ICEPP, The University of Tokyo

Koshiba-sensei

Let's do experiment at the place where there is the highest-energy accelerator!

1974 Predecessor organization formed

1989 LEP-OPAL experiment

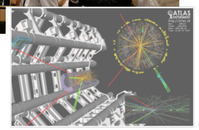
1994 Re-established as ICEPP

2008 LHC & MEG experiments

2021 Quantum-AI Technology division formed

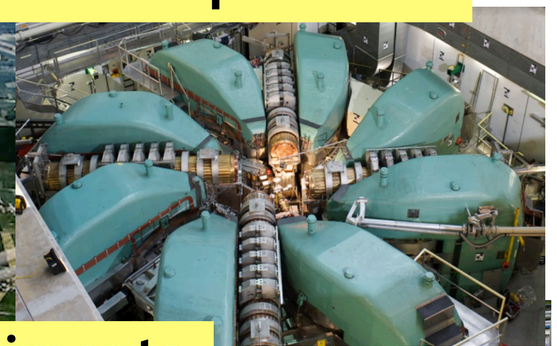
2024 50th Anniversary!

Higgs discovery (2012)

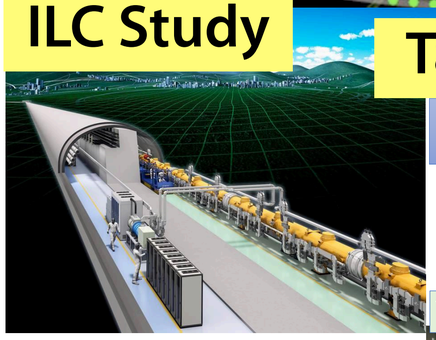


LHC-ATLAS Experiment

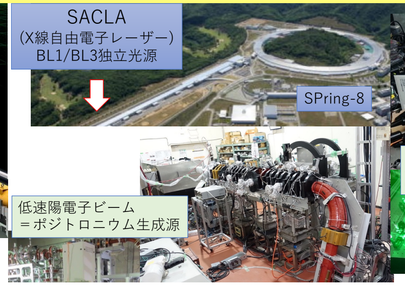
MEG Experiment



ILC Study

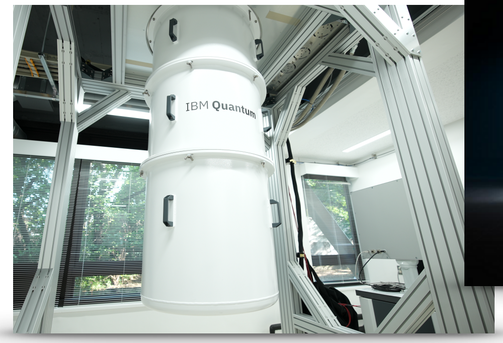


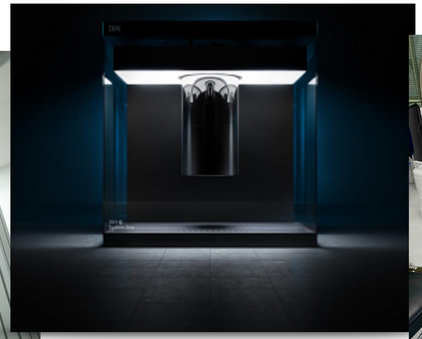
Tabletop Experiments

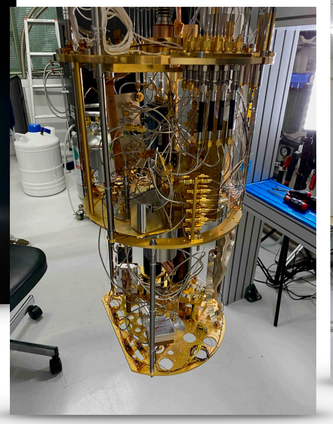


Quantum AI

Physics research and computational science with Qubit technologies





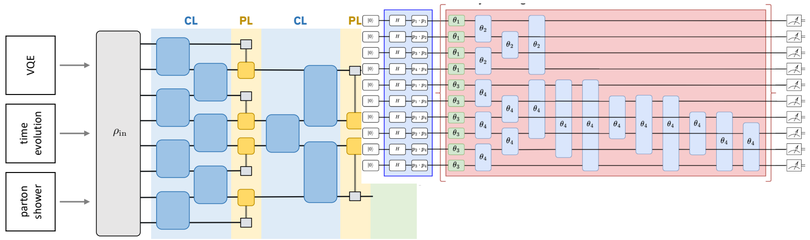


Quantum Research & Education at ICEPP

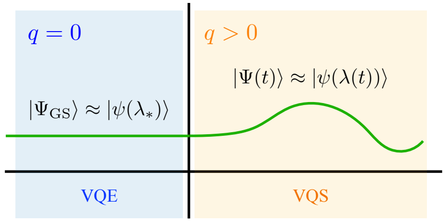
quantum-icepp.jp

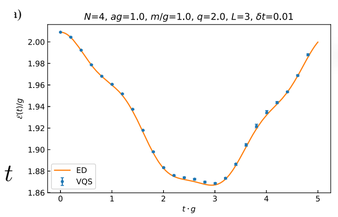
Quantum AI, Simulation & Software

Quantum Machine Learning

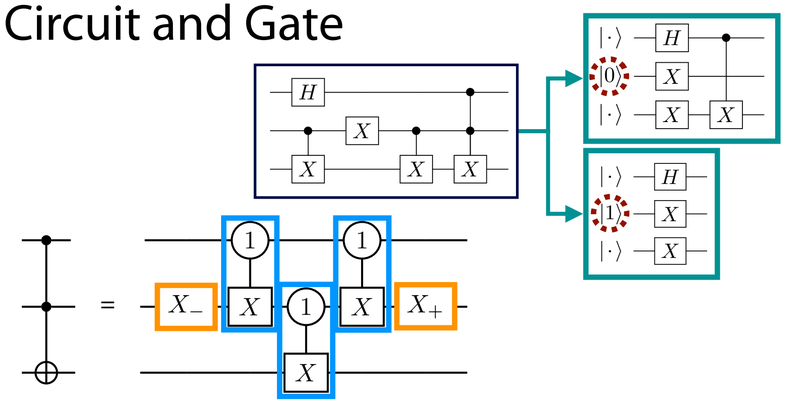


Quantum Simulation



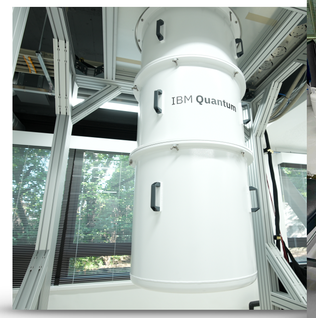


Design/Optimization of Quantum Circuit and Gate

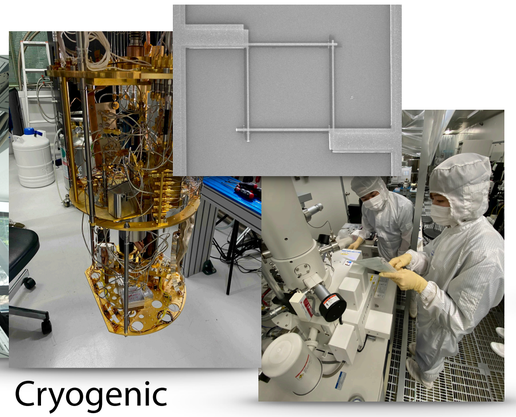


Quantum Sensing & Hardware

