

Quantum Computing

A brief introduction

John Manferdelli

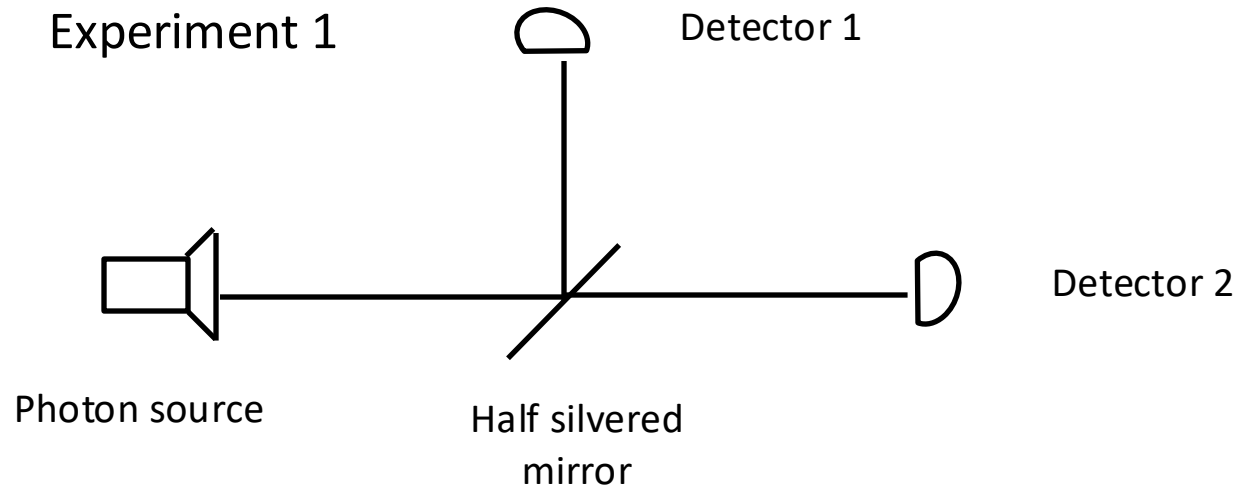
JohnManferdelli@hotmail.com

© 2021-2025, John L. Manferdelli.

This material is provided without warranty of any kind including, without limitation, warranty of non-infringement or suitability for any purpose. This material is not guaranteed to be error free and is intended for instructional use only.

Beam splitters and QM

I can safely say that no one understands Quantum Mechanics - Feynman



Photon source emits stream of photons.

$P(\text{photon arrives at Detector 1}) = .5$

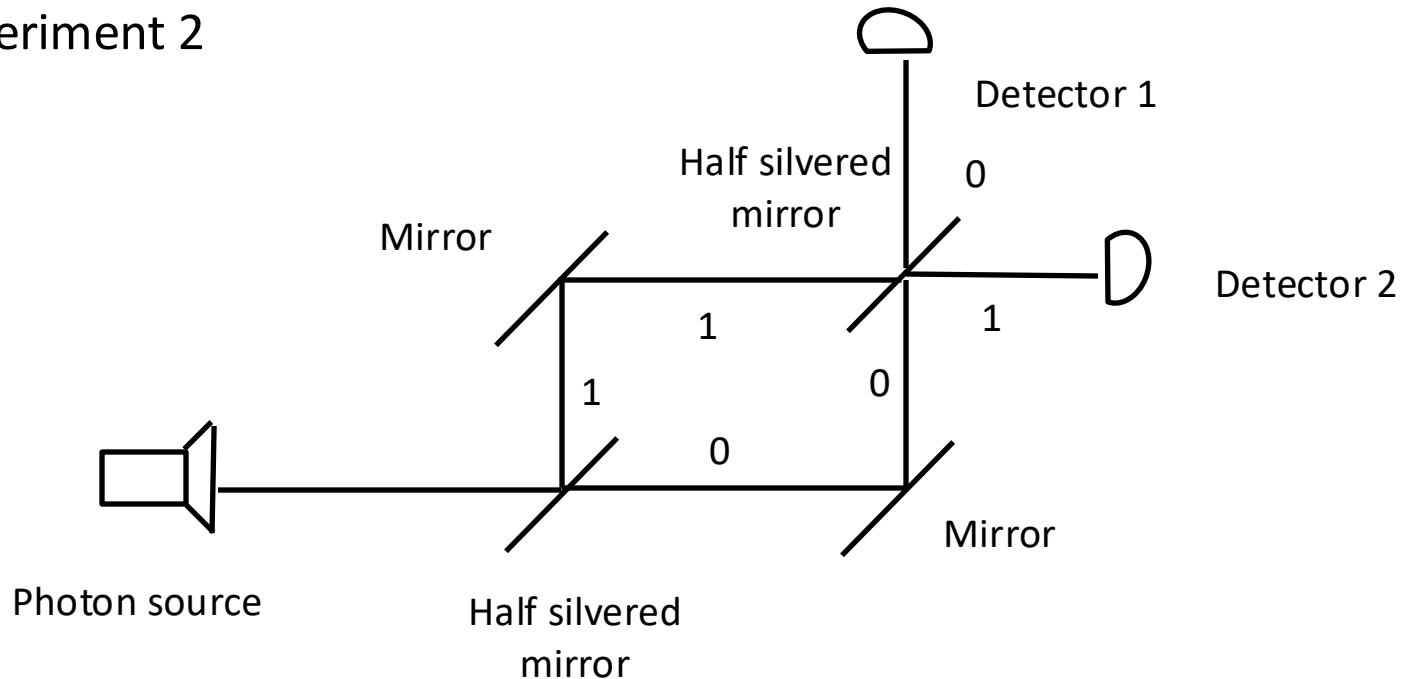
$P(\text{photon arrives at Detector 2}) = .5$

So far, so good

Beam splitters and QM

Mach-Zender Interferometer

Experiment 2



Photon source emits stream of photons.

$P(\text{photon arrives at Detector 1}) = 0$

$P(\text{photon arrives at Detector 2}) = 1$

Huh?

According to QM

Analysis

Beam splitter causes the photon to go into superposition:

$$\alpha_1|0\rangle + \alpha_2|1\rangle, |\alpha_1|^2 = \frac{1}{2}, |\alpha_2|^2 = \frac{1}{2}. |0\rangle \text{ state is right, } |1\rangle \text{ is up.}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Beam splitter acts on incoming state via the matrix $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$.

In experiment 1, if all photons leave source in state $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, after the splitter they are in state $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$. So, they arrive at detector 1 with probability $\frac{1}{2}$ and detector 2 with probability $\frac{1}{2}$.

However, going through another beam splitter, in experiment 2, yields the output state:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix}.$$

So, they always arrive at detector 2.

Postulates

1. State of a system is a unit vector over \mathbb{C} in Hilbert space (\mathcal{H}) of dimension 2^n
 - A qubit is a quantum system, with $n = 1$. A one qubit system is in general state $|\psi\rangle = a|0\rangle + b|1\rangle$, $a\bar{a} + b\bar{b} = 1$
2. A system, with state, $|\psi(t)\rangle$, evolves according to a unitary operator, namely, $U(|\psi(0)\rangle)$
 - U is unitary if $(x, y) = (Ux, Uy)$. Note $UU^\dagger = I$
 - Example is a Hamiltonian: $H(t)|\psi(t)\rangle = i\hbar \frac{d|\psi(t)\rangle}{dt}$
 - $|\varphi(t_2)\rangle = e^{-i\hbar H(t_2-t_1)}|\varphi(t_1)\rangle$
3. Each observable is represented by a Hermitian operator, \hat{Q} , the expectation value of \hat{Q} is $\langle \psi | \hat{Q} | \psi \rangle$. The outcome of a measurement of the operator is an eigenvalue of the operator. The probability of getting a particular eigenvalue, λ , is the square of the λ -component of $|\psi\rangle$

Postulates

4. Two physical systems \mathcal{H}_1 and \mathcal{H}_2 can be treated as a single system, $\mathcal{H}_1 \otimes \mathcal{H}_2$. If \mathcal{H}_1 is in state, $|\psi_1\rangle$ and \mathcal{H}_2 is in state, $|\psi_2\rangle$, the joint state is $|\psi_1\rangle \otimes |\psi_2\rangle$
5. Given an orthonormal basis $\mathcal{B} = \{\varphi_i\}$, one can perform a von-Neuman measurement \mathcal{H}_A on $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle$ that outputs i with probability $|\alpha_i|^2$. It is projective.

