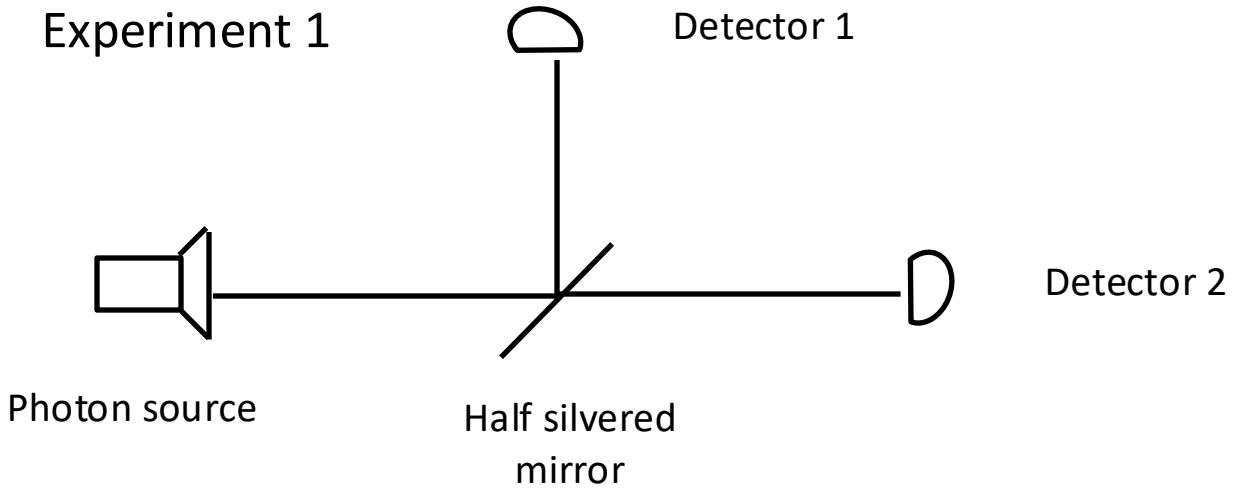
Quantum Computing

A brief introduction

John Manferdelli
JohnManferdelli@hotmail.com

Beam splitters and QM

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



Photon source emits stream of photons.

P(photon arrives at Detector 1)= .5

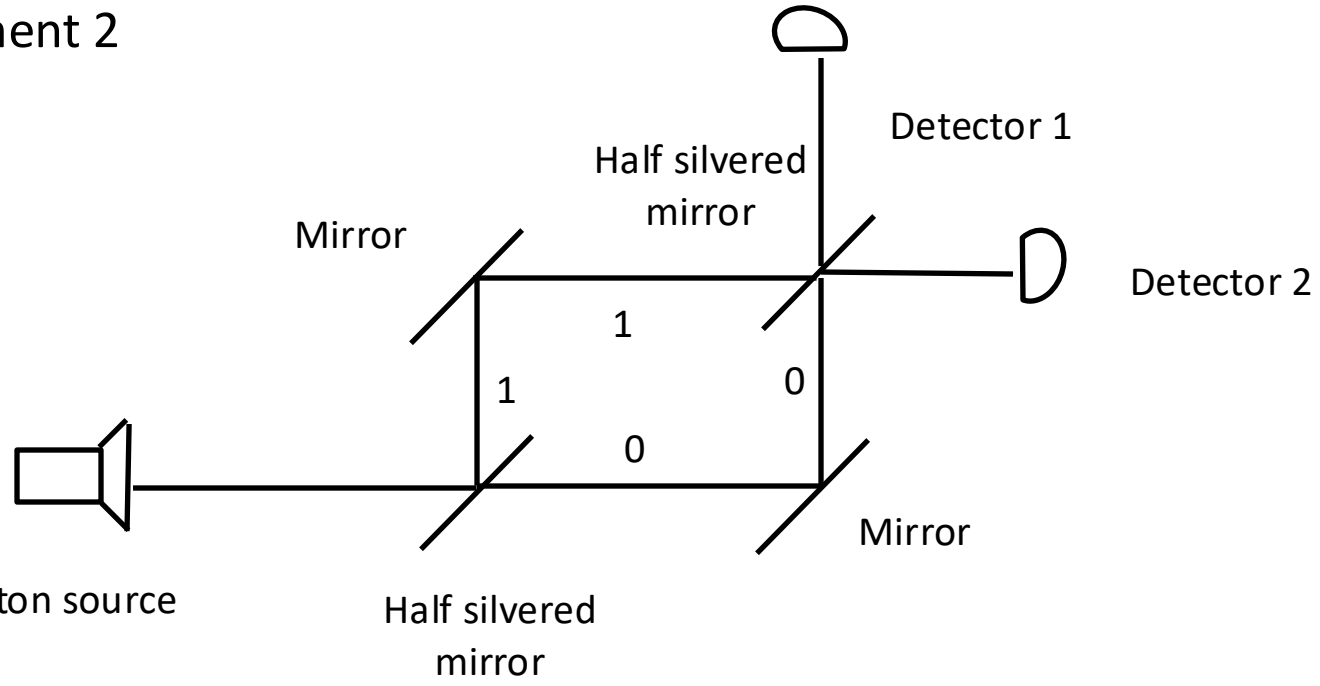
P(photon arrives at Detector 2)= .5

So far, so good

Beam splitters and QM

Mach-Zender Interferometer

Experiment 2



Photon source emits stream of photons.

P(photon arrives at Detector 1)= 0

P(photon arrives at Detector 2)= 1

Huh?