Superconducting Qubits and Sensor Application

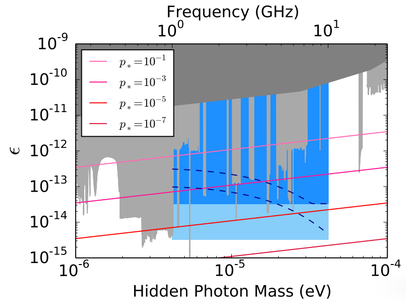


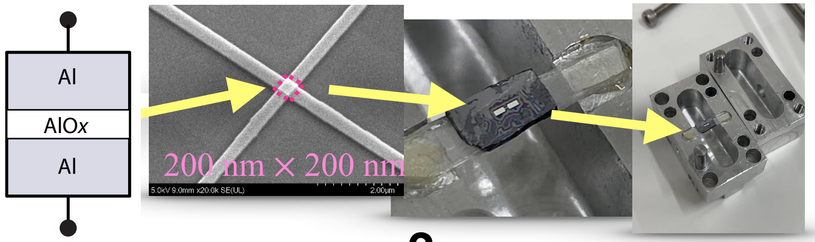
UTokyo Asano campus



Cryogenic Research Center

Search for Dark Matter and Gravitational Waves



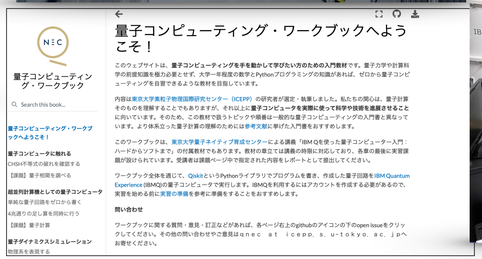


Quantum Computing Education, Collaboration

Quantum Computing Lecture & Workbook

東京大学
量子ネイティブ育成センター
Quantum Native Education Center
The University of Tokyo

Faculty of Science Bld.



Collaboration

- CERN, LBNL, Fermilab, UChicago
- IBM and Industrial Companies

KMI School 2024

Quantum Computing for Particle Physics and Astrophysics
Nagoya University, March 5, 2024

Basics of Quantum Computation

~ Qubit, Gate, Circuit and Quantum Algorithms ~

ICEPP, The University of Tokyo
Koji Terashi

Outline of the Lecture

1. Basics of Quantum Computation
2. Representing Physical System, Dynamics Simulation

} Tuesday

3. Variational Quantum Algorithm, Quantum Machine Learning
4. Quantum Computing Applications to HEP
5. Superconducting Qubits, Gate Operation, Microwave Pulse

} Wednesday

6. Transom Qubits, Fabrication, Quantum Sensing Application

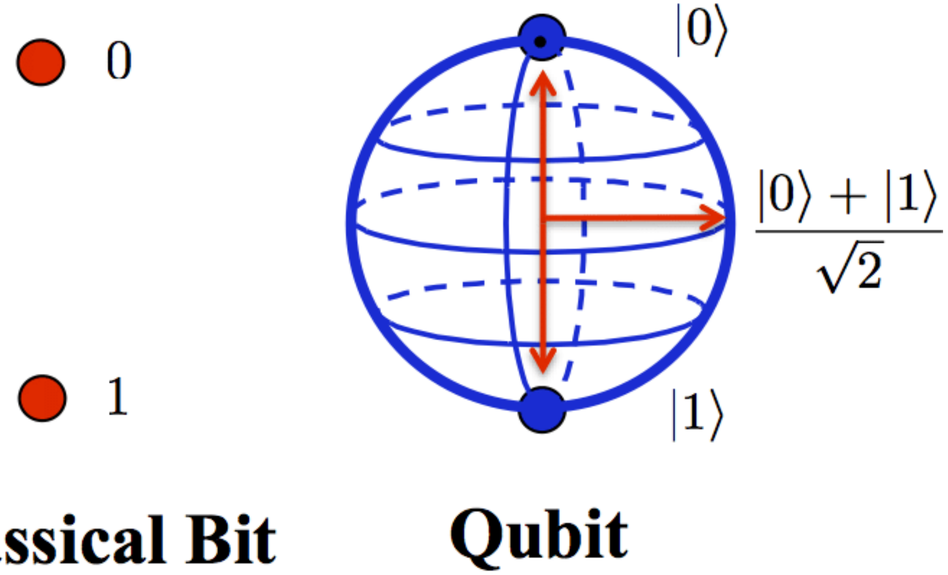
} Thursday

Quantum Bits

Quantum Bits = Unit of quantum information processing:

