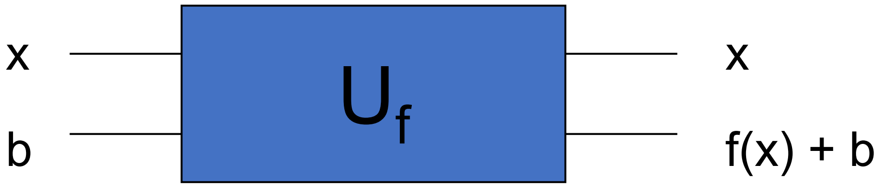
$$|x\rangle = [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes n} = \underbrace{H \otimes H \otimes \ldots H}_{n} \underbrace{|0\rangle \otimes |0\rangle \otimes \ldots |0\rangle}_{n}$$

$$|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

(1) Show the quantum state after the circuit.
(2) Show that if f is constant, the first register is always +…+
(3) Show that if f is balanced, the first register is always orthogonal to +…+

Quantum Parallelism

- Consider the unitary evolution that evaluates f(x)



x=00..0, 00..1,
…, 11..1
binary rep. of 0,1,2,..

$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |f(x)+b\rangle$$

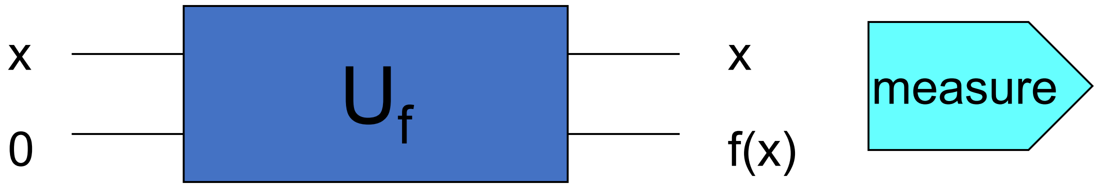
- Use superposition inputs:

$$(|0\rangle + |1\rangle + |2\rangle + \ldots) \otimes |0\rangle$$

$$\rightarrow (|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + |2\rangle \otimes |f(2)\rangle + \ldots)$$

- Parallelism → superposition of (argument, fcn value)
  → potential power of quantum computers!

Measurement causes complication



$$\sum_{k=0}^{2^n-1} |k\rangle \otimes |0\rangle \rightarrow \sum_{k=0}^{2^n-1} |k\rangle \otimes |f(k)\rangle$$

- To obtain answer: Need to measure!

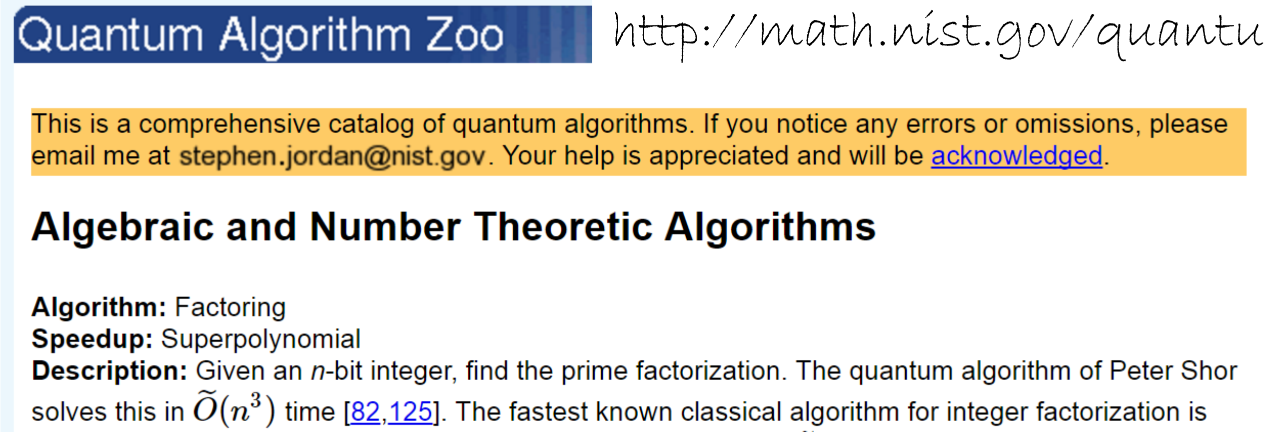
  - e.g. measure first register: *k* ➔ second register: *f*(k)
    only one answer at a time ☹ (and k is random)