According to QM

Analysis

Beam splitter causes the photon to go into superposition:

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

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

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 $|\psi> = a|0> + b|1>$, $a\bar{a} + b\bar{b} = 1$
2. A system, with state, $|\psi(t)>$, evolves according to a unitary operator, namely, $U(|\psi(0)>)$
   - U is unitary if $(x, y) = (Ux, Uy)$. Note $U\overline{U^T} = I$
   - Example is a Hamiltonian: $H(t)|\psi(t)> = \mathrm{i}\hbar\frac{d|\psi(t)>|}{dt}$
   - $|\varphi(t_2)> = e^{-i\hbar H(t_2 - t_1)}|\varphi(t_1)>$
3. Each observable is represented by a Hermitian operator, $\hat{Q}$, the expectation value of $\hat{Q}$ is $<\psi|\hat{Q}\psi>$. 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 $|\psi>$

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, $|\psi_1>$ and $\mathcal{H}_2$ is in state, $|\psi_2>$, the joint state is $|\psi_1> \otimes |\psi_2>$
5. Given an orthonormal basis $\mathcal{B} = \{\varphi_i\}$, one can perform a von-Neuman measurement $\mathcal{H}_A$ on $|\psi> = \sum_i \alpha_i |\varphi_i>$ that outputs i with probability $|\alpha_i|^2$. It is projective. Further, if $|\psi> = \sum_i \alpha_i |\varphi_i> |\gamma_i> \; \mathcal{H}_A \otimes \mathcal{H}_B$ measurement yields i with probability $|\alpha_i|^2$ and leaves state in $|\varphi_i> |\gamma_i>$. $M = \sum m_i P_i = \sum m_i \, |i><i|$

Linear Algebra

- Dirac Notation: Element in Hilbert space of dimension 2^n is represented by n-entry symbol. $|000\ldots00> \leftrightarrow (1,0,\ldots,0)^T$, $|000\ldots01> \leftrightarrow (0,1,\ldots,0)^T$, …, $|111\ldots1> \leftrightarrow (0,0,\ldots,1)^T$ where column vectors have 2^n coordinates.
- Notation: $|0> \otimes |0> \otimes \ldots \otimes |0> = |000\ldots0>$
- 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: $(v_1, v_2, \ldots, v_n) \cdot (w_1, w_2, \ldots, w_n) = \sum_{i=0}^{n} \bar{v_i}\, w_i$
- Outer product: $(|\psi><\phi|)|\gamma> = |\psi>(<\phi|\gamma>)$
- Theorem: Every linear operator can be written as $T = T_{m,n}|b_m><b_n|$,
- $T_{m,n} = <b_m|T|b_n>$

Linear Algebra (continued)

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

$|\varphi_i> \otimes |\phi_i>$ is a basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$. $\binom{\alpha_0}{\alpha_1} \otimes \binom{\beta_0}{\beta_1} = (\alpha_0\beta_0, \alpha_0\beta_1, \alpha_1\beta_0, \alpha_1\beta_1)^T$.

$$A \otimes B = \begin{matrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{matrix}$$

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

$Tr(A) = < b_n|A|b_n >$

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

More notation

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

$$|v><w| = \begin{matrix} v_1\overline{w_1} & v_1\overline{w_2} & \dots & v_1\overline{w_n} \\ \dots & \dots & \dots & \dots \\ v_n\overline{w_1} & v_n\overline{w_2} & \dots & v_n\overline{w_n} \end{matrix}$$, so $I = \sum |\mathrm{i}><i|$ and $M = \sum M_{ij}|\mathrm{i}><j|$

- Pauli matricies
  - $\sigma_0 = I$, $\sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $\sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  - $[X, Y] = iZ, [Y, Z] = iX, [Z, X] = iY$
- $|+> = \frac{1}{\sqrt{2}}(|0> + |1>)$, $|-> = \frac{1}{\sqrt{2}}(|0> - |1>)$, $|i> = \frac{1}{\sqrt{2}}(|0> + i|1>)$, $|-i> = \frac{1}{\sqrt{2}}(|0> - i|1>)$

Mixed states and density

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

- $P(|0>) = <0|\psi><\psi|0> = Tr<0|\psi><\psi|0) = Tr(|0><0|\ |\psi><\psi|$

Mixed states and density

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

      $= \frac{1}{2} Tr(|0 >< 0| \otimes |0 >$

      $< 0|\ + |0 >< 1| \otimes |0 >< 1| + |1 >< 0| \otimes |1 >< 0|\ + |1 >< 1| \otimes |1 >< 1|)$

      $= \frac{1}{2}(|0 >< 0| + |1 >< 1|)$

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 on that for an input product state $|\alpha > |\beta >$, the output state is not a product state (e.g.-CNOT).
  - Example: $|\psi > = \frac{1}{\sqrt{2}}(|00> + |11>)$
- 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: $|\psi> = \cos\left(\frac{\theta}{2}\right)\left|0> + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right| 1>$
- Measurement: $I = \sum|i><i|,\ M = \sum m_i P_i$, M is Hermitian, $P_i = |i><i|$.
- Controlled gates:
  - $c-U|0>|\psi> = |0>|\psi>$
  - $c-U|1>|\psi> = |1> U|\psi>$

Common gates

- Pauli gates

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

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

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

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

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

- Hadamard

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

- 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

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

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

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

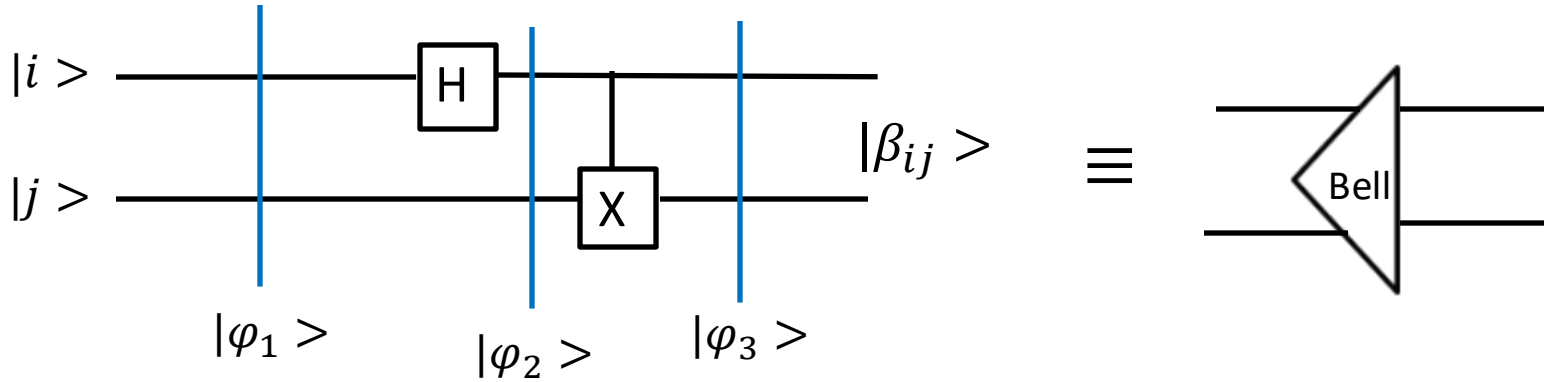
$$H^{\otimes n}(|0000 \ldots 0>) = \frac{1}{\sqrt{2}}(|0> + |1>) \otimes \frac{1}{\sqrt{2}}(|0> + |1>) \otimes \ldots \otimes \frac{1}{\sqrt{2}}(|0> + |1>)$$