- A minimal quantum system that can represent two different states (e.g, $|0\rangle$ and $|1\rangle$)
  - e.g, Spin up/down, Longitudinal/transverse polarization of light, Clockwise/Anti-clockwise rotation of current
- Can represent arbitrary superposition of $|0\rangle$ and $|1\rangle$ states
- Single-qubit state = A vector in 2-dimensional complex space
- Unitary operator (matrix) can change the state of qubits

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



Quantum Bits

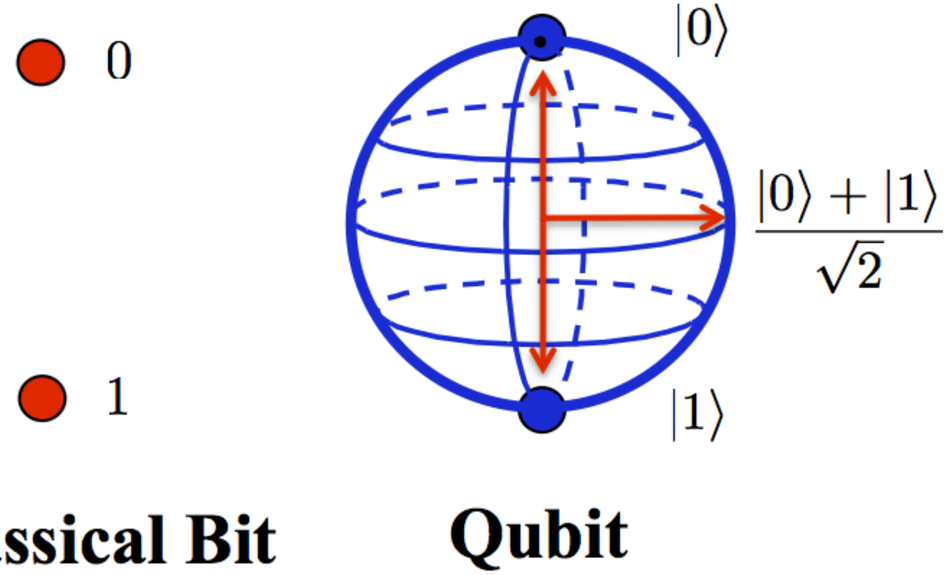
Quantum Bits = Unit of quantum information processing:

- A minimal quantum system that can represent two different states (e.g, $|0\rangle$ and $|1\rangle$)
  - e.g, Spin up/down, Longitudinal/transverse polarization of light, Clockwise/Anti-clockwise rotation of current
- Can represent arbitrary superposition of $|0\rangle$ and $|1\rangle$ states
- Single-qubit state = A vector in 2-dimensional complex space
- Unitary operator (matrix) can change the state of qubits

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

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ as an arbitrary superposition state

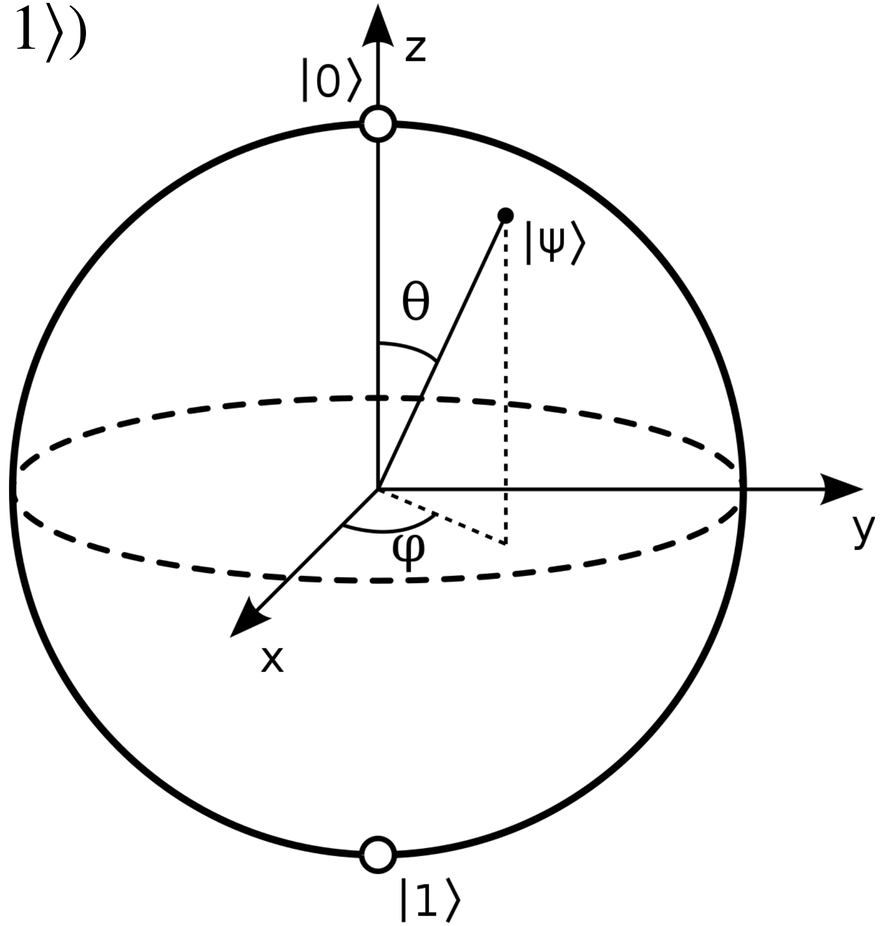
- α, β are complex values ➔ *Amplitude*
- Obtain 0(1) with probability $|\alpha|^2$ ($|\beta|^2$) by measuring $|\psi\rangle$
- 3 degrees of freedom ($|\alpha|^2 + |\beta|^2 = 1$)



Quantum Bits

A quantum state of an isolated qubit can be shown as a unit vector pointing to the surface of a sphere (**Bloch sphere**)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow |\psi\rangle = e^{i\gamma}(\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle)$$



