

Do poll 8/31-(1)

Today 8/31:

(1) Some review: Bloch sphere, mixed states, phase kickback, Deutsch algorithm

(2) Jupyter Notebook Demo

<https://nbviewer.jupyter.org/url/insti.physics.sunysb.edu/~twei/Courses/Fall2020/PHY682/Demo-QubitSphere.ipynb>

(3) More algorithms

(4) Week 2: From foundation to science-fiction teleportation

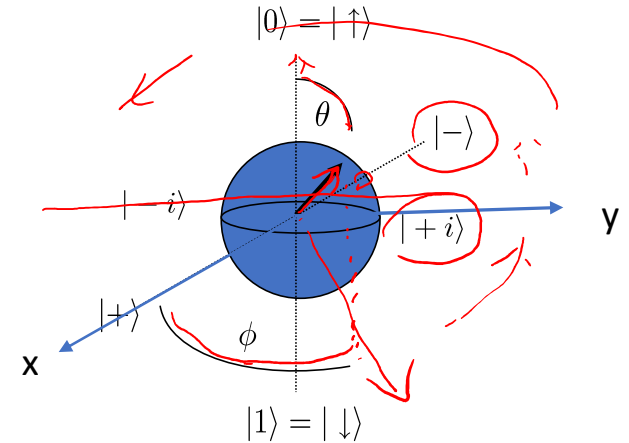
Review: Bloch sphere of a qubit

$|\psi\rangle = \cos(\theta/2)|\uparrow\rangle + e^{i\phi}\sin(\theta/2)|\downarrow\rangle$ is the same as

$\rho_\psi = |\psi\rangle\langle\psi| = \frac{1}{2}(I + r_x X + r_y Y + r_z Z)$

$r_x = \sin\theta \cos\phi, r_y = \sin\theta \sin\phi, r_z = \cos\theta$

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



Example: what is the state on the sphere along negative x axis (|->)? positive y axis (|i>)?

$|-\rangle: \theta = \frac{\pi}{2}, \phi = \pi \quad |-\rangle = \cos\frac{\pi}{4}|0\rangle + e^{i\pi}\sin\frac{\pi}{4}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$|i\rangle: \theta = \frac{\pi}{2}, \phi = \frac{\pi}{2} \quad |i\rangle = \cos\frac{\pi}{4}|0\rangle + e^{i\frac{\pi}{2}}\sin\frac{\pi}{4}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

$|-i\rangle: \theta = \frac{\pi}{2}, \phi = \frac{3\pi}{2} \quad |-i\rangle = \cos\frac{\pi}{4}|0\rangle + e^{i\frac{3\pi}{2}}\sin\frac{\pi}{4}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Example: How do we use quantum gates to obtain these states starting from $|0\rangle$?

$S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
 $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$|0\rangle \xrightarrow{\text{Hadamard}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $|1\rangle = X|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Review: mixed state

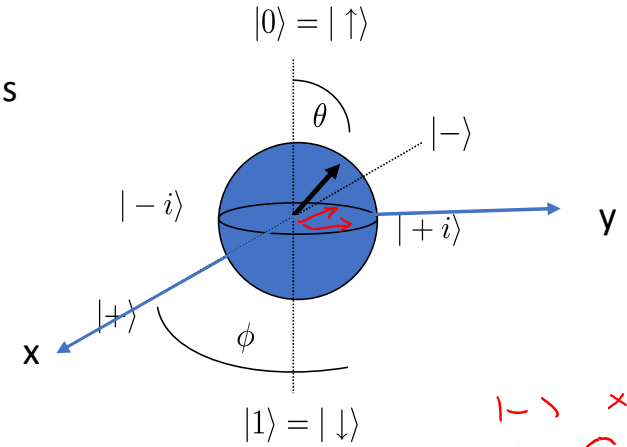
(mixture of pure state)

$|\psi\rangle = \cos(\theta/2)|\uparrow\rangle + e^{i\phi} \sin(\theta/2)|\downarrow\rangle$ is the same as

$$\rho_\psi = |\psi\rangle\langle\psi| = \frac{1}{2}(I + r_x X + r_y Y + r_z Z)$$