  - But can measure in different basis or/and second register

    e.g. measure second register, obtain f_0 ,
    ➔ first register in superposition of x such that f(x) = f_0

➔ QC useful only for determining symmetry properties of f

More quantum algorithms

- 

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@nist.gov. Your help is appreciated and will be acknowledged.

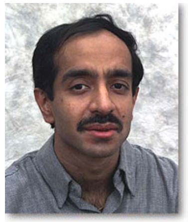
Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is

http://math.nist.gov/quantum/zoo/

- Notable ones:
  - Shor's factoring [~ exponential speedup]
  - Grover's searching [~ quadratic speedup]
  - Quantum Algorithm for Linear System: $A\vec{x} = b$
    [~ can be exponential speedup]
    aka HHL (Harrow-Hassidim-Lloyd) algorithm

Shor

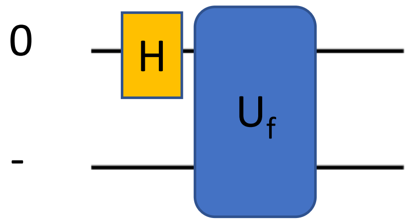


Grover

We will discuss: Grover’s, Shor’s and HHL algorithms later. We discuss two other simpler problems and algorithms next.

Berstein-Vazirani algorithm

- Simplest case: one qubit and the linear function is f(x)= a.x



$$|0\rangle - |1\rangle$$

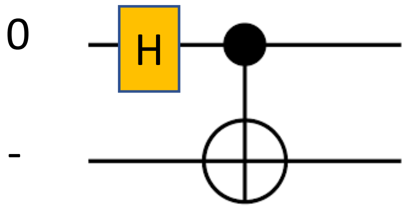
$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |f(x)+b\rangle$$

$$\text{first register}: |0\rangle \xrightarrow{H} |0\rangle + |1\rangle \xrightarrow{U_f} (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$

For a=1, f(x)=x, and thus it is a CNOT

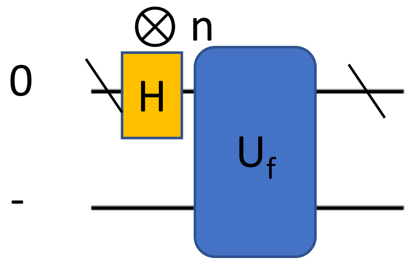
$$\rightarrow |0\rangle - |1\rangle$$

presence of a=1 can be detected in +/- basis



n-qubit Berstein-Vazirani algorithm

- For n qubits: the linear function is **f(x) = a.x**, where **a** & **x** are both n-component binary vectors



$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |f(x)+b\rangle$$

$$|0\rangle - |1\rangle$$

$$\text{first register} : |0^{\otimes n}\rangle \xrightarrow{H^{\otimes n}} \sum_{x_i' s} |x_1\rangle \otimes |x_2\rangle \otimes \cdots |x_n\rangle$$

$$\xrightarrow{U_f} \sum_{x_i' s} (-1)^{\sum_i a_i x_i} |x_1\rangle \otimes |x_2\rangle \otimes \cdots |x_n\rangle = \otimes_i (|0\rangle + (-1)^{a_i}|1\rangle)_i$$