(Smite-Meister - CC BY-SA 3.0)

Quantum Bits

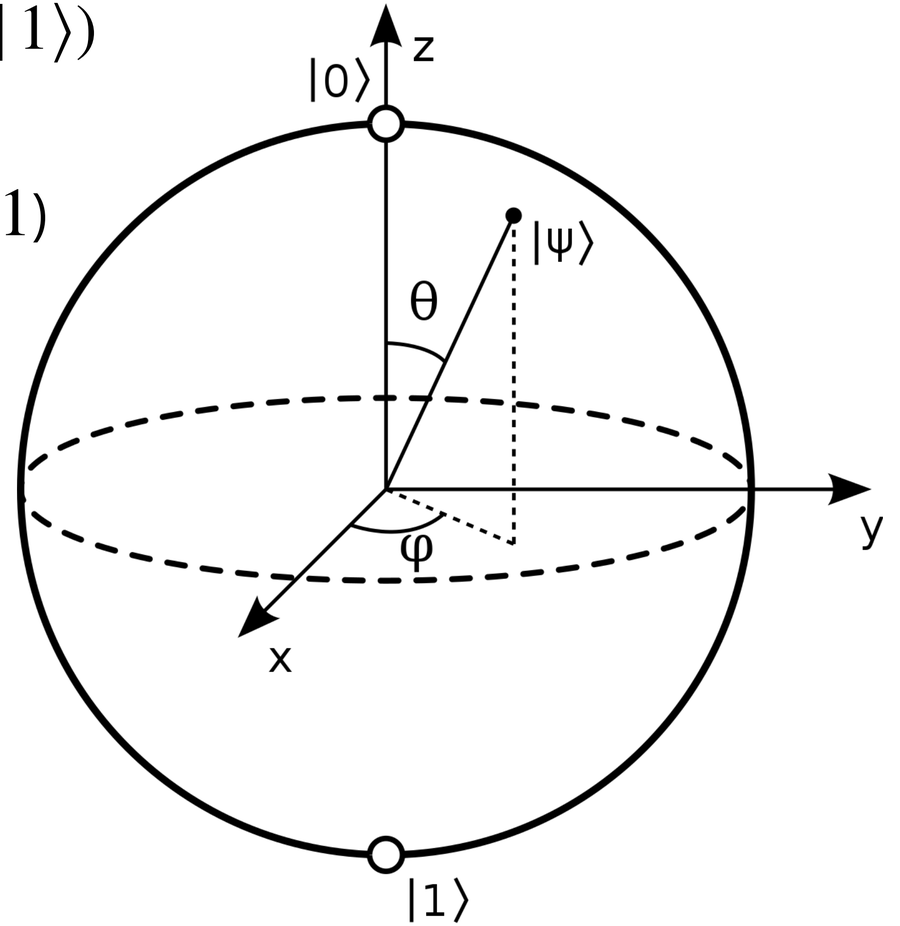
A quantum state of an isolated qubit can be shown as a unit vector pointing to the surface of a sphere (**Bloch sphere**)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow |\psi\rangle = e^{i\gamma}(\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle)$$

- Global phase γ not contribute to the measurement ($|e^{i\gamma}|^2 = 1$)
  - *2 degrees of freedom relevant for a measurement*
- Superposition state with latitude ($0 < \theta < \pi$) and longitude ($0 < \phi < 2\pi$)
- Relative phase of $|1\rangle$ to $|0\rangle = e^{i\phi}$

Multi-qubit system often written as

$$|k\rangle_{n-1}\cdots|j\rangle_1|i\rangle_0 = |k\cdots ji\rangle \;\; (i,j,\cdots,k = \{0,1\})$$



(Smite-Meister - CC BY-SA 3.0)

Quantum State Manipulation

Unitary operation to transform a quantum state of *closed* qubit system

- n-qubit Unitary operation ➔ $2^n \times 2^n$ matrix multiplication

$$|\psi\rangle \rightarrow U|\psi\rangle =: |\phi\rangle \qquad \langle\phi|\phi\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle \text{ for unitary } U$$

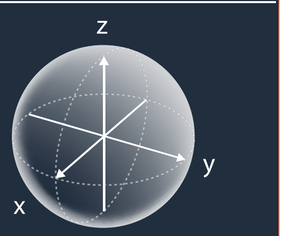
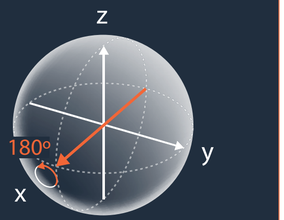
Isolated n-qubit system fully described by a state vector:

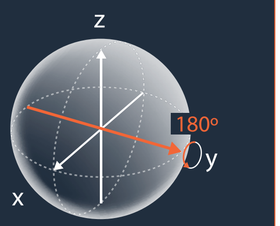
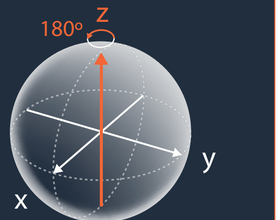
$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle \quad c_i \in \mathbb{C}^{2^n}$$

Classical state-vector simulation ➔ Directly calculate matrix-vector multiplications

Single-Qubit Gate

A Quantum Engineer's Guide to Superconducting Qubits
arXiv:1904.06560

GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE	BLOCH SPHERE
I Identity-gate: no rotation is performed.		$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Input / Output $\|0\rangle$ / $\|0\rangle$ $\|1\rangle$ / $\|1\rangle$	
X gate: rotates the qubit state by π radians (180°) about the x-axis.		$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Input / Output $\|0\rangle$ / $\|1\rangle$ $\|1\rangle$ / $\|0\rangle$	