Further, if $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle |\gamma_i\rangle$ $\mathcal{H}_A \otimes \mathcal{H}_B$ measurement yields i with probability $|\alpha_i|^2$ and leaves state in $|\varphi_i\rangle |\gamma_i\rangle$. $M = \sum m_i P_i = \sum m_i |i\rangle\langle i|$

Linear Algebra

- Dirac Notation: Element in Hilbert space of dimension 2^n is represented by n-entry symbol. $|000 \dots 00 \rangle \leftrightarrow (1, 0, \dots, 0)^T$, $|000 \dots 01 \rangle \leftrightarrow (0, 1, \dots, 0)^T$, ..., $|111 \dots 1 \rangle \leftrightarrow (0, 0, \dots, 1)^T$ where column vectors have 2^n coordinates.
- Notation: $|0 \rangle \otimes |0 \rangle \otimes \dots \otimes |0 \rangle = |000 \dots 0 \rangle$
- A is normal if $A\bar{A}^T = \bar{A}^T A$
- Spectral Theorem: If T is a normal operator in the Hilbert space \mathcal{H} , there is an orthonormal basis v_i ; each is an eigenvector of T . For every such, there is a unitary matrix, P , $T = P\Lambda P^*$, and Λ is diagonal.
- Dual basis
- Inner product: $(v_1, v_2, \dots, v_n) \cdot (w_1, w_2, \dots, w_n) = \sum_{i=1}^n \bar{v}_i w_i$
- Outer product: $(|\psi \rangle \langle \phi|)|\gamma \rangle = |\psi \rangle (\langle \phi|\gamma \rangle)$
- Theorem: Every linear operator can be written as $T = T_{m,n} |b_m \rangle \langle b_n|$,
- $T_{m,n} = \langle b_m | T | b_n \rangle$

Linear Algebra (continued)

Tensor product: If $|\varphi_i\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ is a basis for \mathcal{H}_1 and $|\phi_i\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$ is a basis for \mathcal{H}_2 ,

$$|\varphi_i\rangle \otimes |\phi_i\rangle \text{ is a basis for } \mathcal{H}_1 \otimes \mathcal{H}_2. \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = (\alpha_0\beta_0, \alpha_0\beta_1, \alpha_1\beta_0, \alpha_1\beta_1)^T. A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}$$

Schmidt decomposition: If $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, there is an orthonormal basis $|\varphi_i\rangle$ for \mathcal{H}_1 and an orthonormal basis $|\phi_i\rangle$ for \mathcal{H}_2 and $p_i \geq 0$ such that $|\psi\rangle = \sum_i \sqrt{p_i} |\varphi_i\rangle |\phi_i\rangle$

$$\text{Tr}(A) = \langle b_n | A | b_n \rangle$$

Eigenvector: $T|\psi\rangle = c|\psi\rangle$

More notation

- $A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$, $x \otimes y = (x_1y_1, x_1y_2, \dots, x_ny_n)^T$
- $|v\rangle = (v_1, v_2, \dots, v_n)^T$, $\langle w| = (w_1, w_2, \dots, w_n)$ then

$$|v\rangle\langle w| = \begin{pmatrix} v_1\overline{w_1} & v_1\overline{w_2} & \dots & v_1\overline{w_n} \\ \dots & \dots & \dots & \dots \\ v_n\overline{w_1} & v_n\overline{w_2} & \dots & v_n\overline{w_n} \end{pmatrix}, \text{ so } I = \sum |i\rangle\langle i| \text{ and } M = \sum M_{ij}|i\rangle\langle j|$$

- Pauli matrices

$$\begin{aligned} - \sigma_0 &= I, \sigma_X = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_Y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_Z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ - [X, Y] &= iZ, [Y, Z] = iX, [Z, X] = iY \end{aligned}$$

Mixed states and density

- For pure states, $|\psi\rangle$, density is $\rho = |\psi\rangle\langle\psi|$
- Mixed states: $\{(p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), \dots, (p_n, |\psi_n\rangle)\}$, where the probability that the system is in pure state $|\psi_i\rangle$ is p_i and $\sum p_i = 1$
- Density operator for mixed state is $\sum p_i |\psi_i\rangle\langle\psi_i|$
- Bloch Sphere
 - Pure state in general position is $|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle$.
 - For mixed state $|\psi_i\rangle = p_i(\alpha_{X,i}, \alpha_{Y,i}, \alpha_{Z,i})$ on interior of Bloch sphere
 - $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$ evolves as $\rho = \sum p_i U |\psi_i\rangle\langle\psi_i| U^\dagger$
 - $\rho = \frac{1}{2}I + \alpha_X X + \alpha_Y Y + \alpha_Z Z$
- $P(|0\rangle) = \langle 0|\psi\rangle\langle\psi|0\rangle = \text{Tr} \langle 0|\psi\rangle\langle\psi|0\rangle = \text{Tr}(|0\rangle\langle 0| |\psi\rangle\langle\psi|)$

Mixed states and density

- Partial trace: Consider composite system AB .
 - $\rho^A = \text{Tr}_B(\rho^{AB})$
 - $\text{Tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \text{Tr}(|b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \langle b_2|b_1\rangle$
 - Example
 - $\rho = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$
 $= \frac{1}{2} \text{Tr}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)$
 $= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

Circuits and gates

- Universal gate set: A gate set is universal if $\forall n > 0$, any n -bit unitary operator can be approximated to arbitrary accuracy by a quantum circuit from this set
- An entangling gate is one that for an input product state $|\alpha\rangle |\beta\rangle$, the output state is not a product state (e.g.-CNOT).
 - Example: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Theorem: A set of states with an entangling 2-qubit gate together with all 1-qubit gates is universal.
- Theorem: If U is a 1-qubit gate, $U = e^{ix} R_z(\beta) R_y(\gamma) R_z(\delta)$

Gates and states

- General position on Bloch sphere: $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$
- Measurement: $I = \sum |i\rangle\langle i|$, $M = \sum m_i P_i$, M is Hermitian, $P_i = |i\rangle\langle i|$.
- Controlled gates:
 - $c - U|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$
 - $c - U|1\rangle|\psi\rangle = |1\rangle U|\psi\rangle$

Common gates

- Pauli gates

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

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

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

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

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

- Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$$H^{\otimes n}(|0000 \dots 0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- Rotation

$$R_X(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{iX\theta} \end{pmatrix} = \begin{pmatrix} e^{-iX\theta/2} & 0 \\ 0 & e^{iX\theta/2} \end{pmatrix}$$

- 2 qubit gate

$$CNOT(|xy\rangle) = |x, x \oplus y\rangle$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

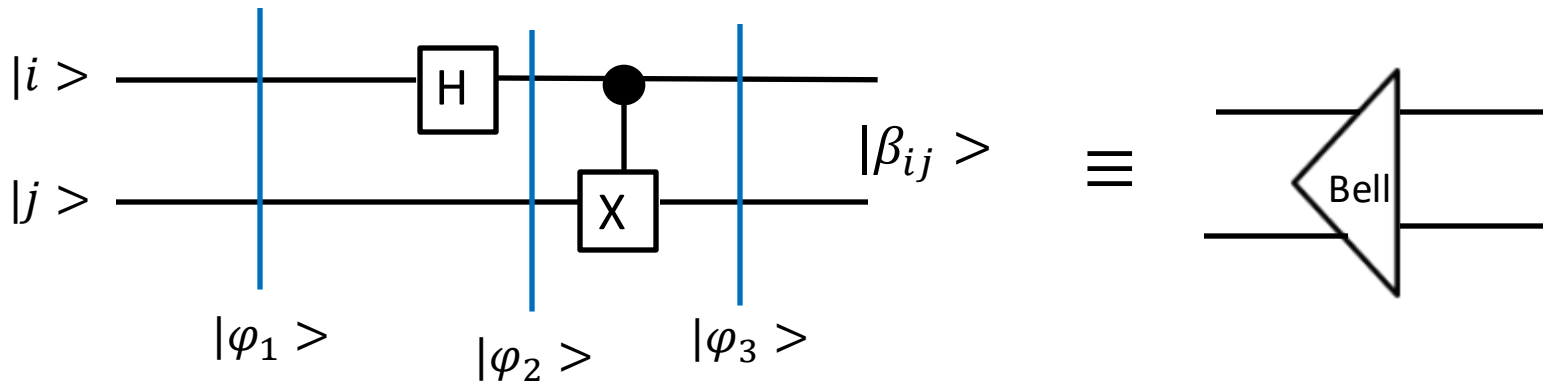
- If $A^2 = 1$, $e^{i\theta X} = I \cos(\theta) + iX \sin(\theta)$

Measurement in alternate basis

- Computational basis is $|i\rangle$. $U|\varphi_j\rangle = |j\rangle$
- Suppose we want to measure $|\psi\rangle$ with respect to basis $B = \{|\varphi_j\rangle\}$
- $|\psi\rangle = \sum \alpha_j |\varphi_j\rangle$
- To measure wrt $B = \{|\varphi_j\rangle\}$, Project $|\psi\rangle$ onto $|\varphi_j\rangle\langle\varphi_j|$
- $(\text{Tr}(|\psi\rangle\langle\psi||\varphi_j\rangle\langle\varphi_j|)) = \text{Tr}(\langle\varphi_j|\psi\rangle\langle\psi|\varphi_j\rangle) = \alpha_j^2$
- $\rho = |\psi\rangle\langle\psi|$ is density operator for the pure state $|\psi\rangle$.
- $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$ is the density operator for mixed states $\{(p_i, |\psi_i\rangle)\}$