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

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



$|-\rangle$ x-y plane mixture $|+i\rangle$

Example: how do we represent equal weight mixture of $|-\rangle$ and $|i\rangle$?

mixture $(\alpha|-\rangle + \beta|i\rangle)$ not mixing $\rightarrow |\rho| = 1$

$$\rho = \frac{1}{2}|-\rangle\langle-| + \frac{1}{2}|i\rangle\langle i|$$

$$\rho = \frac{1}{2}r_- + \frac{1}{2}r_i$$

$\text{tr}(\hat{O}_S \rho)$
 $= \langle \psi | \hat{O}_S | \psi \rangle$

Example: a mixed state can arise from entanglement with other system

2-qubit $|\psi\rangle = \frac{1}{\sqrt{2}}(|-\rangle|0\rangle + |i\rangle|1\rangle)$

when I "ignore" (trace over) the env \Rightarrow get mixed for the system.

Review: observable and measurement

- Strong measurement projects wavefunction; outcome is often probabilistic

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

randomly $|\uparrow\rangle$ or $|\downarrow\rangle$



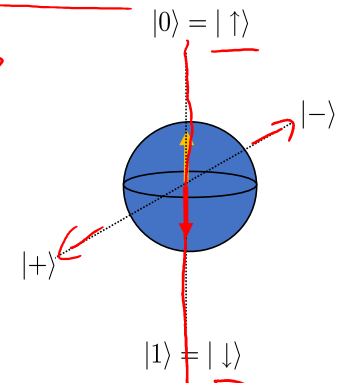
$$P_{\uparrow} = |\alpha|^2 = |\langle\uparrow|\psi\rangle|^2$$

$$\sigma_z = +1$$



$$P_{\downarrow} = |\beta|^2 = |\langle\downarrow|\psi\rangle|^2$$

$$\sigma_z = -1$$



'Observables' \leftrightarrow 'basis' of measurement (and possible measured values)

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

$$\text{Expectation value: } \langle\psi|Z|\psi\rangle = P_{\uparrow} \cdot (+1) + P_{\downarrow} \cdot (-1)$$

Suppose two-qubit eg.

$$|\Psi\rangle = \alpha|\uparrow\rangle|0\rangle_{env} + \beta|\downarrow\rangle|1\rangle_{env}$$

if measure the system

$$\left\{ \begin{array}{l} \uparrow : |\alpha|^2, env \Rightarrow |0\rangle \\ \downarrow : |\beta|^2, env \Rightarrow |1\rangle \end{array} \right.$$

- Example: When the observable is X? What is the probability to measure +?

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (+1)|+\rangle\langle+| + (-1)|-\rangle\langle-|$$

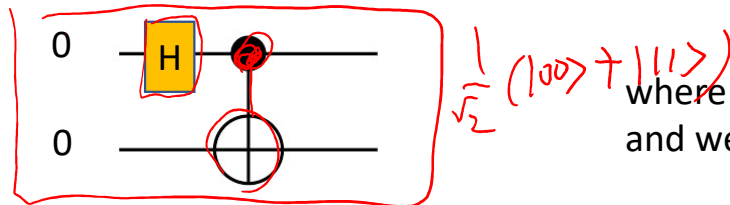
$$P_{+} = |\langle+|\Psi\rangle|^2 \quad P_{-} = |\langle-|\Psi\rangle|^2$$

Review: CNOT (controlled-NOT) gate and the balanced function

$$\text{CNOT}_{12} = \underbrace{|\uparrow\rangle\langle\uparrow|}_{10X01} \otimes I + \underbrace{|\downarrow\rangle\langle\downarrow|}_{01X01} \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{array}{l} \begin{array}{l} \boxed{00} \rightarrow \boxed{00} \\ \boxed{01} \rightarrow \boxed{01} \end{array} \quad \begin{array}{l} \boxed{10} \rightarrow \boxed{11} \\ \boxed{11} \rightarrow \boxed{10} \end{array} \\ |x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |b + f(x)\rangle \end{array}$$