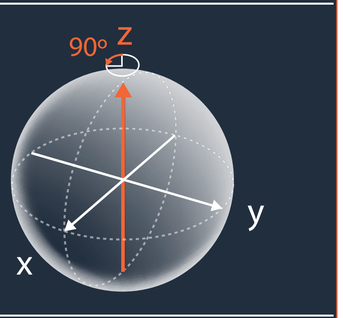
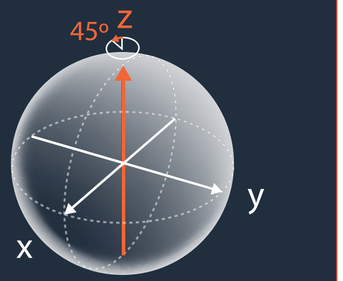
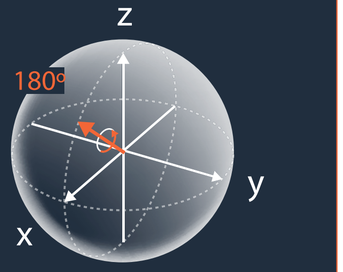
GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE	BLOCH SPHERE
Y gate: rotates the qubit state by π radians (180°) about the y-axis.		$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	Input / Output $\|0\rangle$ / $i\|1\rangle$ $\|1\rangle$ / $-i\|0\rangle$	
Z gate: rotates the qubit state by π radians (180°) about the z-axis.		$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Input / Output $\|0\rangle$ / $\|0\rangle$ $\|1\rangle$ / $-\|1\rangle$	

Single-qubit rotation around X, Y, Z axes

$$R_X(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \quad R_Y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \quad R_Z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Single-Qubit Gate

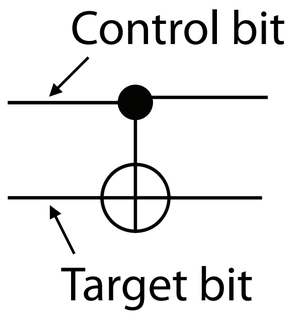
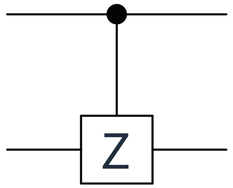
A Quantum Engineer's Guide to Superconducting Qubits
arXiv:1904.06560

GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE	BLOCH SPHERE
S gate: rotates the qubit state by $\frac{\pi}{2}$ radians (90°) about the z-axis.	S	$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$	Input / Output $\|0\rangle$ / $\|0\rangle$ $\|1\rangle$ / $e^{i\frac{\pi}{2}}\|1\rangle$	
T gate: rotates the qubit state by $\frac{\pi}{4}$ radians (45°) about the z-axis.	T	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$	Input / Output $\|0\rangle$ / $\|0\rangle$ $\|1\rangle$ / $e^{i\frac{\pi}{4}}\|1\rangle$	
H gate: rotates the qubit state by π radians (180°) about an axis diagonal in the x-z plane. This is equivalent to an X-gate followed by a $\frac{\pi}{2}$ rotation about the y-axis.	H	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	Input / Output $\|0\rangle$ / $\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$ $\|1\rangle$ / $\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	

S and T gates to shift phases

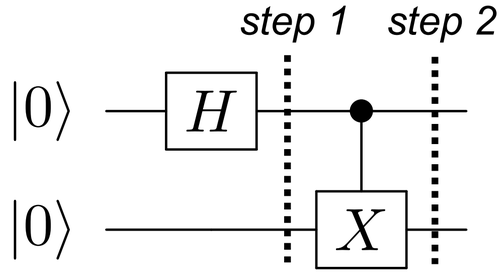
H gate for creating superposition

Two-Qubit Gate

GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE
Controlled-NOT gate: apply an X-gate to the target qubit if the control qubit is in state $\|1\rangle$		$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	Input / Output $\|00\rangle$ / $\|00\rangle$ $\|01\rangle$ / $\|01\rangle$ $\|10\rangle$ / $\|11\rangle$ $\|11\rangle$ / $\|10\rangle$
Controlled-phase gate: apply a Z-gate to the target qubit if the control qubit is in state $\|1\rangle$		$\text{CPHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$	Input / Output $\|00\rangle$ / $\|00\rangle$ $\|01\rangle$ / $\|01\rangle$ $\|10\rangle$ / $\|10\rangle$ $\|11\rangle$ / $-\|11\rangle$

Controlled-U gate with control qubit i and target qubit j generally written as $C_j^i[U]$

Gates to create entangled states



Write $|0\rangle|0\rangle$ as $|00\rangle$

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

step 2 $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ state cannot be written as a product of two qubit states "$|a\rangle \otimes |b\rangle$"

→ Entanglement

Basis and Measurement

Given a state $|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$ written in *some basis states* $|i\rangle$, the measurement outcome of $|\psi\rangle$ in *the* $|i\rangle$ *basis* is i with the probability $|c_i|^2$

Usually quantum computer is measured in the *computational basis* (or Z *basis*) : $|i\rangle = \{0,1,\cdots,2^{n-1}\}$

Basis and Measurement

Given a state $|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$ written in *some basis states* $|i\rangle$, the measurement outcome of $|\psi\rangle$ in *the* $|i\rangle$ *basis* is i with the probability $|c_i|^2$

Usually quantum computer is measured in the *computational basis* (or Z *basis*) : $|i\rangle = \{0,1,\cdots,2^{n-1}\}$