Converting to Bell Basis

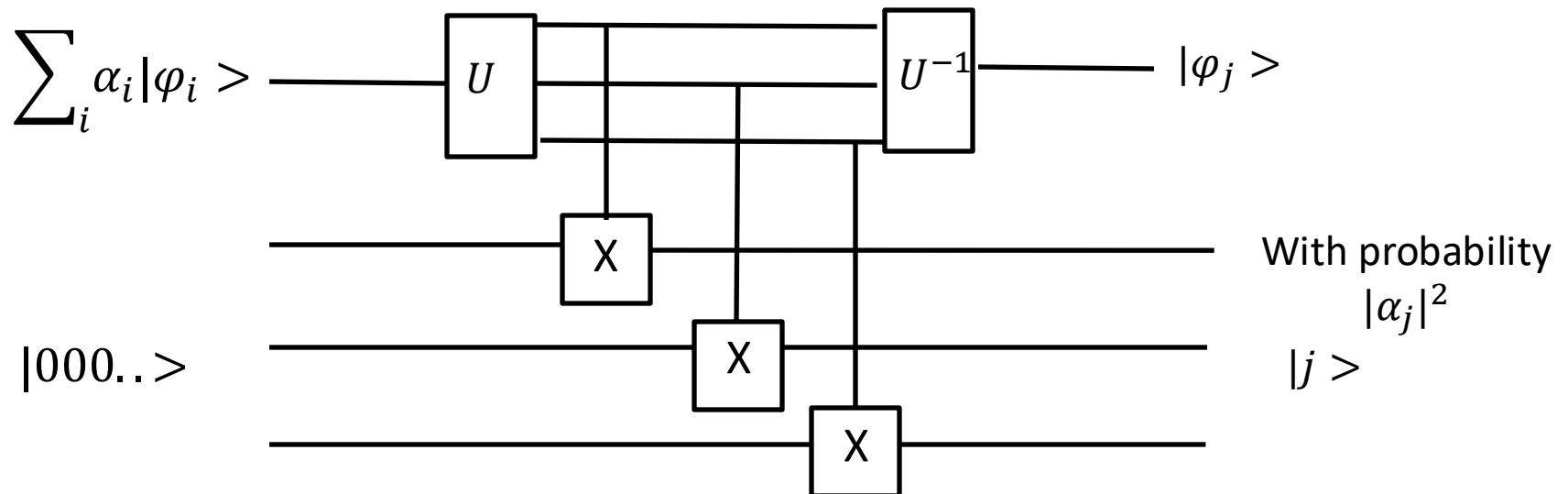
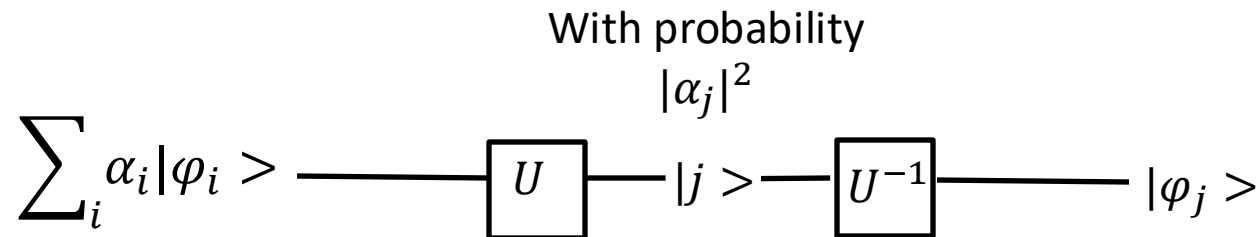
- Computational basis is $|i\rangle$, $U|\varphi_j\rangle = |j\rangle$
- $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$



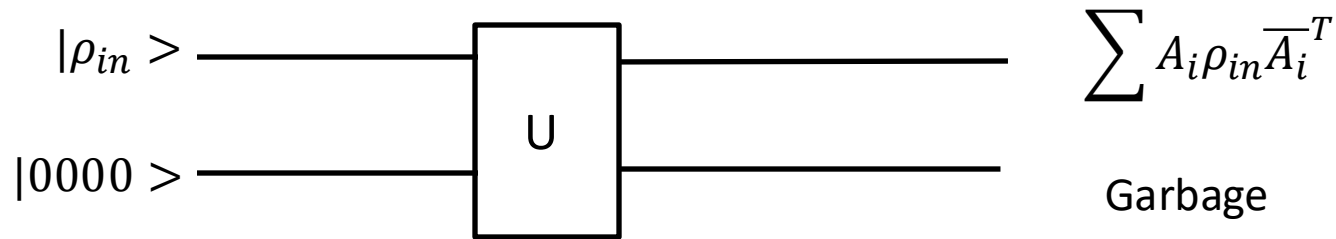
- $|\varphi_1\rangle = |00\rangle$
- $|\varphi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
- $|\varphi_3\rangle = |\beta_{00}\rangle$

Changing Measurement Basis

- Suppose $|\varphi_i\rangle$ is a basis and our measurement basis is $|i\rangle$, $U|\varphi_i\rangle = |i\rangle$



Super-operator and mixed states



- $\rho = |\psi\rangle\langle\psi|$, $U|\psi\rangle$ has density $\rho = U|\psi\rangle\langle\psi|\bar{U}^T = U\rho U^\dagger$
- $\langle 0|\psi\rangle\langle\psi|0\rangle = \langle 0|\rho|0\rangle = P(|0\rangle)$
- $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
- $\text{Tr}(A) = \langle b_n|A|b_n\rangle$
- $\rho_{in} \rightarrow \rho_{out} = \text{Tr}_b(U(\rho_{in} \otimes |000\dots\rangle\langle 000\dots 0|U^\dagger)$
- $\rho_{in} \rightarrow \sum A_i \rho_{in} A_i^\dagger$, where A_i are Kraus operators with $\sum A_i^\dagger A_i = I$

No Cloning Theorem

- Theorem: Qubits can't be copied

- Proof

Suppose they can be. Then there is an operator, U , such that for any state $|\varphi\rangle$, $U(|\varphi\rangle|0\rangle) = |\varphi\rangle|\varphi\rangle$. Now let $|\psi\rangle$ and $|\phi\rangle$ be non-orthogonal, different pure states.

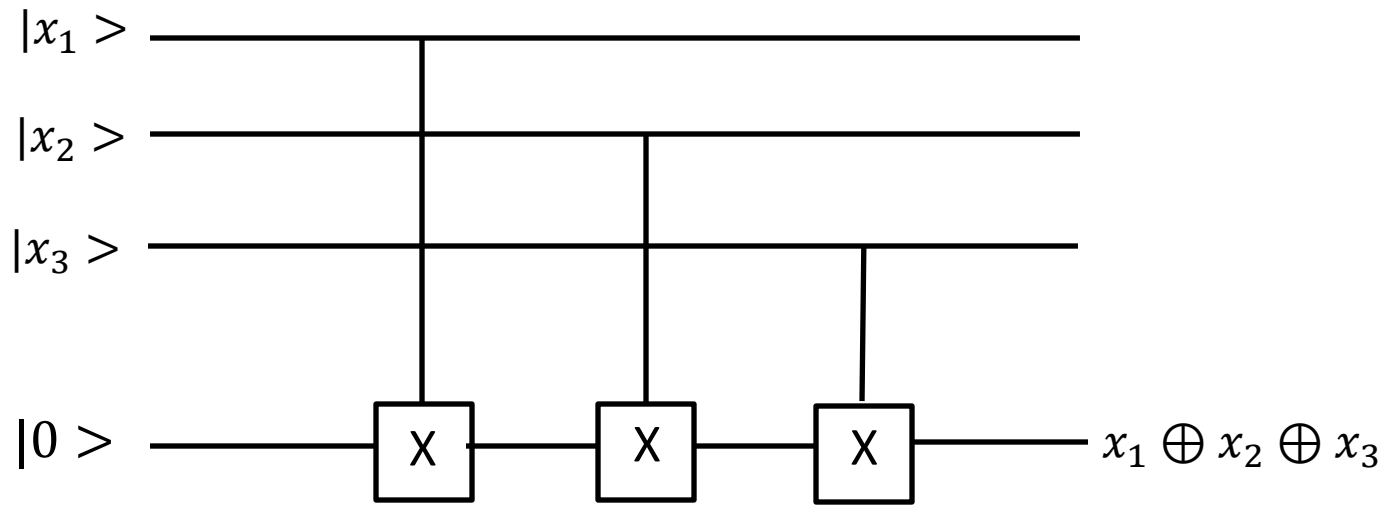
$$(|\psi\rangle|0\rangle, |\phi\rangle|0\rangle) = \langle\psi|\phi\rangle\langle 0|0\rangle = \langle\psi|\phi\rangle.$$

Since U is unitary,

$$\begin{aligned}\langle\psi|\phi\rangle &= (|\psi\rangle|0\rangle, |\phi\rangle|0\rangle) = (U|\psi\rangle|0\rangle, U|\phi\rangle|0\rangle) = \\ &= (|\psi\rangle|\psi\rangle, |\phi\rangle|\phi\rangle) = \langle\psi|\phi\rangle^2. \text{ So, } \langle\psi|\phi\rangle = 1. \text{ This is a contradiction.}\end{aligned}$$