Measurement in alternate basis

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

Converting to Bell Basis

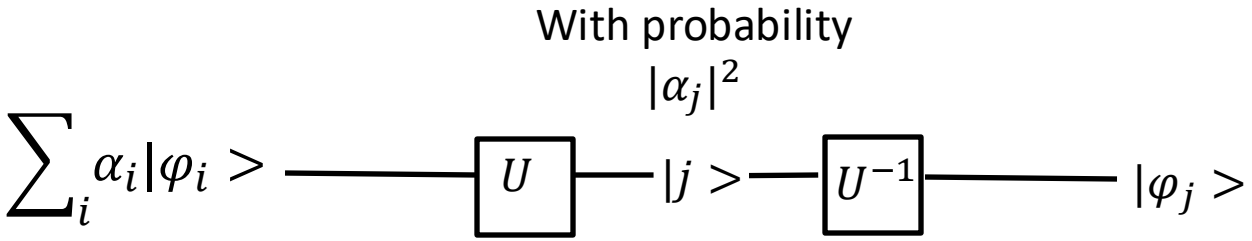
- Computational basis is $|i>$, $U|\varphi_j> = |j>$
- $|\beta_{00}> = \frac{1}{\sqrt{2}}(|00> + |11>)$, $|\beta_{01}> = \frac{1}{\sqrt{2}}(|01> + |10>)$
- $|\beta_{10}> = \frac{1}{\sqrt{2}}(|00> - |11>)$, $|\beta_{11}> = \frac{1}{\sqrt{2}}(|01> - |10>)$

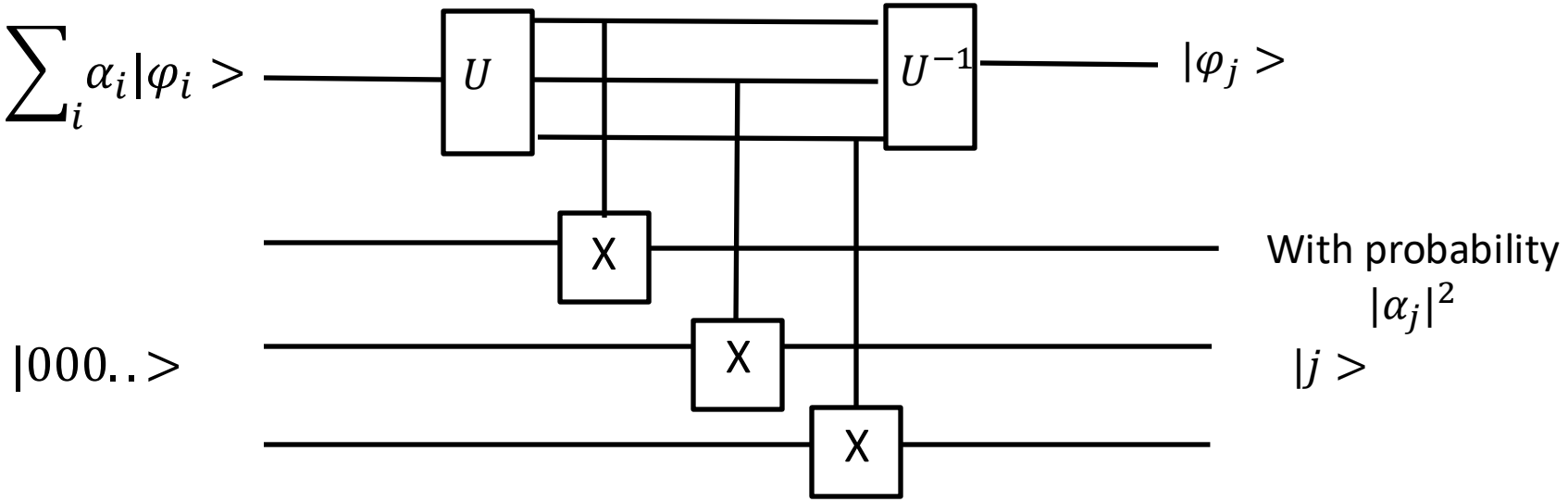


- $|\varphi_1> = |00>$
- $|\varphi_2> = \frac{1}{\sqrt{2}}(|0> + |1>)|0> = \frac{1}{\sqrt{2}}(|00> + |10>)|$
- $|\varphi_3> = |\beta_{00}>$

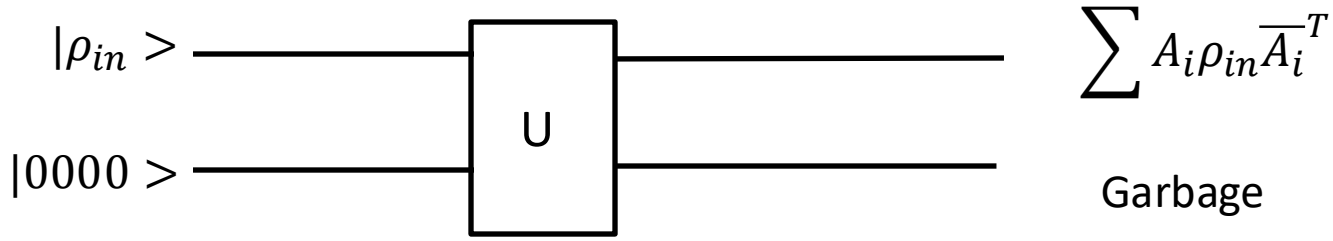
Changing Measurement Basis

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





Superoperator and mixed states



- $\rho = |\psi >< \psi|$, $U|\psi >$ has density $\rho = U|\psi >< \psi|\overline{U}^T > = U\rho U^\dagger$
- $< 0|\psi >< \psi|0 > = < 0|\rho|0 > = P(|0 >)$
- $\rho = \sum_i p_i |\psi_i >< \psi_i|$
- $Tr(A) = < b_n|A|b_n >$
- $\rho_{in} \to \rho_{out} = Tr_b(U(\rho_{in} \otimes |000 \ldots >< 000 \ldots 0|U^\dagger)$
- $\rho_{in} \to \sum A_i \rho_{in} {A_i}^\dagger$, where A_i are Kraus operators with $\sum {A_i}^\dagger A_i = I$