Nothing special about the basis in terms of quantum computation

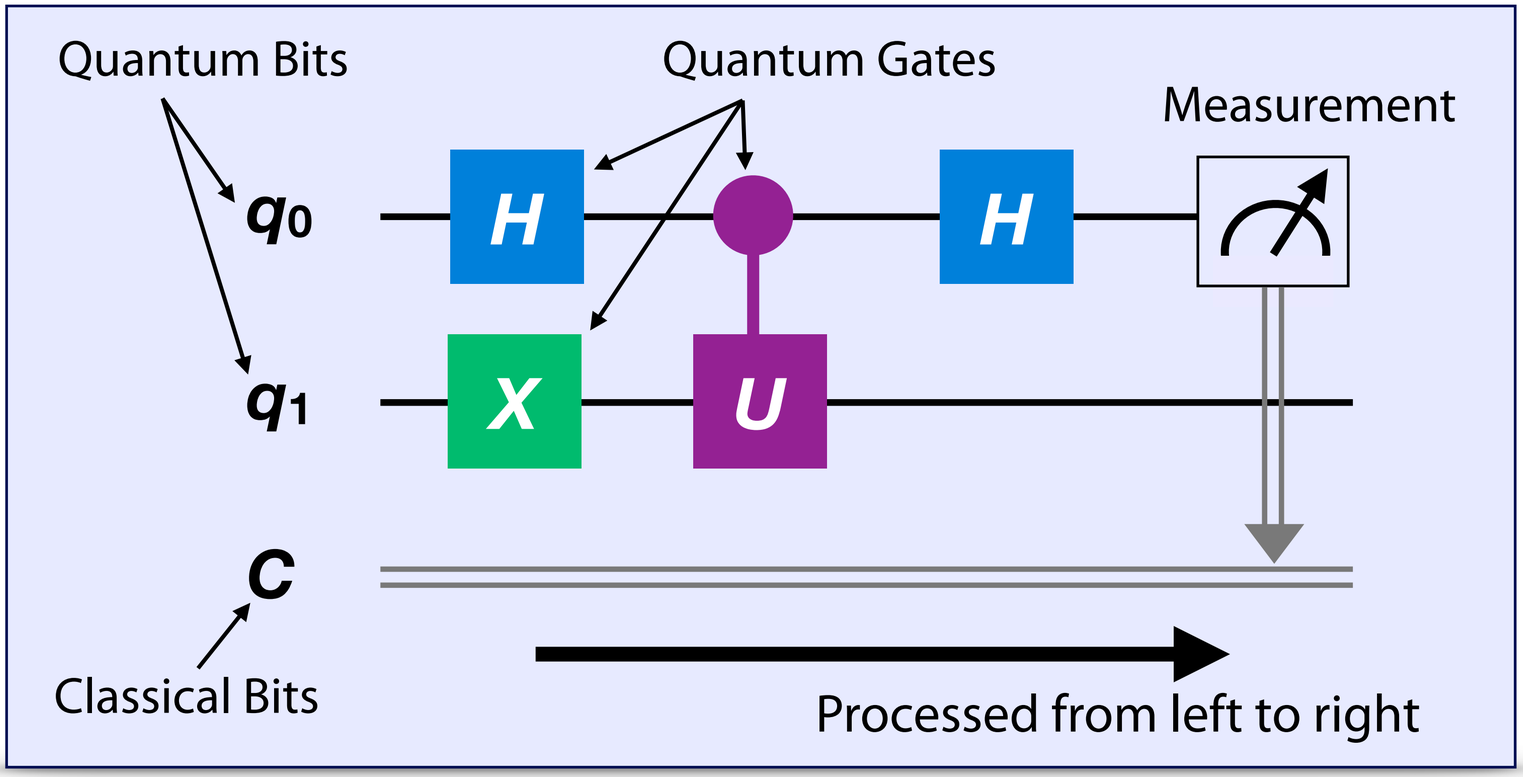
Consider X basis : $|+\rangle := H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle := H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

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

Measure $\pm$ in X basis with the probabilities $\frac{(a \pm b)^2}{2}$

➡ Equivalent to changing the basis to X basis and measuring the state in computational basis: $|\psi\rangle \rightarrow H|\psi\rangle = \frac{1}{\sqrt{2}}(a+b)|0\rangle + \frac{1}{\sqrt{2}}(a-b)|1\rangle$

Quantum Circuit



A circuit is expressed by matrix multiplications to the initial state:

$$H_0 C_1^0[U] X_1 H_0 |0\rangle_1 |0\rangle_0$$

acting from right to left

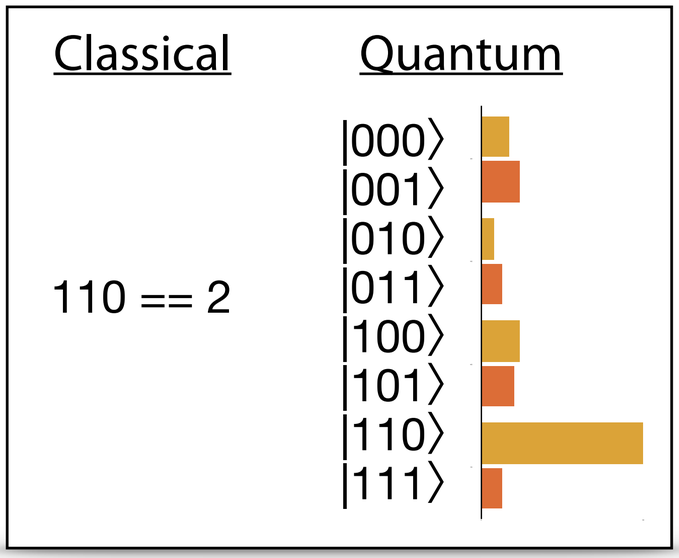
- Construct quantum circuit by arranging quantum gates in order defined by a quantum algorithm
- Prepare an initial state and process the state by quantum circuit
- Measure the output state, resulting in a collection of classical bits