- No checkpointing

Parity Circuit

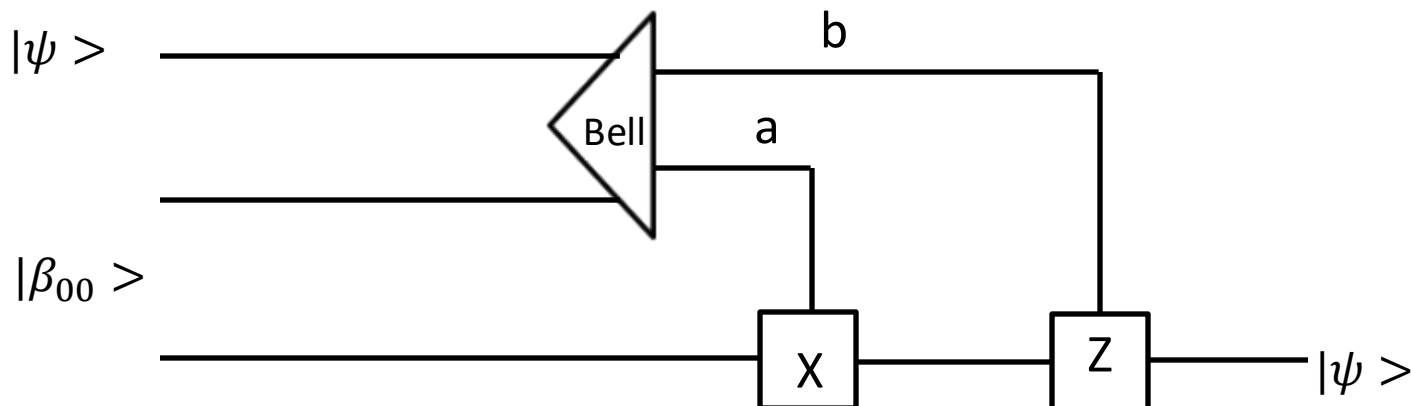


Superdense coding

- Alice and Bob share $|\beta_{00}\rangle$, Alice has first bit, Bob second bit
- Alice performs one of I, X, Y, Z producing $I \otimes I$ (to send 00), $X \otimes I$ (to send 01), $Y \otimes I$ (to send 10) or $Z \otimes I$ (to send 11).
- Bob measures joint state qubit measurement

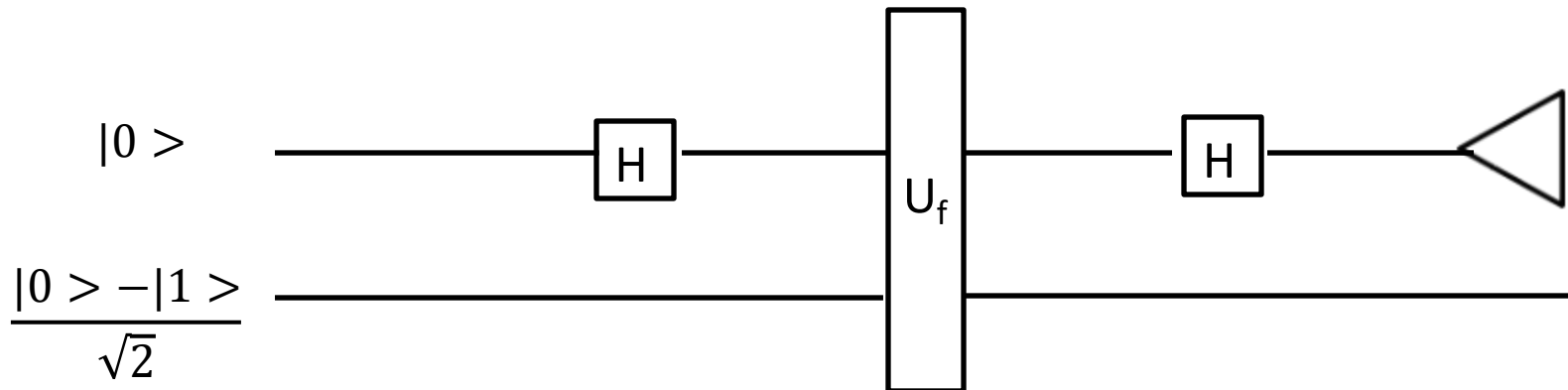
- Can be used to teleport $|\psi\rangle$:

- $I \otimes I := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $X \otimes I := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $Z \otimes I := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- $ZX \otimes I := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$



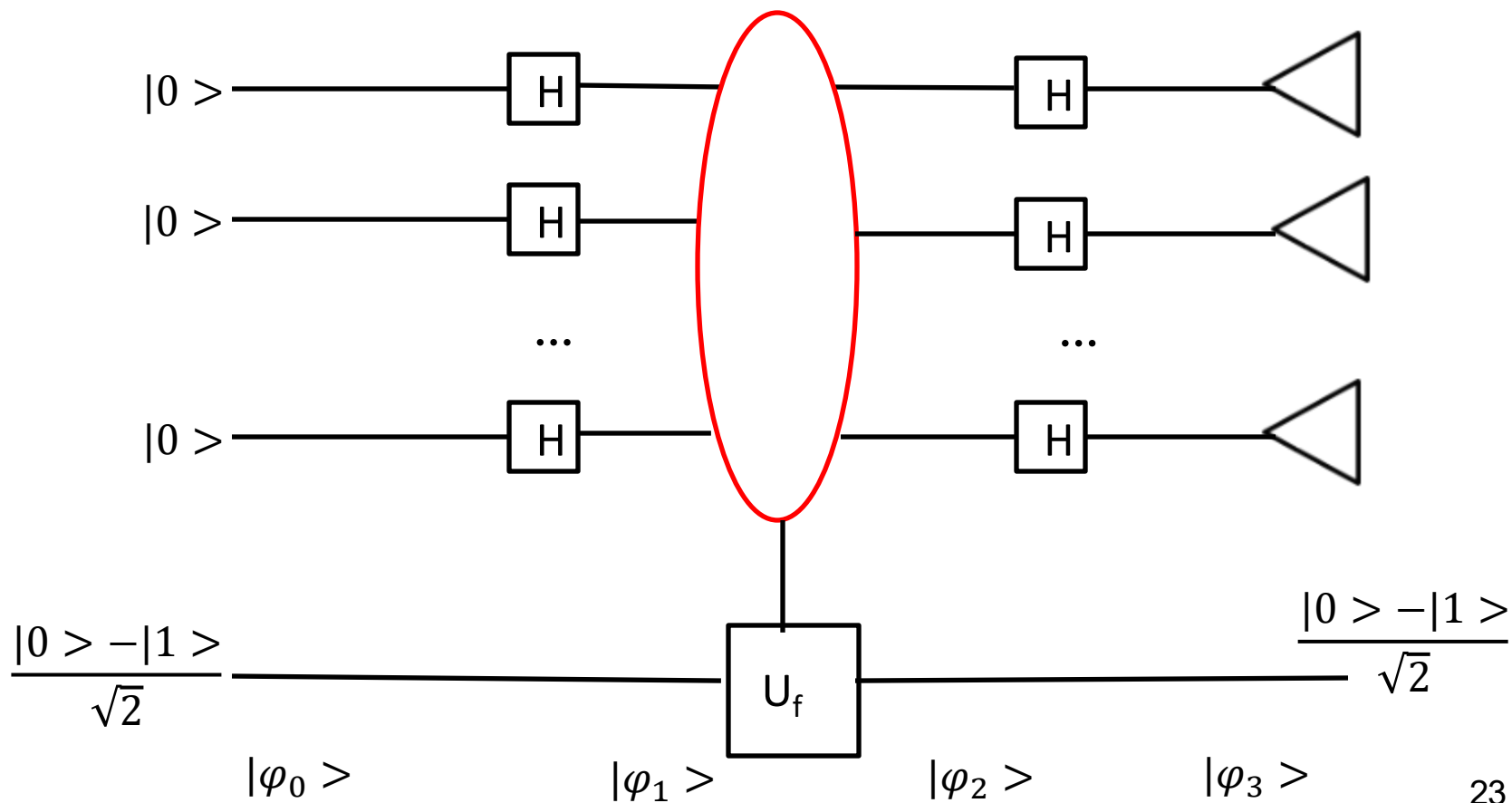
Deutsch

- Problem: Determine $f(0) + f(1)$ in one measurement
- $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$
- If $f(0) + f(1) = 1$, $|\psi_3\rangle = (-1)^{f(0)} |1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- If $f(0) + f(1) = 0$, $|\psi_3\rangle = (-1)^{f(0)} |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$



Deutsch-Josza

- Problem: $f: \{0,1\}^n \rightarrow \{0,1\}$, which is either constant or balanced.
- Which is it?
- Put $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, x is an n -bit quantity



DJ

- $|\varphi_0\rangle = |0\rangle^{\otimes n} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\varphi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\varphi_3\rangle = \frac{1}{2^n} \sum_{\mathbf{x}} \sum_{\mathbf{z}} |(-1)^{f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{z}} \mathbf{z}\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Simon

- $f: \{0,1\}^n \rightarrow X, \exists \vec{s} = s_1, s_2, \dots, s_n: f(x) = f(y)$ iff $x = y$ or $x = y + \vec{s}$
- $U_f: |x\rangle |b\rangle = |x\rangle |b \oplus f(x)\rangle$
- $H^{\otimes n}(|x\rangle) = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle$

1. $i = 1$
2. Prepare $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0\rangle$
3. Apply U_f to get $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$
4. Measure second bit
5. Apply $H^{\otimes n}$ to first register
6. Measure first register to get w_i
7. If $\text{din}(w_i) \neq n - 1$, go to 2
8. Output s : $w^t s^t = 0$