No Cloning Theorem

- Qubits can't be copied
- Proof

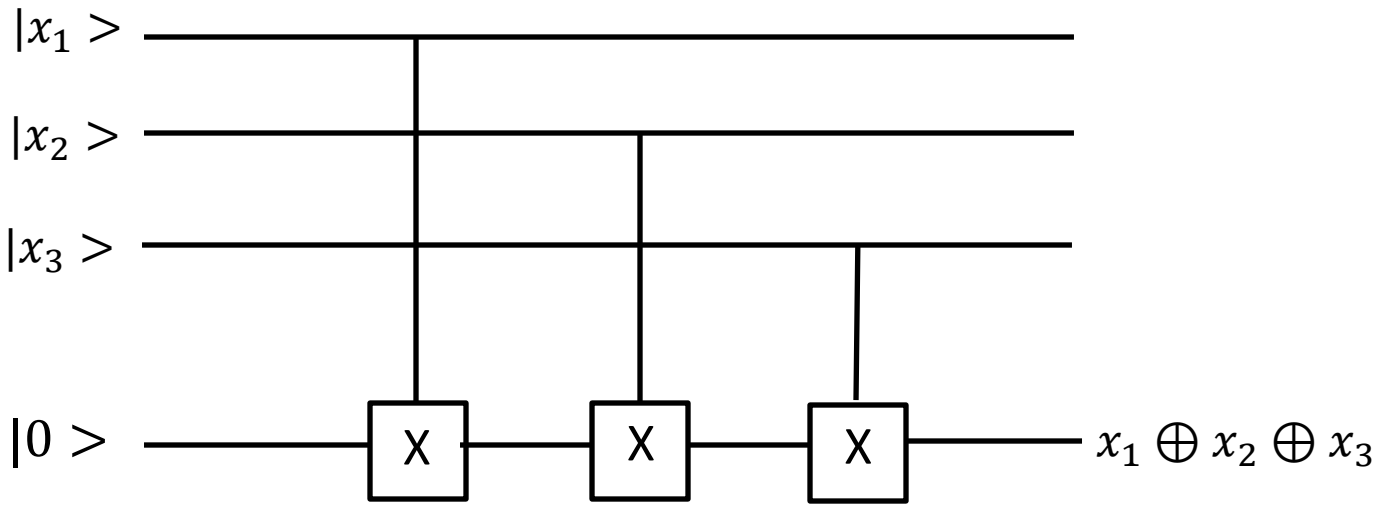
  Suppose they can be. Then there is an operator, U, such that for any state $|\varphi>$, $U(|\varphi>|0>) = |\varphi>|\varphi>$. Now let $|\psi>$ and $|\phi>$ be non-orthogonal, different pure states.

  $(|\psi>|0>, |\phi>|0>) = <\psi|\phi><0|0> = <\psi|\phi>$.

  Since U is unitary,

  $<\psi|\phi> = (|\psi>|0>, |\phi>|0>) = (U|\psi>|0>, U|\phi>|0>) = (|\psi>|\psi>, |\phi>|\phi>) = <\psi|\phi>^2$. So, $<\psi|\phi> = 1$. This is a contradiction.
- No checkpointing