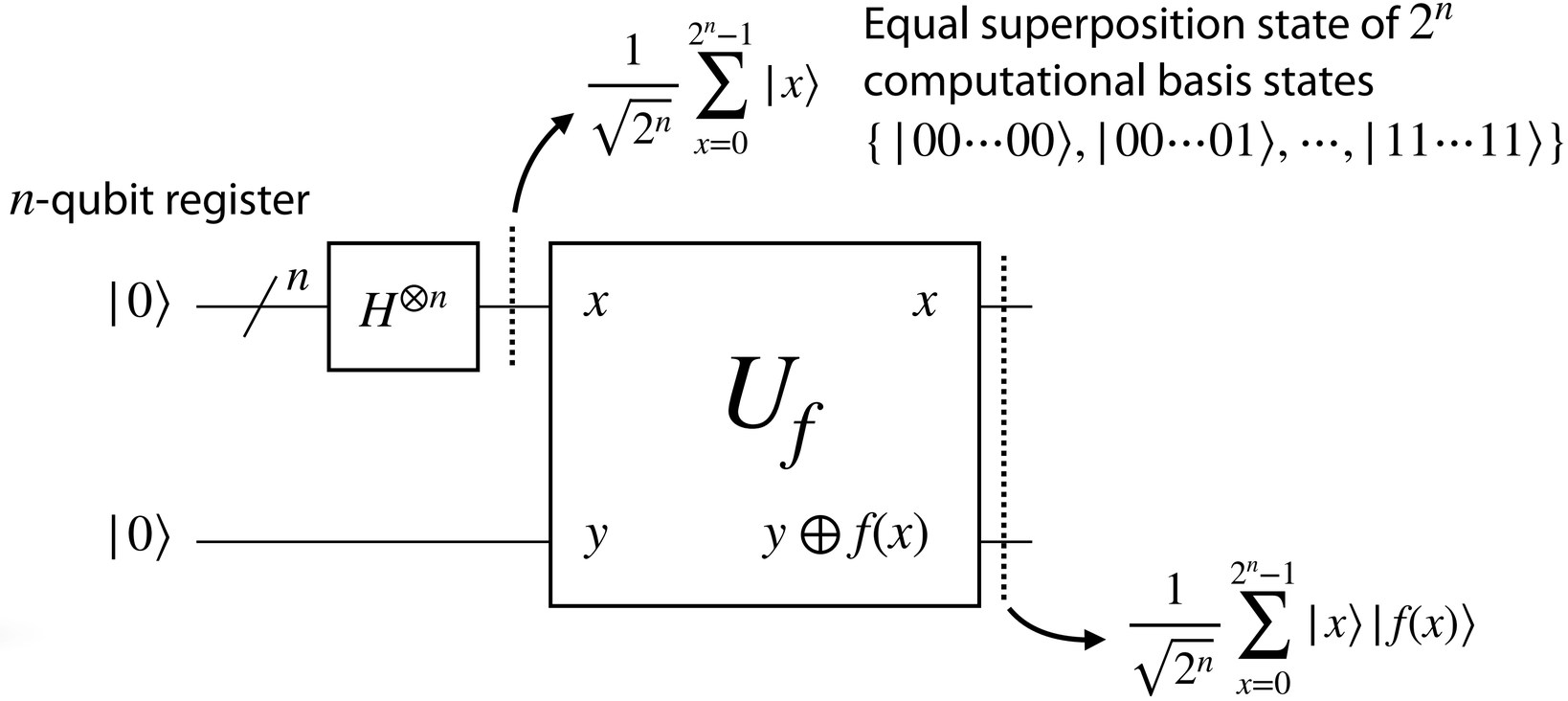
➡ Gate-based quantum computing in quantum circuit model

Quantum Computation (I)

① Perform parallel computation using superposition states

Superposition





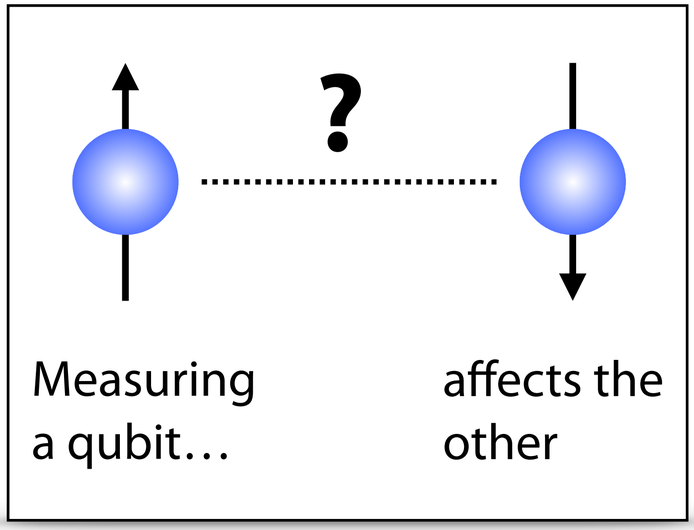
10 qubits → 1000 states
50 qubits → 1000 trillion states
300 qubits → states of the number of all atoms in the Universe

A single unitary operation, acting as $U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, will allow us to calculate $f(x)$ for all $x's$ simultaneously (though there is a caveat)

Quantum Computation (II)

② Increase information capacity by using entangled states

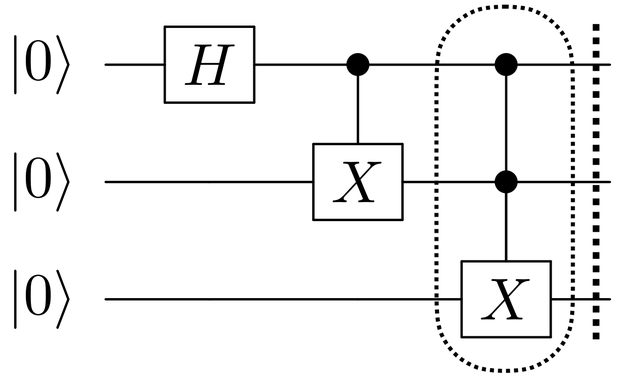
Entanglement



A quantum state such as $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ is maximally entangled, and called **Bell state**

If qubit 1 is observed to be $|0(1)\rangle$, qubit 2 is determined to be $|1(0)\rangle$ instantly