Phase kick back

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

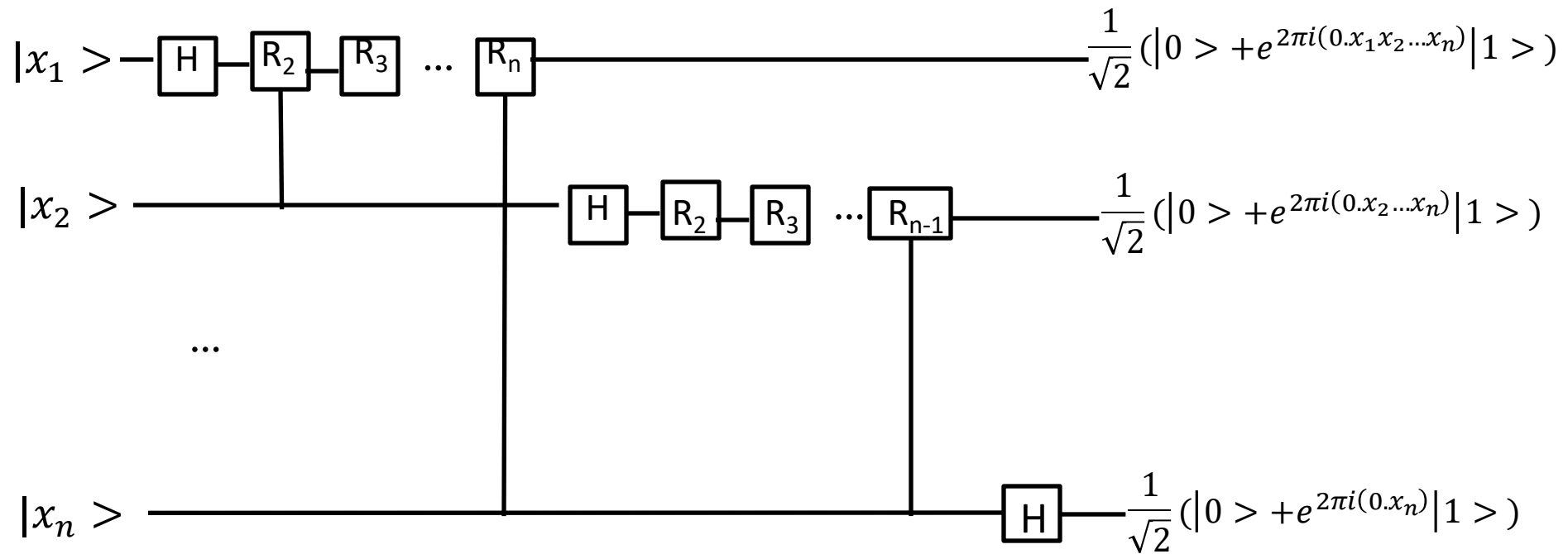
Phase Estimation

- Phase estimation problem: Given $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_y e^{2\pi i \omega y} |y\rangle$, estimate ω
- Theorem: $\frac{x}{2^n} \leq \omega \leq \frac{x+1}{2^n}$ with probability $\geq \frac{8}{\pi^2}$
- $e^{2\pi i 2^k \cdot x_1 x_2 \dots} = e^{2\pi i (x_{k+1} x_{k+2} \dots)}$
- Suppose $\omega = .x_1$, $|\psi\rangle = \frac{1}{\sqrt{2}} \sum_{|y\rangle} e^{2\pi i \omega |y\rangle} = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_1} |1\rangle)$ and $H(|\psi\rangle) = |x_1\rangle$
- In general, $H^{\otimes n}(|\mathbf{x}\rangle) = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y}} (-1)^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{y}\rangle$ and $H^{\otimes n}(H^{\otimes n}(|\mathbf{x}\rangle)) = |\mathbf{x}\rangle$
- So, $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{|y\rangle} e^{2\pi i \omega y} |y\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 2^{n-1} \omega} |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 2^{n-2} \omega} |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i \omega} |1\rangle)$
- Denote $R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-n}} \end{pmatrix}$

Quantum Fourier Transform

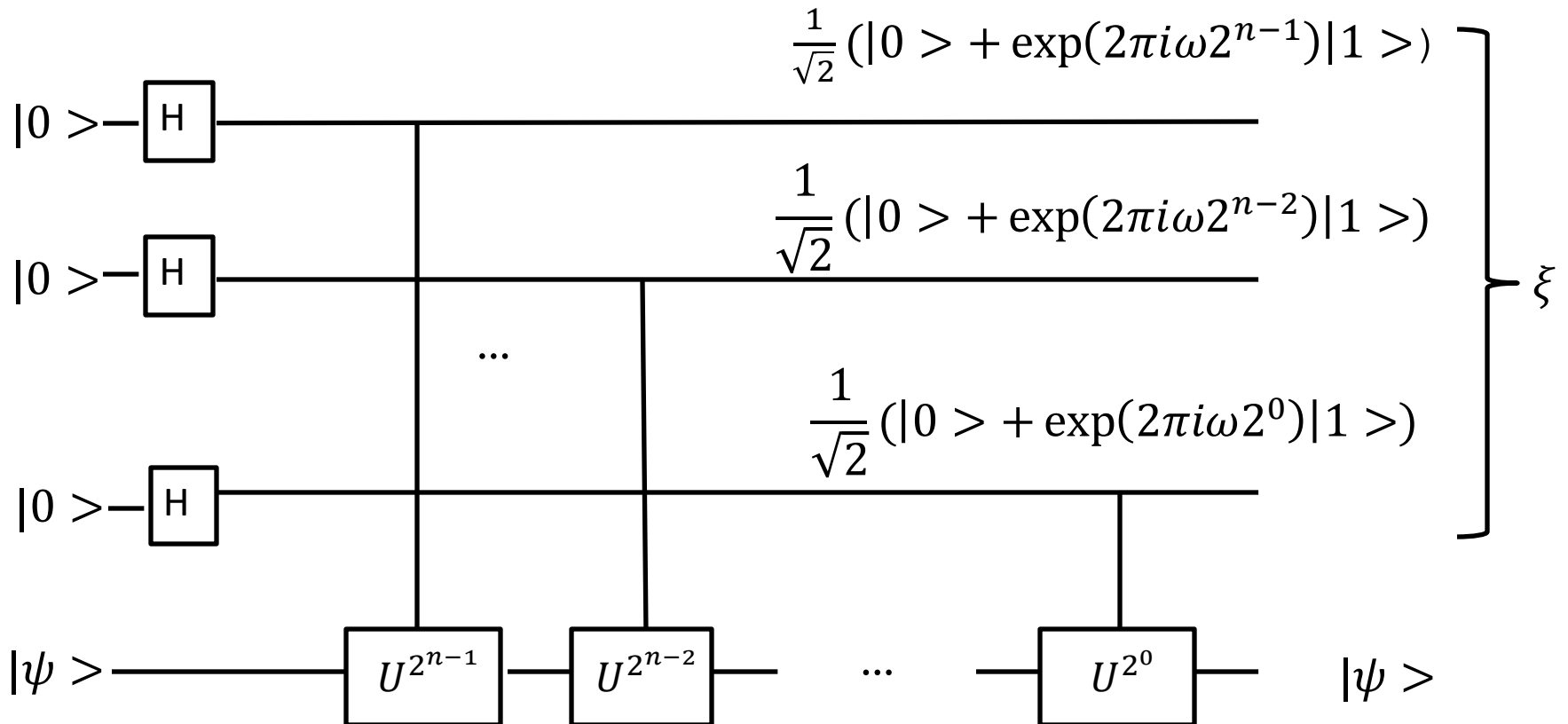
- $H^{\otimes n}(|\mathbf{x}\rangle) = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y}} (-1)^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{y}\rangle$
- $H^{\otimes n}(H^{\otimes n}(|\mathbf{x}\rangle)) = |\mathbf{x}\rangle$
- $QFT_m(|x\rangle) = \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} e^{2\pi i/m(x \cdot y)} |y\rangle$
- $QFT_m^{-1}(|x\rangle) = \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} e^{-2\pi i/m(x \cdot y)} |y\rangle$

Quantum Fourier Circuit



Eigenvalue Estimation

- Suppose $|\psi\rangle$ is an eigenstate of a unitary operator, U , so $U|\psi\rangle = \exp(2\pi i\phi)|\psi\rangle$. $|\phi\rangle = .x_1x_2 \dots x_n$ (a binary expansion)



Eigenvalue Estimation

- $U|\psi\rangle = \exp(2\pi i\phi) |\psi\rangle$, so $U^{2^j}|\psi\rangle = \exp(2\pi i\phi 2^j) |\psi\rangle$.
- Applying QFT_n^{-1} to ξ , gives $\langle x_n, x_{n-1}, \dots, x_1 \rangle$, where $|\phi\rangle = .x_1x_2 \dots x_n$
- Measure χ to get ϕ
- $\frac{y}{2^n}$ is a good estimate for $\phi = \frac{j}{r}$

Factorization using order finding (Shor)

- Suppose $N = pq$ and $a^r = 1 \pmod{N}$ then $r = 0 \pmod{\phi(pq)}$
- If r is even, say, $r = 2s$, $(a^s + 1)(a^s - 1) = 0 \pmod{pq}$.
- There is a good chance $p|(a^s - 1)$ but $(q, (a^s - 1)) = 1$.
- Then $((a^s - 1), N) = p$. Voila!
- Note that $|v_t\rangle = \frac{1}{r} \sum_{k=0}^{r-1} \exp(-\frac{2\pi i k t}{r}) |k \pmod{N}\rangle$ is an eigenvalue of $U_x(k) = |xk \pmod{N}\rangle$.
- In Shor, $|1\rangle = \frac{1}{\sqrt{r}} \sum |v_t\rangle$.
- Applying QFT^{-1} to control gives phase of eigenvalues
- Measurement of target gives $|\frac{s}{r}\rangle$ with $\Pr(|y\rangle) = \frac{1}{2^{2n}} \left| \frac{1-r^{2^n}}{1-r} \right|^2$, where $r = \exp(-2\pi i(\frac{y}{2^n} - \phi))$

Order Finding

Problem: Given $a, N \in \mathbb{Z}$ with $(a, N) = 1$, find r : $a^r \pmod{N} = 1$