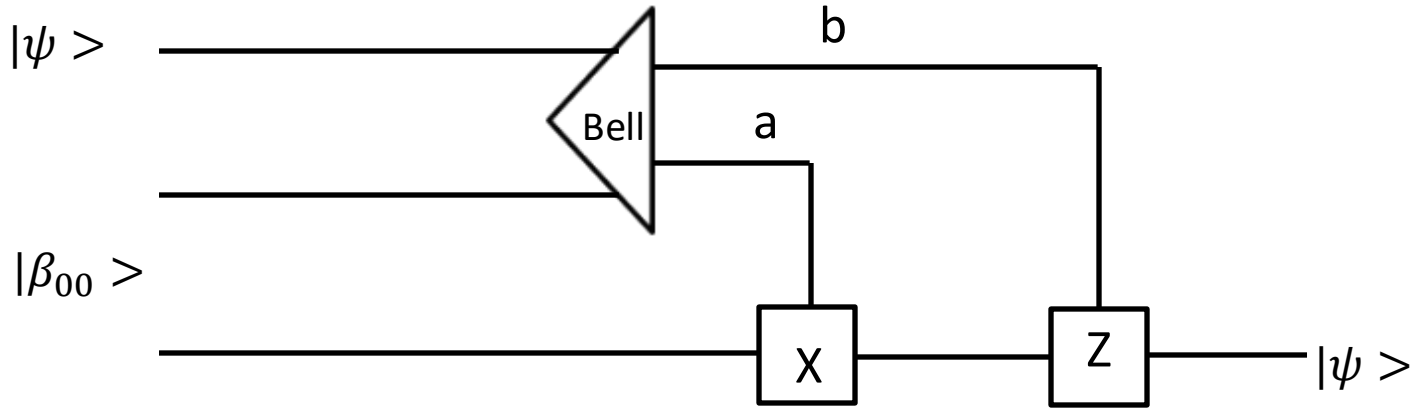
Parity Circuit



Superdense coding

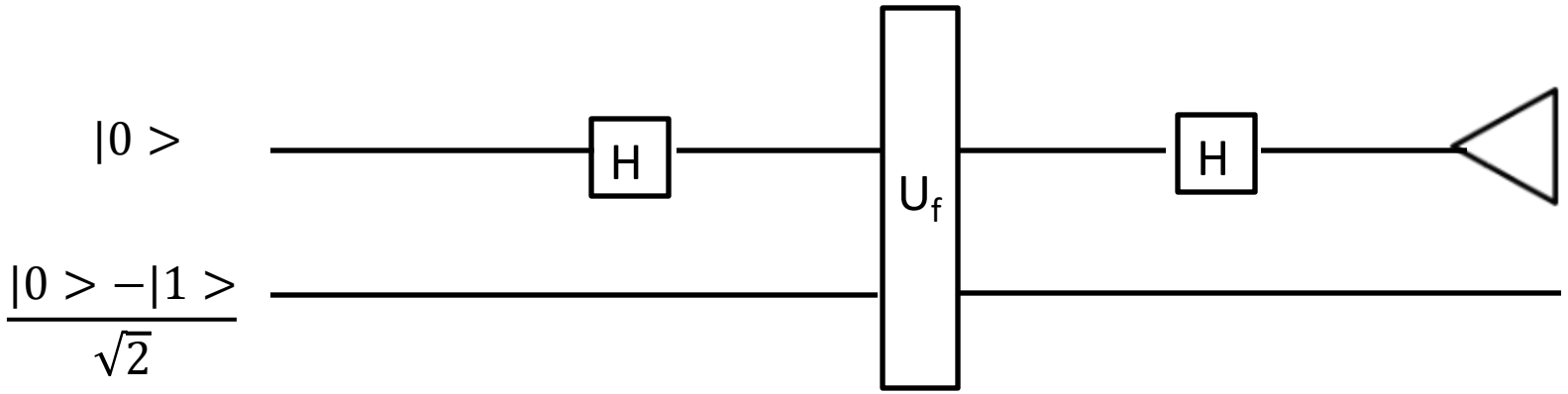
- Alice and Bob share $|\beta_{00}>$, Alice has first bit, Bob second bit
- Alice performs one of I, X, Y, Z producing $I \otimes I$ (to send 00), $X \otimes I$ (to send 01), $Y \otimes I$ (to send 10) or $Z \otimes I$ (to send 11).
- Bob measures joint state qubit measurement

- Can be used to teleport $|\psi>$:
  - $I \otimes I := \frac{1}{\sqrt{2}}(|00> + |11>) \rightarrow \frac{1}{\sqrt{2}}(|00> + |11>)$
  - $X \otimes I := \frac{1}{\sqrt{2}}(|00> + |11>) \rightarrow \frac{1}{\sqrt{2}}(|01> + |10>)$
  - $Z \otimes I := \frac{1}{\sqrt{2}}(|00> + |11>) \rightarrow \frac{1}{\sqrt{2}}(|00> - |11>)$
  - $ZX \otimes I := \frac{1}{\sqrt{2}}(|00> + |11>) \rightarrow \frac{1}{\sqrt{2}}(|01> - |10>)$