✓ Presence of a_i=1 can be detected in +/- basis

Simon's algorithm

- Consider a function f:{0,1}^{n} → finite set X.
  We are promised that there is some "hidden" string $\boldsymbol{s}$=$s_1s_2..s_n$
  such that f($\boldsymbol{x}$)=f($\boldsymbol{y}$) if and only if $\boldsymbol{x}$=$\boldsymbol{y}$ or $\boldsymbol{x}$=$\boldsymbol{y}\oplus\boldsymbol{s}$ (bitwise XOR)
  ➔ Find string $\boldsymbol{s}$

- Observation: n-qubit Hadamard

$$|\mathbf{0}\equiv 0^{\otimes n}\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}}\sum_{z_i's}|z_1\rangle\otimes|z_2\rangle\otimes\cdots|z_n\rangle = \frac{1}{2^{n/2}}\sum_{\mathbf{z}}|\mathbf{z}\rangle$$

$$|\mathbf{s}\equiv s_1\ldots s_n\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}}\sum_{\mathbf{z}}(-1)^{\mathbf{s}\cdot\mathbf{z}}|\mathbf{z}\rangle$$

➢ If we have a superposition:

$$\frac{1}{\sqrt{2}}(|\mathbf{0}\rangle+|\mathbf{s}\rangle) \xrightarrow{H^{\otimes n}} \frac{1}{2^{(n+1)/2}}\sum_{\mathbf{z}}(1+(-1)^{\mathbf{s}\cdot\mathbf{z}})|\mathbf{z}\rangle$$

➔ no amplitude for $\boldsymbol{s}\cdot\boldsymbol{z}$=1 (mod 2)
i.e. only get $\boldsymbol{z}$ orthogonal to $\boldsymbol{s}$

$$= \frac{1}{2^{(n-1)/2}}\sum_{\mathbf{z}\in\{\mathbf{s}\}^{\perp}}|\mathbf{z}\rangle$$

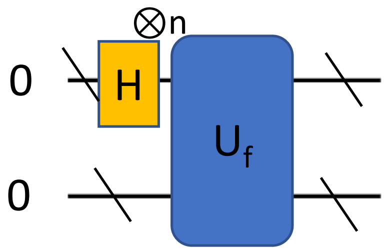
Simon's algorithm (cont'd)

$$\frac{1}{\sqrt{2}}(|\mathbf{0}\rangle + |\mathbf{s}\rangle) \xrightarrow{H^{\otimes n}} \frac{1}{2^{(n-1)/2}} \sum_{\mathbf{z}\in\{\mathbf{s}\}^{\perp}} |\mathbf{z}\rangle$$

- More generally $$\frac{1}{\sqrt{2}}(|\mathbf{x}\rangle + |\mathbf{x}\oplus\mathbf{s}\rangle) \xrightarrow{H^{\otimes n}} \frac{1}{2^{(n-1)/2}} \sum_{\mathbf{z}\in\{\mathbf{s}\}^{\perp}} (-1)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle$$

Algorithm for Simon's Problem

$$U_f : |\mathbf{x}\rangle \otimes |\mathbf{b}\rangle \to |\mathbf{x}\rangle \otimes |f(\mathbf{x}) \oplus \mathbf{b}\rangle$$



1. Set a counter $i = 1$.
2. Prepare $\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle|\mathbf{0}\rangle$.
3. Apply U_f, to produce the state

$$\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle|f(\mathbf{x})\rangle.$$

4. (optional[2]) Measure the second register.
5. Apply $H^{\otimes n}$ to the first register.
6. Measure the first register and record the value $\mathbf{w}_i$.
7. If the dimension of the span of $\{\mathbf{w}_i\}$ equals $n-1$, then go to Step 8, otherwise increment i and go to Step 2.
8. Solve the linear equation $\mathbf{W}\mathbf{s}^T = \mathbf{0}^T$ and let $\mathbf{s}$ be the unique non-zero solution.
9. Output $\mathbf{s}$.