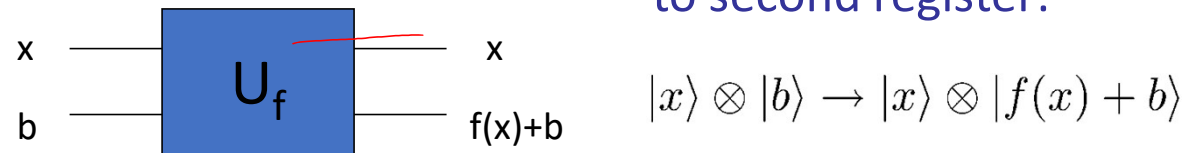
$$|\uparrow\uparrow\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \otimes |\uparrow\rangle \xrightarrow{\text{CNOT}_{12}} \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$$



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

Review: 'phase kickback'

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



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

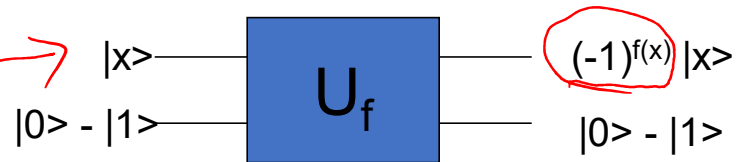
$$\begin{aligned}
 |x\rangle \otimes (|0\rangle - |1\rangle) &\rightarrow |x\rangle \otimes (|f(x)\rangle - |f(x) + 1\rangle) && \text{By linearity \& superposition} \\
 &= |x\rangle \otimes (-1)^{f(x)} (|0\rangle - |1\rangle) && \text{verify } \begin{cases} f(0) = 0 \\ f(1) = 1 \end{cases}
 \end{aligned}$$

forget this

- Phase kickback:

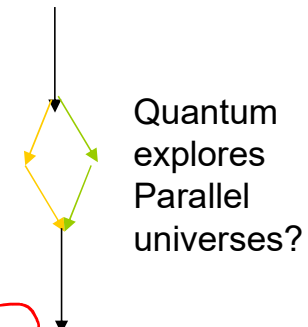
$$|x\rangle \otimes (|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch algorithm: one function call

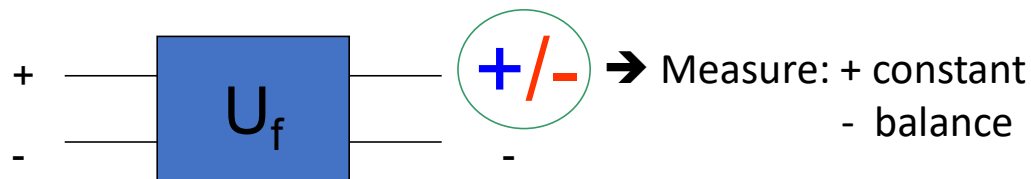


- Consider sending $|0\rangle + |1\rangle$ in first register (and $|0\rangle - |1\rangle$ in the second):

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



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

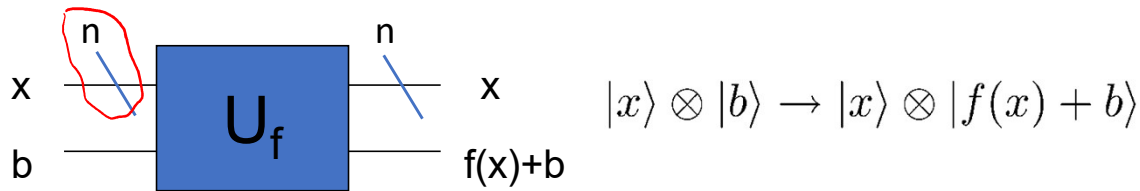


- First hint that quantum computer can be powerful!

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.

n lines
 $\times \{ \equiv \}$



$$|x\rangle = \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right]^{\otimes n} = \underbrace{H \otimes H \otimes \dots \otimes H}_n |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle$$

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

$$H^{\otimes n} = H \otimes H \otimes \dots \otimes H$$

$$H^{\otimes n} |s_1 s_2 \dots s_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1, z_2, \dots, z_n} (-1)^{\sum s_i z_i} |z_1 z_2 \dots z_n\rangle$$