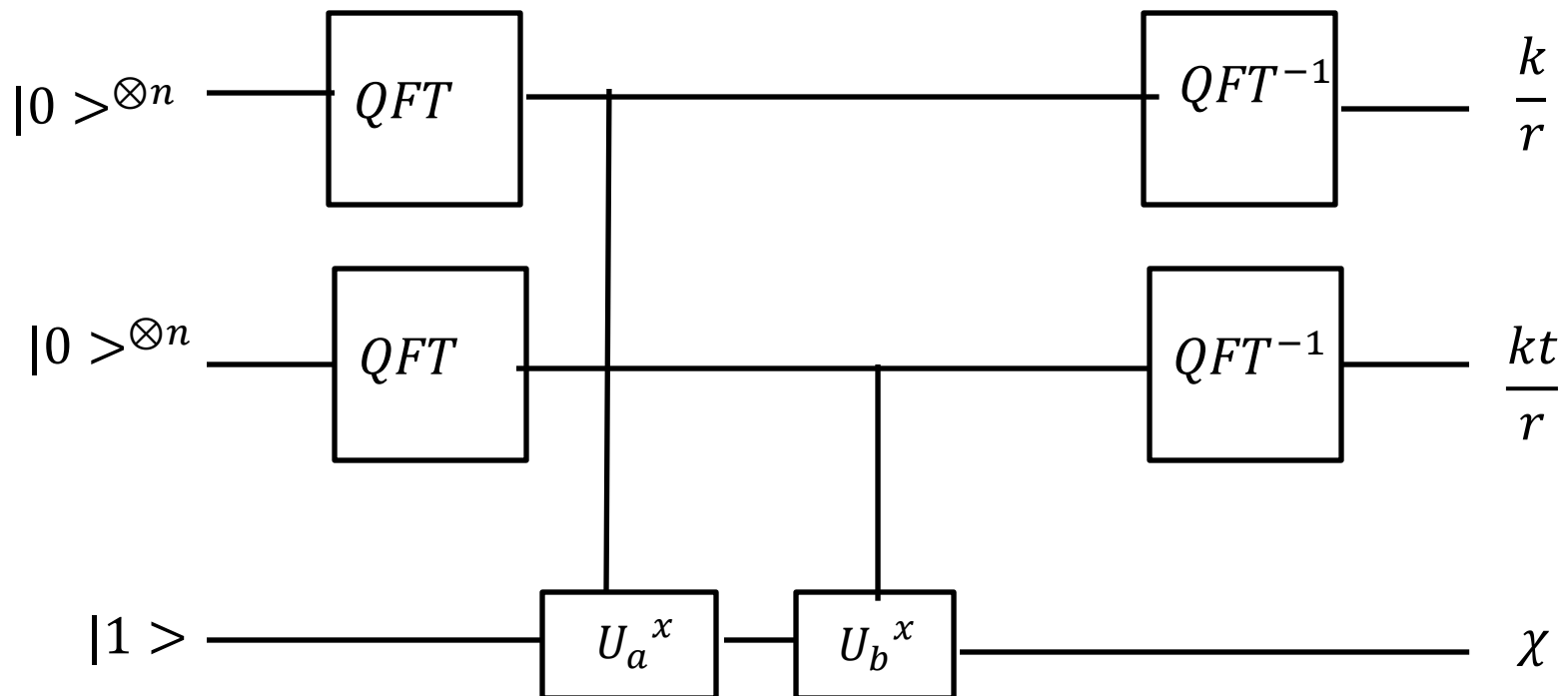
1. Choose n : $2^n \geq 2r^2$
2. Initialize control register $|000 \dots 0\rangle = |0\rangle^{\otimes 2n}$
3. Initialize target register to $= |000 \dots 01\rangle = |000 \dots 0\rangle = |0\rangle^{\otimes 2n} \otimes |1\rangle$
4. Apply QFT to control register
5. Apply $c - U_a^x$ to control and target register
6. Apply QFT^{-1} to control register
7. Measure CR to get estimate of $\frac{x_1}{2^n}$ of multiple of $\frac{1}{r}$
8. Use continued fraction to get c_1, r_1 : $\left| \frac{x_1}{2^n} - \frac{c_1}{r_1} \right| \leq 2^{-(n-1)/2}$
9. Repeat 1-8 to get c_2, r_2 : $\left| \frac{x_2}{2^n} - \frac{c_2}{r_2} \right| \leq 2^{-(n-1)/2}$, if none, FAIL
10. Compute $r = LCM(r_1, r_2)$ and $a^r \pmod{N}$
11. If $a^r \pmod{N} = 1$, output r , otherwise FAIL

Order Finding

- Order finding has quantum complexity $O(\lg(N)^2 \lg(\lg(N)) \lg(\lg(\lg(N)))$
- Classical complexity is $\exp(O(\sqrt{\lg(N) \lg(\lg(N))}))$

Discrete log

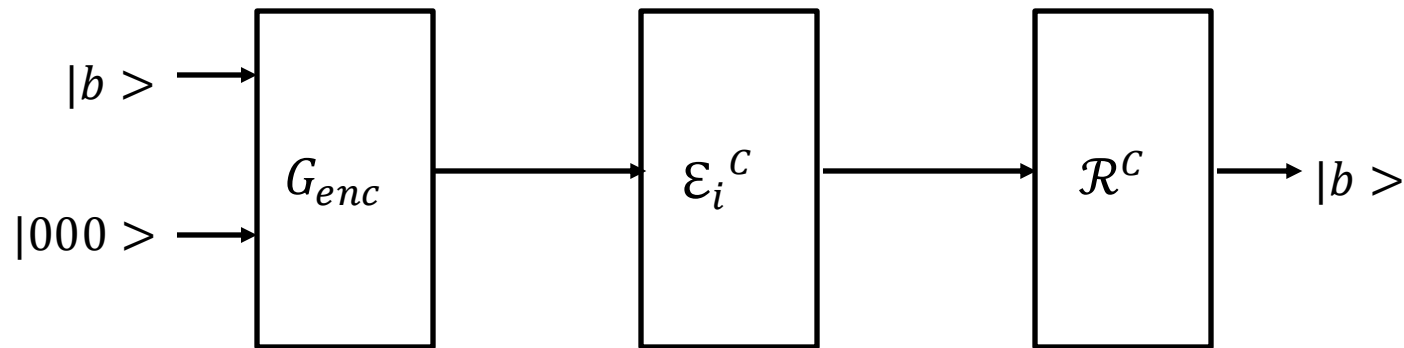
- Suppose $a = b^x \pmod{p}$, b has known order. We want $r: b^r = 1 \pmod{p}$
- Put $U_a(|x\rangle) = |ax \pmod{p}\rangle$ and $U_b(|x\rangle) = |bx \pmod{p}\rangle$.
- Consider the circuit below. $|1\rangle = \frac{1}{\sqrt{r}} \sum |v_t\rangle$. Below, $t = xy^{-1}$



Discrete log

- Measuring first control register gives $|\frac{k}{r}\rangle$
- Measuring first control register gives $|\frac{kt}{r}\rangle$
- Quantum complexity is $O(\lg(p)^2 \lg(\lg(p)) \lg(\lg(\lg(p))))$
- Best known classical requires $\exp(O(\sqrt{\lg(p)} \lg(\lg(p))))$

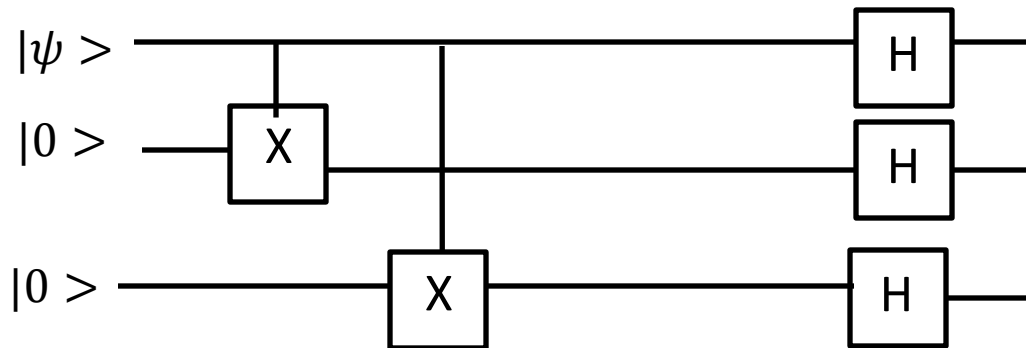
Error Correction



- Unlike classical error correction, the no cloning theorem restricts codes
- $|0\rangle|E\rangle \rightarrow \beta_1|0\rangle|E_1\rangle + \beta_2|1\rangle|E_2\rangle$
- $|1\rangle|E\rangle \rightarrow \beta_3|0\rangle|E_3\rangle + \beta_4|1\rangle|E_4\rangle$
- $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \rightarrow \alpha_0\beta_1|0\rangle|E_1\rangle + \alpha_0\beta_2|1\rangle|E_2\rangle + \alpha_1\beta_3|0\rangle|E_3\rangle + \alpha_1\beta_4|1\rangle|E_4\rangle$
- $|\psi\rangle = \frac{1}{2}|\psi\rangle(\beta_1|E_1\rangle + \beta_3|E_3\rangle) + \frac{1}{2}\langle Z|\psi\rangle(\beta_1|E_1\rangle - \beta_3|E_3\rangle) + \frac{1}{2}\langle X|\psi\rangle(\beta_2|E_2\rangle + \beta_4|E_4\rangle) + \frac{1}{2}\langle XZ|\psi\rangle(\beta_2|E_2\rangle - \beta_4|E_4\rangle)$