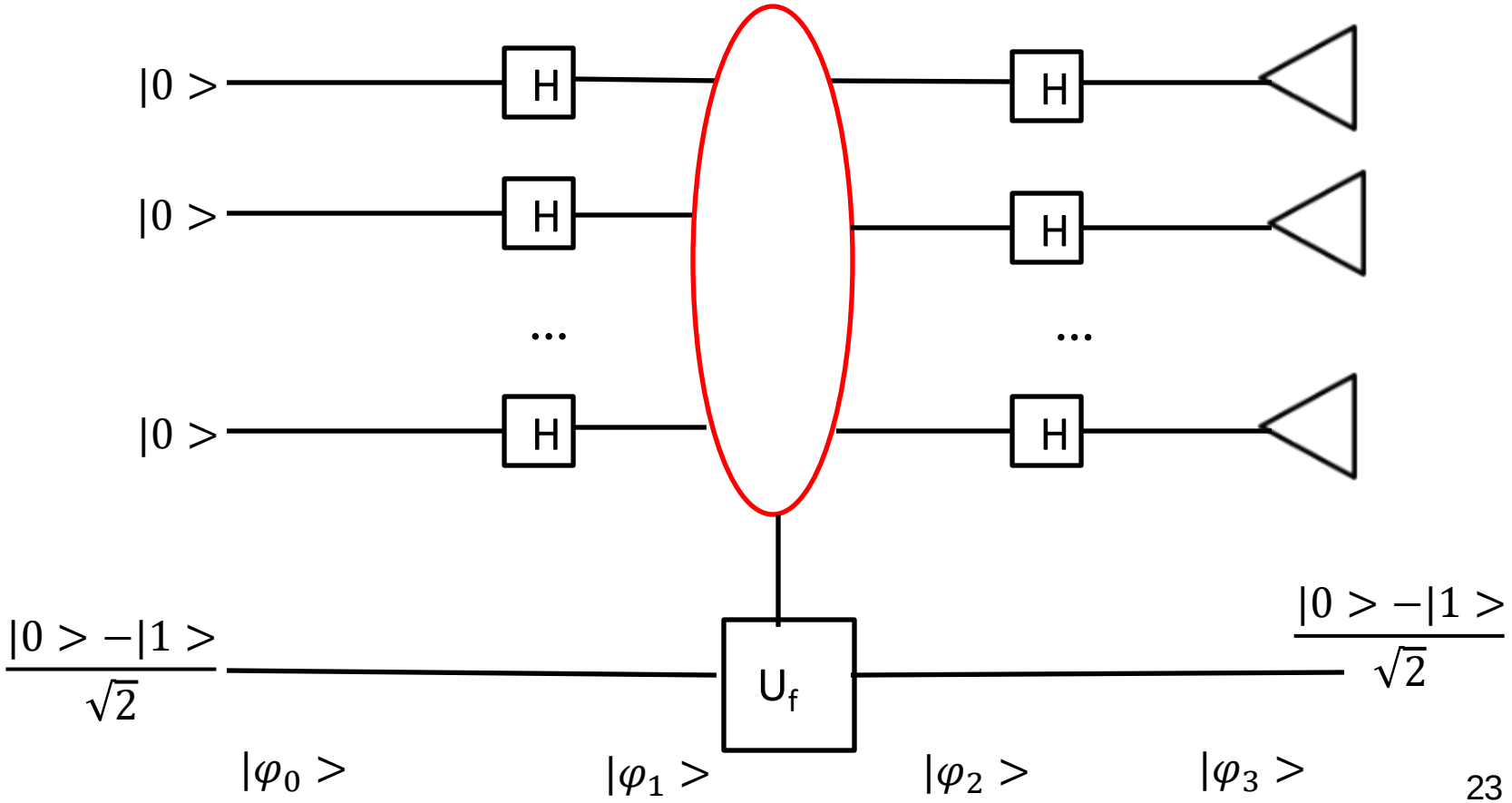
Deutch

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



Deutch-Josza

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



DJ

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

Simon

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

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

Phase kick back

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

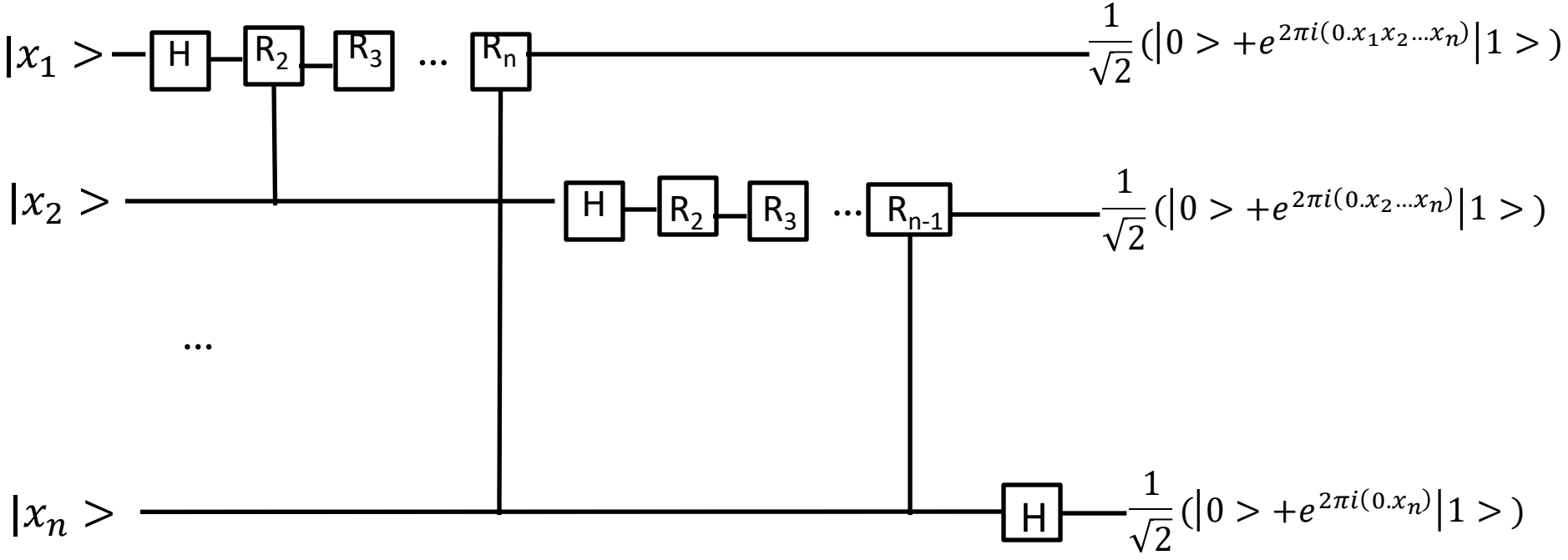
Phase Estimation

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

Quantum Fourier Transform

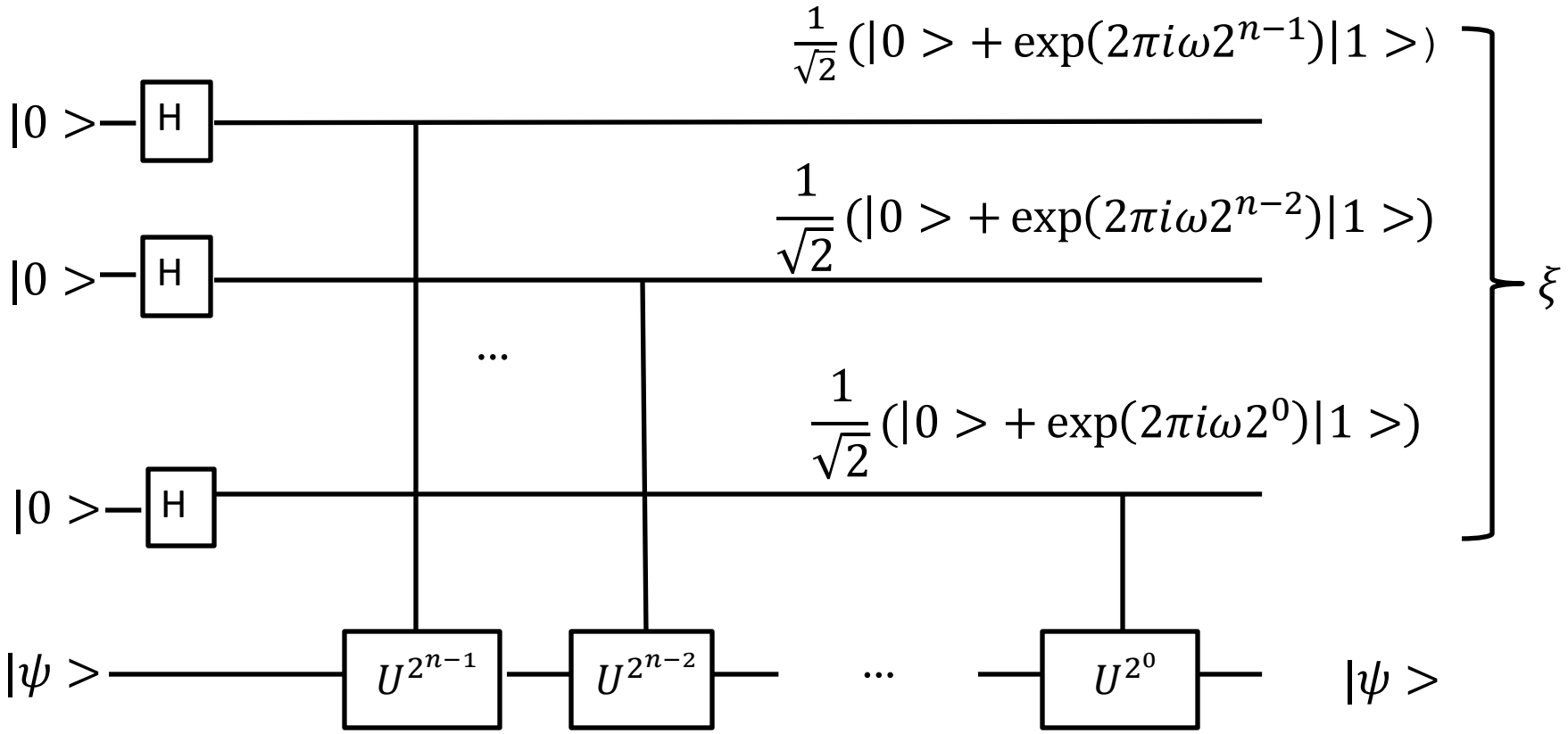
- $H^{\otimes n}(|\boldsymbol{x}>) = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{y}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}} |\boldsymbol{y}>$
- $H^{\otimes n}(H^{\otimes n}(|\boldsymbol{x}>)) = |\boldsymbol{x}>$
- $QFT_m(|x>) = \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} e^{2\pi i/m (x\cdot y)} |y>$
- $QFT_m{}^{-1}(|x>)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