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

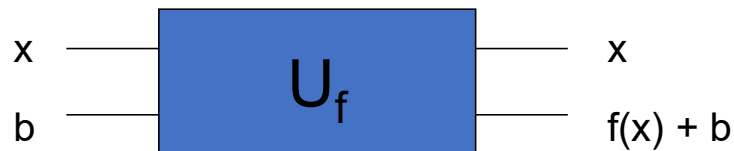
$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$H^{\otimes n} |s_1\rangle = \frac{1}{\sqrt{2}} \sum_{z_1, z_2, \dots, z_n} (-1)^{\sum s_i z_i} |z_1 z_2 \dots z_n\rangle$$

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

Quantum Parallelism

- Consider the unitary evolution that evaluates $f(x)$



$x=00..0, 00..1, \dots, 11..1$
binary rep. of $0, 1, 2, \dots$

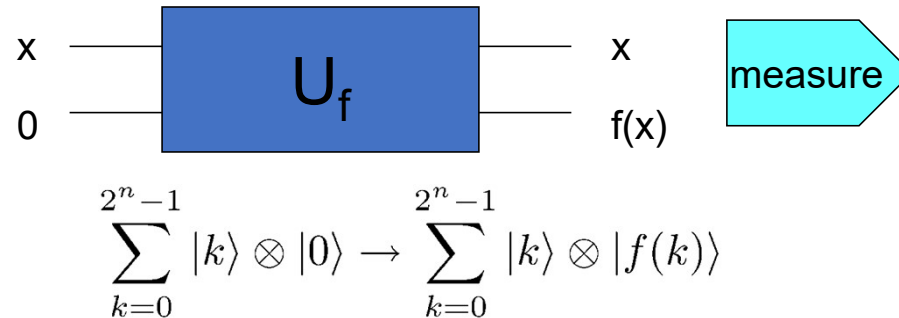
$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |f(x) + b\rangle$$

- Use superposition inputs:

$$\begin{aligned} &(|0\rangle + |1\rangle + |2\rangle + \dots) \otimes |0\rangle \\ &\rightarrow (|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + |2\rangle \otimes |f(2)\rangle + \dots) \end{aligned}$$

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

Measurement causes complication



❑ To obtain answer: Need to measure!

- e.g. measure first register: $k \rightarrow$ 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 ,
 \rightarrow first register in superposition of x such that $f(x) = f_0$
- \rightarrow QC useful only for determining symmetry properties of f

More quantum algorithms

- Quantum Algorithm Zoo <http://math.nist.gov/quantum/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 $\tilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is

Notable ones:

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



Shor



Grover

We will first see a Jupyter Notebook demo

(Just to give you an idea of the programming as an alternative way to learn quantum computing. You don't need to understand all the details; as long as you can modify and have fun with the codes.)

<https://nbviewer.jupyter.org/url/insti.physics.sunysb.edu/~twei/Courses/Fall2020/PHY682/Demo-QubitSphere.ipynb>

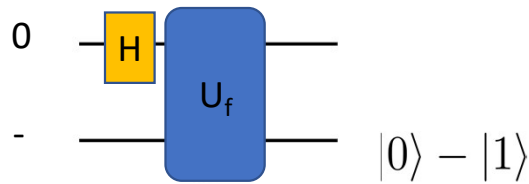
We will then look at two other simple algorithms.

Berstein-Vazirani algorithm

$f: \{ \text{bit} \} \rightarrow \{ \text{bit} \}$

Simplest case: one qubit and the linear function is $f(x) = a \cdot x$

$f(x) = a \cdot x$



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

$a \in \{0, 1\}$
 $a=0, f(x)=0$
 $a=1, f(x)=x$

$f(x) = x$

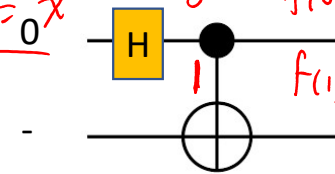
first register : $|0\rangle \xrightarrow{H} |0\rangle + |1\rangle \xrightarrow{U_f} (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$