Error Correction

- $\rho = U_{err}|\psi\rangle\langle\psi|U_{err}^\dagger$
- $|\psi_{enc}\rangle = U_{enc}|\psi\rangle|000\dots\rangle$
- $\mathcal{E}_0 = I \otimes I \otimes I, \mathcal{E}_1 = X \otimes I \otimes I$
- $\mathcal{E}_2 = I \otimes X \otimes I, \mathcal{E}_3 = I \otimes I \otimes X$
- $\rho: |\psi\rangle\langle\psi| \rightarrow (1-p)|\psi\rangle\langle\psi| + p X|\psi\rangle\langle\psi|X$
- $\frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) \rightarrow \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \neq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes^3$
- 3-bit code, Shor 9-bit code



Amplitude Amplification

- $|\psi\rangle = A |00\dots 0\rangle = \sum_x \alpha_x |x\rangle |junk(x)\rangle$
- $|\psi\rangle = \sum_{x,good} \alpha_x |x\rangle |junk(x)\rangle + \sum_{x,bad} \alpha_x |x\rangle |junk(x)\rangle$
- $|\psi_{good}\rangle = \sum_{x,good} \alpha_x |x\rangle |junk(x)\rangle$
- $|\psi_{bad}\rangle = \sum_{x,bad} \alpha_x |x\rangle |junk(x)\rangle$
- $|\psi\rangle = \sqrt{p_{good}} |\psi_{good}\rangle + \sqrt{p_{bad}} |\psi_{bad}\rangle = \sin(\theta) |\psi_{good}\rangle + \cos(\theta) |\psi_{bad}\rangle$
- $p_{good} = \sin(\theta)^2$

Grover

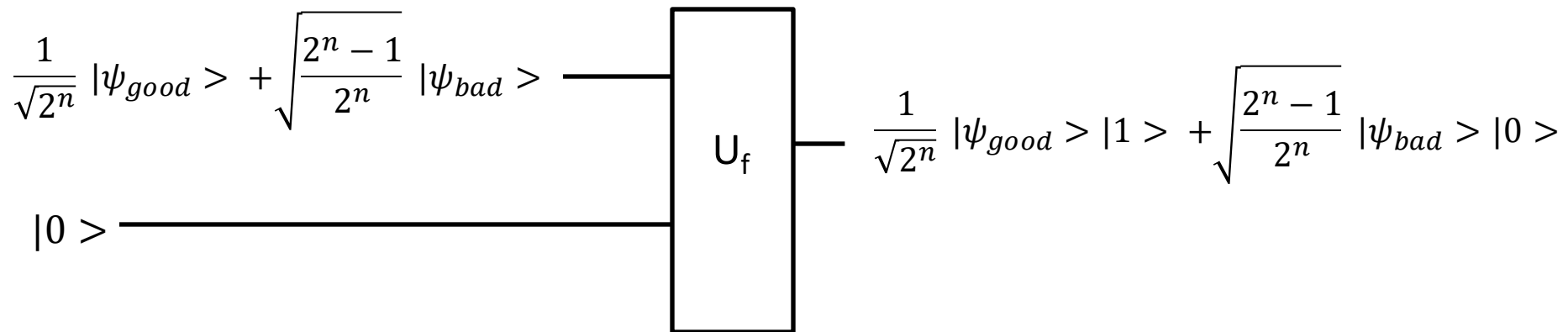
Search

Input: $U_f: f: \{0,1\}^n \rightarrow \{0,1\}$

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

$$|\psi_{good}\rangle = \mathbf{w}$$

$$|\psi_{bad}\rangle = \frac{1}{\sqrt{N-1}} \sum_{\mathbf{x} \neq \mathbf{w}} |\mathbf{x}\rangle$$



Grover

1. Initialize n -qubits $|0000 \dots 0\rangle$.
2. Apply $H^{\otimes n}$ to get $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$
3. Apply Grover G $\frac{\pi}{4\sqrt{n}}$ times
4. Measure output

Algorithm G

1. Apply U_f
2. Apply $H^{\otimes n}$
3. Apply U_{0^\perp}
4. Apply $H^{\otimes n}$

Search

Input: $U_f: f: \{0,1\}^n \rightarrow \{0,1\}$

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

$$|\psi_{good}\rangle = |\mathbf{w}\rangle$$

$$|\psi_{bad}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$$

Algorithm U_{0^\perp}

$$U_{0^\perp}: |x\rangle \rightarrow -|x\rangle, x \neq 0$$

$$U_{0^\perp}: |0\rangle \rightarrow 0|x\rangle$$

End

Strings and thermo

- String: $dU = \frac{1}{2} \mu \omega^2 y^2 dx$, $P(t) = Z = F \frac{\partial \psi}{\partial t}$, $v_\phi = \frac{\omega}{k}$, $Z = \frac{T}{v_\phi}$, $\frac{T}{\mu} = \omega^2$
- $I = I_0 \left(\frac{\sin(\beta/2)}{\beta/2} \right)^2$, $P_R = \frac{P_T G_R G_T \lambda^2}{(4\pi R)^2}$
- $Z = \sum_i e^{-\beta E_i}$, $\beta = \frac{1}{kT}$, $\langle E \rangle = \frac{\partial(\ln(Z))}{\partial \beta}$
- $\Delta Q + \Delta W = \Delta E$, ΔQ – heat in system, ΔW - work on system
- $W = Q(1 - \frac{T}{T_0})$, $e = (1 - \frac{T_C}{T_H})$, $S = k \ln(\Omega) \Omega$
- $c_v = \frac{3}{2} R$
- $I(\lambda) = \frac{2\pi h c^2}{\lambda^5 (\exp(\frac{hc}{k\lambda T}) - 1)}$

EM

- $E_n = \frac{-13.6}{n^2}, a_0 = \epsilon_0 \frac{h^2}{\pi m e^2}, d_n = \frac{(2m)^{3/2} V E^{3/2}}{3\pi h^3}, g(E) = \frac{(2m)^{3/2} V}{2\pi h^2} \sqrt{E}$
- $\nabla \cdot j = -\frac{\partial \rho}{\partial t}, \nabla \cdot E = \frac{\rho}{\epsilon_0}, \nabla \times E = -\frac{\partial B}{\partial t}, \nabla \times B = 0, c^2 \nabla \times B = \frac{j}{\epsilon_0} + \frac{\partial E}{\partial t}$
- $c^2 = \frac{1}{\epsilon_0 \mu_0}, I = \sigma T^4, D = \epsilon E, B = \mu H$
- Solution to $\nabla^2 \psi - \frac{1}{c^2} \frac{\partial^2 \psi}{\partial t^2} = -s, \psi(t) = \frac{1}{4\pi} \frac{S(t-\frac{r}{c})}{r}, S(t) = \int s(t) dV$
- $\phi(1, t) = \int \frac{\rho(2, t-\frac{r}{c})}{4\pi \epsilon_0 r_{12}} dV, A(1, t) = \int \frac{\rho(2, t-\frac{r}{c})}{4\pi c^2 \epsilon_0 r_{12}} dV$
- $\nabla \phi = E + \frac{\partial A}{\partial t}, S = \epsilon_0 c^2 E \times B$
- Oscillating dipole: $\psi = \frac{dz}{4\pi \epsilon_0} \left[\frac{q(t-\frac{r}{c})}{r^3} + \frac{I(t-\frac{r}{c})}{r^2 c} \right]$
- $x' = \gamma(c - ut), t' = \gamma(t - \frac{ux}{c^2}), E^2 + (pc)^2 = (m_0 c^2)^2$

Susskind

- $|\psi\rangle = \sum_i \alpha_i |\lambda_i\rangle$ is the state of a system, the $|\lambda_i\rangle$ is a complete set of orthonormal vectors which are eigenvectors
- $\langle L \rangle = \sum_i P(\lambda_i) \lambda_i$ is the expected value
- $\langle L \rangle = \langle \psi | L | \psi \rangle = \sum_i \bar{\alpha}_i \alpha_i \langle \lambda_i | \lambda_i \rangle, \alpha_i \in \mathbb{C}$
- If φ, ψ are states in a continuous variable, $\langle \varphi | \psi \rangle = \int_{-\infty}^{\infty} \bar{\varphi} \psi dx$
- $I = \sum_i |i\rangle \langle i|, \text{Tr}(L) = \sum_i \langle i | L | i \rangle, I = \int |x\rangle \langle x| dx$
- If $|\psi\rangle = \sum_i \alpha_i |i\rangle, \langle j | \psi \rangle = \sum_i \alpha_i \langle j | i \rangle$
- C-S: $|\vec{x}| |\vec{y}| \geq |\vec{x} \cdot \vec{y}|$, Triangle: $|\vec{x}| + |\vec{y}| \geq |\vec{x} + \vec{y}|$
- Eigenvectors of a Hermitian operator are a complete set
- Eigenvectors with different eigenvalues are orthogonal.