Quantum Fourier Circuit



Eigenvalue Estimation

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



Eigenvalue Estimation

- $U|\psi> = \exp(2\pi i\phi)\ |\psi>$, so $U^{2^j}|\psi> = \exp\left(2\pi i\phi 2^j\right)\ |\psi>$.
- Applying ${QFT_n}^{-1}$ to ξ, gives $< x_n,\ x_{n-1}, \dots, x_1 >$, where $|\phi> =. x_1 x_2 \dots x_n$
- 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 $a^r = 1\ (mod\ N)$ then $r = 0\ \big(mod\ \varphi(pq)\big)$
- If r is even, say, $r = 2s$, $(a^s + 1)(a^s - 1) = 0\ (mod\ pq)$.
- There is a good chance $p|(a^s - 1)$ but $\big(q, (a^s - 1)\big) = 1$.
- Then $\big((a^s - 1), \mathrm{N}\big) = \mathrm{p}$. Voila!
- Note that $|v_t> = \frac{1}{r}\sum_{k=0}^{r-1} \exp(-\frac{2\pi ikt}{r})|k(mod\ N)>$ is an eigenvalue of $U_x\ (k) = |xk\ (mod\ N)>$.
- In Shor, $|1> = \frac{1}{\sqrt{r}}\sum |v_t>$.
- Applying QFT^{-1} to control gives phase of eigenvalues
- Measurement of target gives $|\frac{s}{r}>$ with $\Pr(|y>) = \frac{1}{2^{2n}}\ |\frac{1-r^{2^n}}{1-r}|^2$, 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: $a^r (mod\ N) = 1$

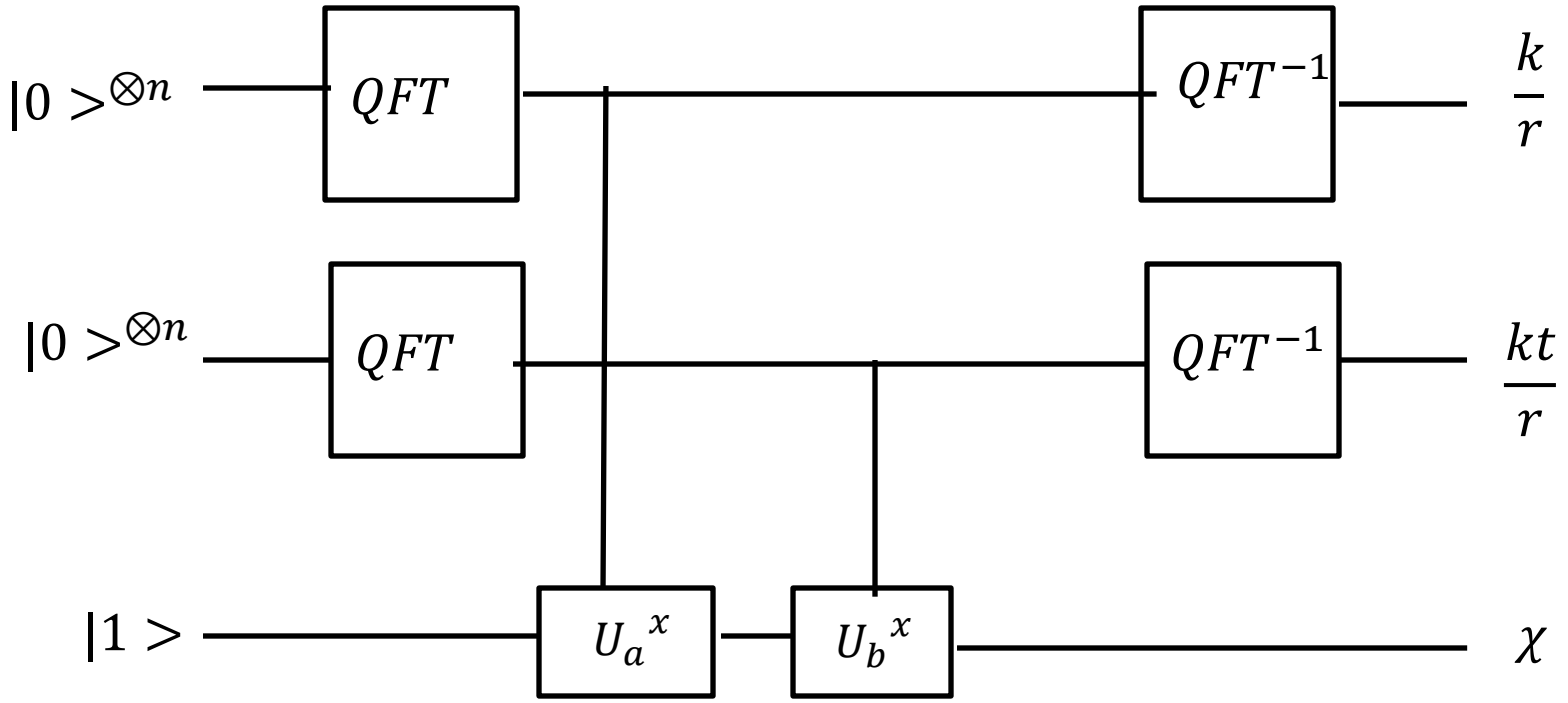
1. Choose n: $2^n \geq 2r^2$
2. Initialize control register $|000 \ldots 0> = |0>^{\otimes 2n}$
3. Initialize target register to $= |000 \ldots 01> = |000 \ldots 0> = |0>^{\otimes 2n} \otimes |1>$
4. Apply QFT to control register
5. Apply $c - U_a{}^x$ to control and target register
6. Apply QFT^{-1} 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 $c_2, 2$: $\left|\frac{x_2}{2^n} - \frac{c_2}{r_2}\right| \leq 2^{-(n-1)/2}$, if none, FAIL
10. Compute r $= LCM(r_1, r_2)$ and $a^r\ (mod\ N)$
11. If $a^r\ (mod\ N) = 1$, 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 $a = b^x \ (mod\ p)$, b has known order. We want r: $b^r = 1 (mod\ p)$
- Put $U_a(\ |x>) = |ax\ (mod\ p)>$ and $U_b(\ |x>) = |bx\ (mod\ p)>$.
- Consider the circuit below. $|1> = \frac{1}{\sqrt{r}} \sum |v_t>$. Below, $t = xy^{-1}$