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

$|0\rangle - |1\rangle$

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

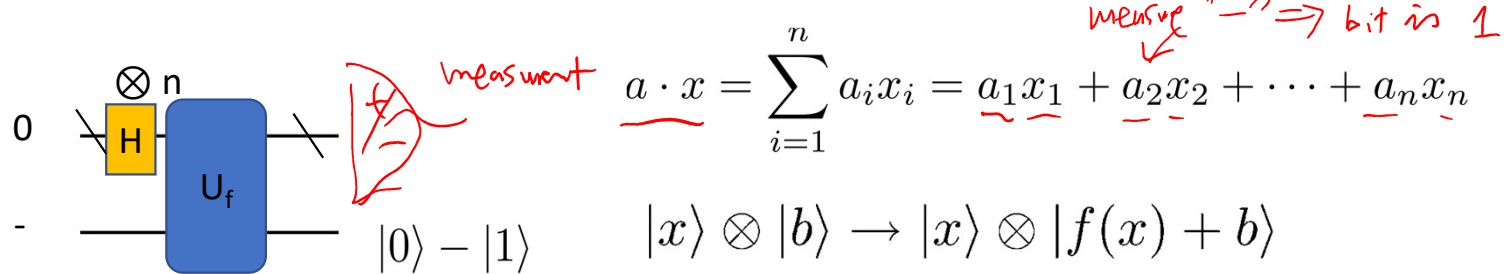
$f(x) = 0$



$f(0) = 0 \rightarrow$ add 0 to b (no action)
 $f(1) = 1 \rightarrow$ add 1 to b (flip b)

n-qubit Bernstein-Vazirani algorithm

- For n qubits: the linear function is $\mathbf{f}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x}$, where \mathbf{a} & \mathbf{x} are both n-component binary vectors



first register : $|0^{\otimes n}\rangle \rightarrow \sum_{x'_i s}^{\mathbf{H}^{\otimes n}} |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$

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

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

Simon's algorithm*

□ Consider a function $f: \{0,1\}^n \rightarrow \text{finite set } X$.

We are promised that there is some "hidden" string $\mathbf{s} = s_1 s_2 \dots s_n$ such that $f(\mathbf{x}) = f(\mathbf{y})$ if and only if $\mathbf{x} = \mathbf{y}$ or $\mathbf{x} = \mathbf{y} \oplus \mathbf{s}$ (bitwise XOR)

→ Find string \mathbf{s}

$x = 000$
 $s = 010$
 $y = 010$ → evaluate to same value

□ Observation: n-qubit Hadamard

$$|0 \equiv 0^{\otimes n}\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}} \sum_{z'_i} |z_1\rangle \otimes |z_2\rangle \otimes \dots \otimes |z_n\rangle = \left(\frac{1}{2^{n/2}} \sum_{\mathbf{z}} |\mathbf{z}\rangle \right)$$

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

$$\mathbf{s} \cdot \mathbf{z} = \sum_i s_i z_i \quad (\text{binary addition})$$

➤ If we have a superposition:

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

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

→ no amplitude for $\mathbf{s} \cdot \mathbf{z} = 1 \pmod{2}$
 i.e. only get \mathbf{z} orthogonal to \mathbf{s}

$$\mathbf{s} \cdot \mathbf{z} = 0$$

Simon's algorithm (cont'd)*

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

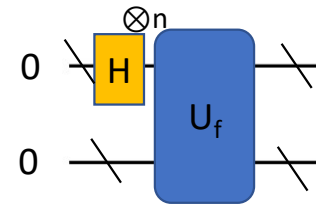
➤ More generally $\frac{1}{\sqrt{2}}(|\mathbf{x}\rangle + |\mathbf{x} \oplus \mathbf{s}\rangle) \xrightarrow{H^{\otimes n}} \frac{1}{2^{(n-1)/2}} \sum_{\mathbf{z} \in \{\mathbf{s}\}^\perp} (-1)^{\mathbf{x} \cdot \mathbf{z}} |\mathbf{z}\rangle$