Susskind

- Observables: $M|\lambda\rangle = \lambda|\lambda\rangle$, λ is the observed value, M is projective and Hermitian
- The rules
 1. Observables are represented by linear operators. States are vectors
 2. Results of measurements are eigenvalues
 3. Distinguishable states correspond to orthogonal eigenvalues
 4. If $|\psi\rangle$ is a state and L is an observable,
 $P(\lambda_i) = \langle \psi | \lambda_i \rangle \langle \lambda_i | \psi \rangle$
 5. Evolution of states governed by a unitary operator

Spin

- Spin field: $H = \sigma \cdot B$
 - $\langle \dot{\sigma}_z \rangle = \frac{i\omega}{2} \langle [\sigma_z, \sigma_z] \rangle, \langle \dot{\sigma}_y \rangle = -\omega \langle \sigma_x \rangle$
- $\langle \dot{\sigma}_x \rangle = \frac{-i}{\hbar} \langle [\sigma_x, H] \rangle, \langle \dot{\sigma}_y \rangle = \frac{-i}{\hbar} \langle [\sigma_y, H] \rangle, \langle \dot{\sigma}_z \rangle = \frac{-i}{\hbar} \langle [\sigma_z, H] \rangle$
- $|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |d\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $|r\rangle = \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle), |l\rangle = \frac{1}{\sqrt{2}}(|u\rangle - |d\rangle)$
- $|i\rangle = \frac{1}{\sqrt{2}}(|u\rangle + i|d\rangle), |o\rangle = \frac{1}{\sqrt{2}}(|u\rangle - i|d\rangle)$
- Pauli matrices: $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
- $\sigma_n = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$
- $\lambda_1 = 1, |\lambda_1\rangle = \begin{pmatrix} \cos(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) \end{pmatrix}, \lambda_2 = -1, |\lambda_2\rangle = \begin{pmatrix} -\sin(\frac{\theta}{2}) \\ \cos(\frac{\theta}{2}) \end{pmatrix}$

Entanglement

- Composite: $|\varphi\rangle \in H^A$, $|\psi\rangle \in H^B$, $\varphi \otimes \psi \in H^{AB}$
- $L|\lambda_i, \mu_i\rangle = \lambda_i|\lambda_i, \mu_i\rangle$, $M|\lambda_i, \mu_i\rangle = \mu_i|\lambda_i, \mu_i\rangle$ for independent action
- If A state coefficients are a and B state coefficients are B ,
- $|\varphi \otimes \psi\rangle = \sum_{a,b} |\varphi(a)\rangle \otimes |\psi(b)\rangle = |ab\rangle$
- Alice and Bob spins: $(\alpha_u|u\rangle + \alpha_d|d\rangle) \otimes (\beta_u|u\rangle + \beta_d|d\rangle)$ as product state
- General entangled: $\psi_{uu}|uu\rangle + \psi_{ud}|ud\rangle + \psi_{du}|du\rangle + \psi_{dd}|dd\rangle$
- Entangled: $|sing\rangle = \frac{1}{\sqrt{2}}(|ud\rangle - |du\rangle)$,
- $\langle sing|\sigma_z|sing\rangle = 0$

Susskind and density

- $\tau_z \sigma_z |sing\rangle = -|sing\rangle, \tau_x \sigma_x |sing\rangle = -|sing\rangle$
- $\langle L \rangle = Tr(\rho L)$ for states prepared with probability p_i
- If $\langle L \rangle = p_\psi \langle \psi | L | \psi \rangle + p_\phi \langle \phi | L | \phi \rangle$, density operator is
- $P = p_\psi |\psi\rangle \langle \psi| + p_\phi |\phi\rangle \langle \phi|$
- $P_{a,a'} = \overline{\psi(a)} \psi(a') \sum_b \overline{\phi(b)} \phi(b)$
- $\langle \psi | L | \psi \rangle = \sum_{a,a',b,b'} \bar{\psi}_{a',b'} L_{a',a} \psi_{a,b}$

Uncertainty, Evolution and Schrodinger

- Uncertainty: From triangle, $(\Delta X)(\Delta Y) \geq \frac{1}{2} | \langle \psi | [A, B] | \psi \rangle |$
- Unitary evolution: $U^\dagger(t)U(t) = I, |\psi(t)\rangle = U(t)|\psi(0)\rangle$
- $U(\epsilon) = (I + \frac{i}{\hbar}\epsilon H)|\psi(0)\rangle$, so
- $\frac{|\psi(\epsilon)\rangle - |\psi(0)\rangle}{\epsilon} = -\frac{i}{\hbar}H|\psi(0)\rangle$, or, $\frac{\partial |\psi(t)\rangle}{\partial t} = -\frac{i}{\hbar}H|\psi(t)\rangle$
- $\frac{d}{dt} \langle \psi | L | \psi \rangle = \langle \dot{\psi} | L | \psi \rangle + \langle \psi | L | \dot{\psi} \rangle =$
 $\frac{i}{\hbar} (\langle \psi | HL | \psi \rangle - \langle \psi | LH | \psi \rangle) = \frac{i}{\hbar} \langle \psi | [H, L] | \psi \rangle$
- This gives conservation of energy since $[H, H] = 0$
- Example: $H = \frac{\hbar\omega}{2} \sigma \cdot n$

Momentum space and Fourier

- $P|\psi\rangle = p|\psi\rangle$ is equivalent to $P = -i\hbar \frac{\partial}{\partial x}$
- Eigenvectors are solutions of $-i\hbar \frac{\partial \psi}{\partial x} = p\psi$, $\psi_p(x) = A \exp(i \frac{px}{\hbar})$
- Wavelength of $A \exp(i \frac{px}{\hbar})$ is $\lambda = \frac{2\pi\hbar}{p}$
- $P(p) = |\langle P|\psi\rangle|^2$, put $\tilde{\psi}(p) = \langle P|\psi\rangle$
- $\tilde{\psi}(p) = \int dx \langle p|x\rangle \langle x|\psi\rangle$ but $\psi(x) = \langle x|\psi\rangle$ and
- $\langle p|x\rangle = \frac{1}{\sqrt{2\pi}} \exp(-i \frac{px}{\hbar})$
- Similarly, $\psi(x) = \langle x|\psi\rangle = \int dp \langle x|p\rangle \langle p|\psi\rangle$ and
- $\psi(x) = \frac{1}{\sqrt{2\pi}} \int dp \exp(i \frac{px}{\hbar}) \tilde{\psi}(p)$
- $\psi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp(i \frac{px}{\hbar}) \tilde{\psi}(p) dp$,
- $\tilde{\psi}(p) = \frac{1}{\sqrt{2\pi}} \int \exp\left(-i \frac{px}{\hbar}\right) \psi(x) dx$

Susskind

- $\psi(x, t) = A \exp \left(i \frac{px - \frac{p^2 t}{2m}}{\hbar} \right)$ is a complete set of solutions
- $\psi(x, t) = \int dp \tilde{\psi}(p) \exp \left(i \frac{px - \frac{p^2 t}{2m}}{\hbar} \right)$
- Dynamics:
- $X|\psi\rangle = x|\psi\rangle, P|\psi\rangle = i\hbar \frac{\partial}{\partial x} |\psi\rangle$
- $V|\psi\rangle \rightarrow V(x)\psi(x)$, get $E\psi = -\frac{\hbar^2}{2m} \frac{\partial^2 \psi}{\partial x^2} + V(X)\psi$
- $\langle v \rangle = \frac{d}{dt} \langle \psi | X | \psi \rangle,$
- $\frac{d}{dt} \langle P \rangle = \frac{i}{\hbar} [V, P] = -\langle \frac{\partial V}{\partial x} \rangle,$
- $[V, P] = i\hbar \frac{dV}{dx}$

Standard solution

- Standard method:
 1. Get H
 2. Prepare $|\psi(0)\rangle$
 3. Find $H|E_j\rangle = E_j|E_j\rangle$
 4. $\alpha_j(0) = \langle E_j|\psi(0)\rangle$, $\alpha_j(t) = \alpha_j(0)\exp(-i\frac{E_j t}{\hbar})$
 5. $|\psi(t)\rangle = \sum_j \alpha_j(t) |E_j\rangle$
 6. $P_\lambda(t) = |\langle \lambda|\psi(t)\rangle|^2$
- Correlation and means
 - $\Delta A^2 = \sum_a (A - \bar{A})^2 P(a) = |\langle A^2|\psi\rangle|^2$
 - $(\Delta A)(\Delta B) \geq \frac{1}{2} |\langle \psi|[A, B]|\psi\rangle|^2$
 - $C(A, B) = \langle AB\rangle - \langle A\rangle\langle B\rangle$
 - $C(\sigma_x, \tau_x) = -1$

Harmonic Oscillator, etc

- $H = \frac{1}{2}\dot{X}^2 + \frac{1}{2}\omega^2 x^2 = \frac{P^2 + \omega^2 x^2}{2} = \frac{1}{2}(P + i\omega X)(P - i\omega X) - \omega^2[X, P]$
- Ground state: $\psi(x) = \exp(-\frac{\omega}{2\hbar}x^2)$, $E_0 = \frac{\omega\hbar}{2}$
- $a^- = \frac{i}{\sqrt{2\omega\hbar}}(P - i\omega X)$, $a^+ = \frac{-i}{\sqrt{2\omega\hbar}}(P + i\omega X)$
- $[a^-, a^+] = 1$. If $N = a^+ a^-$, $H = \omega\hbar(N + \frac{1}{2})$, $N|n\rangle = n|n\rangle$,
- $a^+|n\rangle = |n+1\rangle$
- Particle in box: $E_n = \frac{n^2\hbar^2}{8mL^2}$, $\psi_n = C\sin(\frac{n\pi x}{L})$

Hidden subgroup

- $S \leq G$, $f(x) = f(y)$ iff $x + S = y + S$