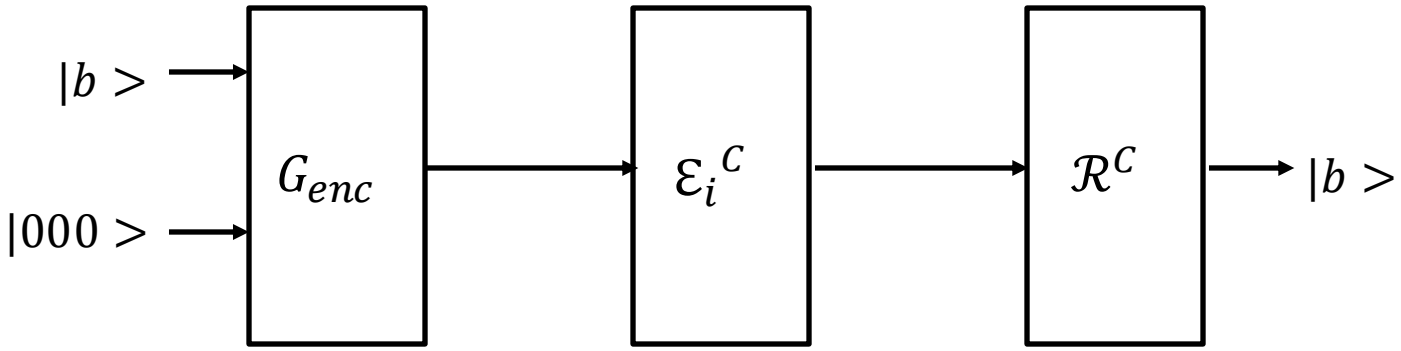


Discrete log

- Measuring first control register gives $|\frac{k}{r}>$
- Measuring first control register gives $|\frac{kt}{r}>$

- Quantum complexity is $O(\lg(p)^2 \lg(\lg(p)) \lg(\lg(\lg(p))))$
- Best known classical requires $\exp(O(\sqrt{\lg(p) \lg(\lg(p))}))$

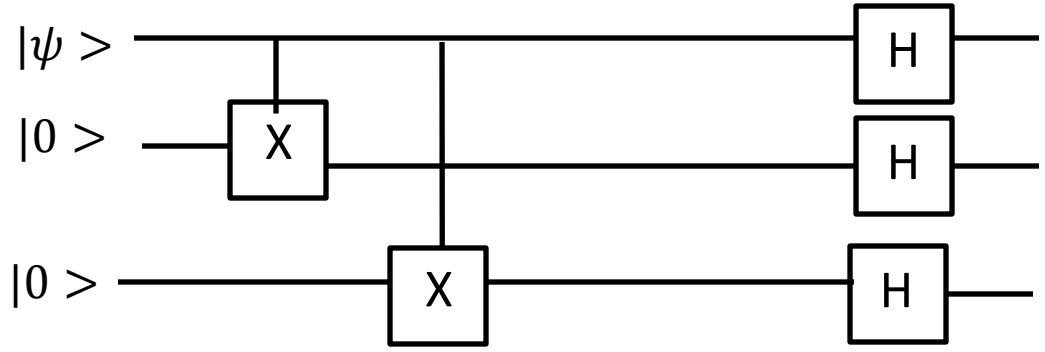
Error Correction



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

Error Correction

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



Amplitude Amplification

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

Grover

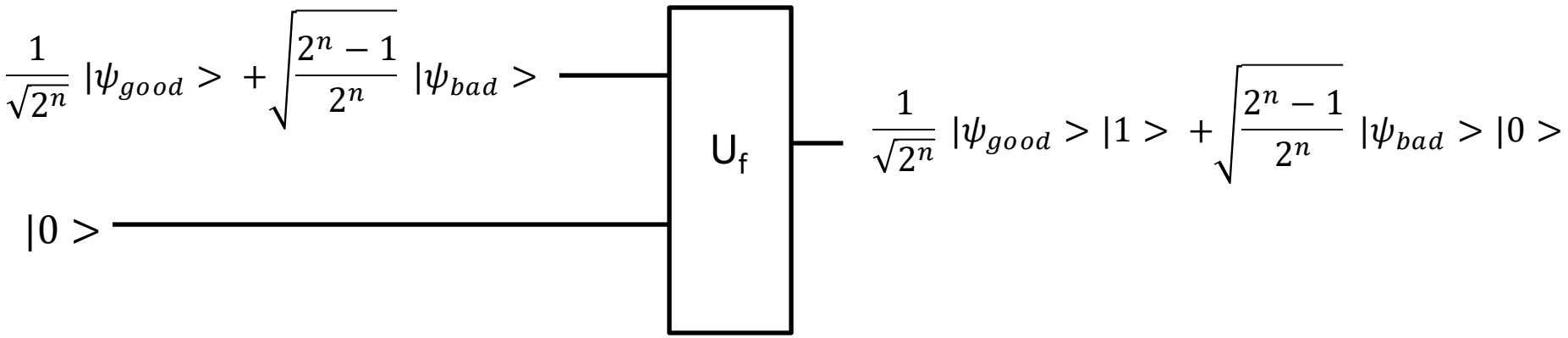
Search

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

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

$|\psi_{good}> = \boldsymbol{w}$

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



Grover

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

Search

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

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

$|\psi_{good}> = \boldsymbol{w}$

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

Algorithm G

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

Algorithm $U_{0^\perp}$

$U_{0^\perp}: |\mathrm{x}> \longrightarrow -|x>, x \neq 0$

$U_{0^\perp}: |0> \longrightarrow 0|x>$

End

Hidden subgroup

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