Algorithm for Simon's Problem

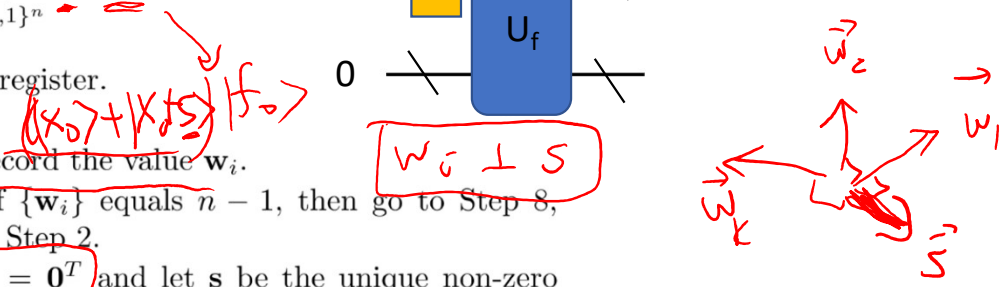
1. Set a counter $i = 1$.
2. Prepare $\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle |\mathbf{0}\rangle$.
3. Apply U_f , to produce the state

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

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



4. (optional²) 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} .



Week 2: From foundation to science-fiction teleportation: Bell inequality, teleportation of states and gates, entanglement swapping, remote state preparation, superdense coding, and superdense teleportation

Quantum entangled states have correlations stronger than classical states

are useful as well

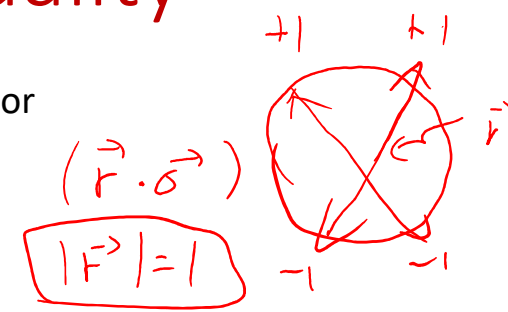
A simple equality and an inequality

We have seen measurement of observables X, Y, Z or any one-qubit operator

$$\vec{r} \cdot \vec{\sigma}, \text{ where } \vec{\sigma} \equiv (X, Y, Z), \quad |\vec{r}| = 1$$

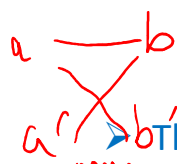
gives an eigenvalue randomly, which is ± 1 in this case.

read out ± 1



It is interesting that for four variables a, a', b, b' which can be ± 1 , we have:

$$ab + ab' + a'b - a'b' = a(b + b') + a'(b - b') = \pm 2$$



Thus, for any probability distribution $p(a, a', b, b')$ we have [using \mathbf{E} to denote expectation]

$$-2 \leq \mathbf{E}(ab + ab' + a'b - a'b') \equiv \sum_{a, a', b, b'} p(a, a', b, b')(ab + ab' + a'b - a'b') \leq 2$$

$b + b' = 0 \quad a + 2 \quad -2$
 $\begin{matrix} +1 & -1 \\ +1 & +1 \\ -1 & +1 \end{matrix}$
 $b - b' = 2a - 2 \quad 0$

In the context of measuring two choices of observables at two locations A: a & a' , B: b & b' , we have the so-called Clauser-Horne-Shimony-Holt (CHSH) inequality:

$$-2 \leq \mathbf{E}(a, b) + \mathbf{E}(a, b') + \mathbf{E}(a', b) - \mathbf{E}(a', b') \leq 2$$

CHSH-Bell inequality (I_{2222})

CHSH generalized John Bell's idea (his original Bell inequality). The assumption is that a source emits e.g. a pair of photons



The choice of measurement axis (a or a') at A or (b or b') at B **cannot affect the outcome of the other side**. Nevertheless, **outcomes can be correlated** and described by some unknown-to-us distribution (depending on some hidden variable λ). This is also called the “**Local hidden variable**” theory

$$E_L(a, b) \equiv \int d\lambda \rho(\lambda) A(a, \lambda) B(b, \lambda)$$

where $A(a, \lambda) = \pm 1$ and $B(b, \lambda) = \pm 1$ are **predetermined results for the measurement settings a for A and b for B depending on the local hidden variable λ** ; $\rho(\lambda)$ is its distribution. Locality requires that the outcome $A(a, \lambda)$ does not depend on setting b and that of $B(b, \lambda)$ does not depend on setting a.

Violation of CHSH-Bell inequality



By averaging over the local hidden variable, we still have

$$|E_L(a, b) + E_L(a, b') + E_L(a', b) - E_L(a', b')| \leq 2. \quad (1)$$

Quantum mechanics can violate this inequality. To be specific, the operators to be measured are the Pauli operators $\vec{\sigma}$. Let $E_Q(a, b) \equiv \langle \psi | \vec{\sigma} \cdot \vec{a} \otimes \vec{\sigma} \cdot \vec{b} | \psi \rangle$ denote expectation of repeated measurement with along axes of unit vectors \vec{a} and \vec{b} , respectively. Define

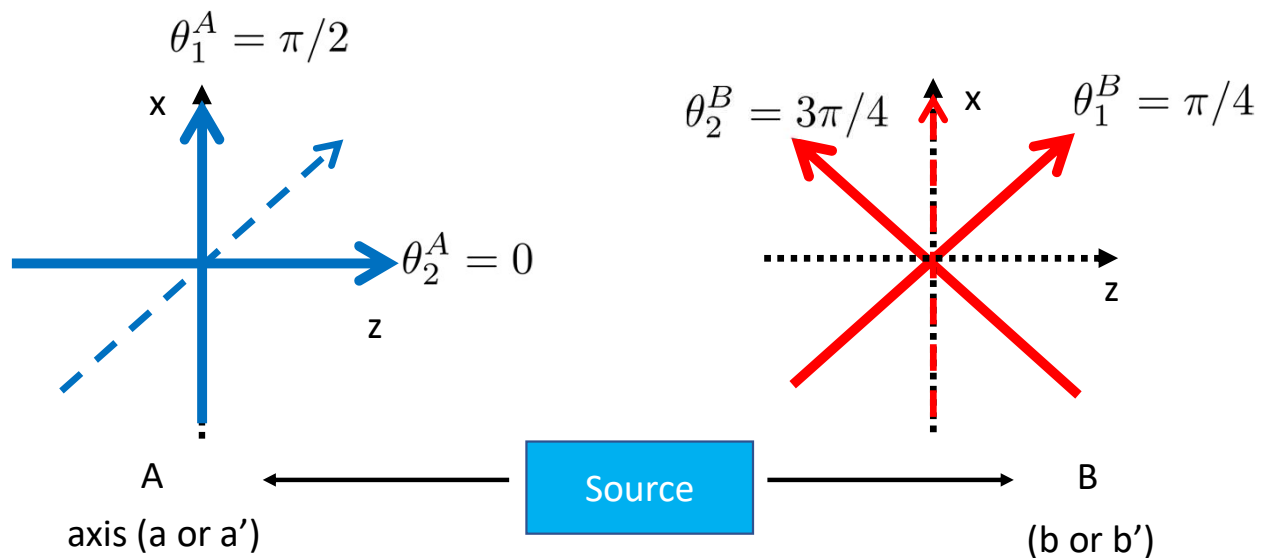
$$2B \equiv \vec{\sigma} \cdot \vec{a} \otimes \vec{\sigma} \cdot \vec{b} + \vec{\sigma} \cdot \vec{a} \otimes \vec{\sigma} \cdot \vec{b}' + \vec{\sigma} \cdot \vec{a}' \otimes \vec{\sigma} \cdot \vec{b} - \vec{\sigma} \cdot \vec{a}' \otimes \vec{\sigma} \cdot \vec{b}'.$$

For a singlet state $|\psi\rangle = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)/\sqrt{2}$, $\max_{a, a', b, b'} |\langle \psi | 2B | \psi \rangle| = 2\sqrt{2}$, which can be achieved for the settings $\theta_a = \pi/2$, $\theta'_a = 0$, $\theta_b = \pi/4$, and $\theta'_b = 3\pi/4$, where the angles are measured from the z -axis in the $z-x$ plane.

Violation of Bell inequality

- Measurement along axes 1 and 2 of A & B are used to check violation of Bell inequality

note: $\langle \psi | \vec{\sigma} \cdot \vec{a} \otimes \vec{\sigma} \cdot \vec{b} | \psi \rangle = -\vec{a} \cdot \vec{b}$



- The bound $2\sqrt{2}$ is the Tsirelson bound. Deriving maximal violation and measurement settings for an arbitrary state is a math problem; see Horodecki et al.