3-qubit maximally entangled state =
GHZ (Greenberger-Horne-Zeilinger) state



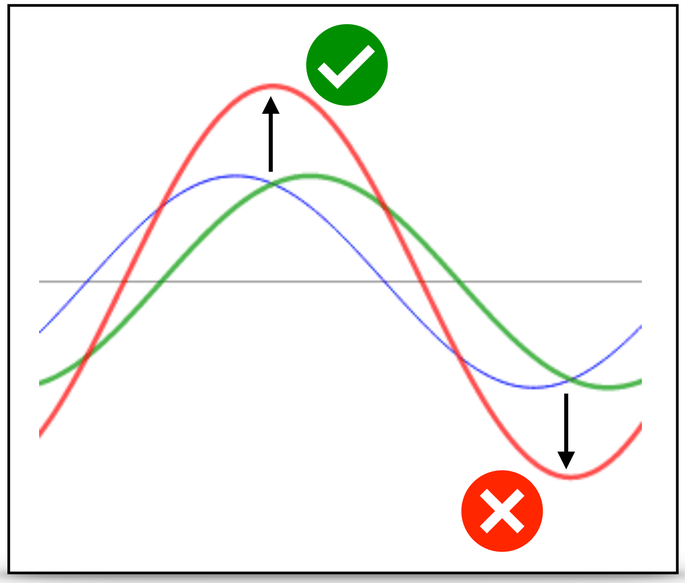
Toffoli gate

$$\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

Quantum Computation (III)

③ Utilizing interference of quantum superposition for efficient computation

Interference



Manipulate quantum states so that a right (wrong) answer has a larger (smaller) amplitude

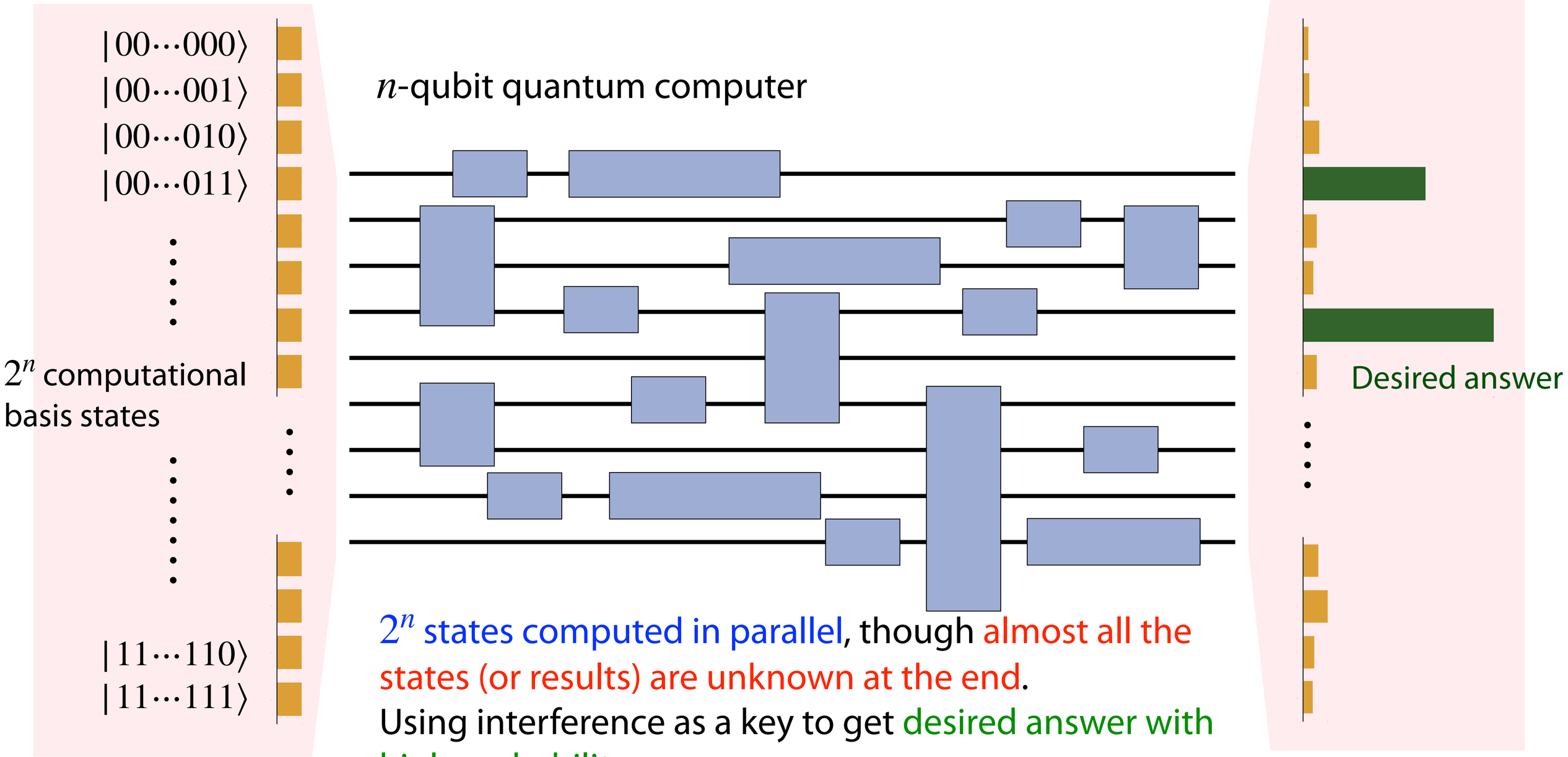
Using phase information is crucial for quantum interference

Quantum Fourier Transform (QFT) to be learned later is often a key technique

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi ijk}{N}\right) |k\rangle$$

➡ Periodic property of the amplitude $e^{\frac{2\pi ijk}{N}}$ utilized to enhance correct answers

Computation with Quantum Circuit



2^n states computed in parallel, though almost all the states (or results) are unknown at the end.

Using interference as a key to get desired answer with high probability

Inner Product of State Vector

Inner product of two n-qubit state vectors

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle,\ |\phi\rangle = \sum_{i=0}^{2^n-1} d_i |i\rangle \quad \Rightarrow \quad \langle\psi|\phi\rangle = \sum_{i=0}^{2^n-1} c_i^* d_i$$

Cauchy-Schwarz inequality: $|\langle\psi|\phi\rangle|^2 \leq \langle\psi|\psi\rangle\langle\phi|\phi\rangle = 1$

$|\langle\psi|\phi\rangle|^2 = 1$ if $|\psi\rangle$ and $|\phi\rangle$ are the same

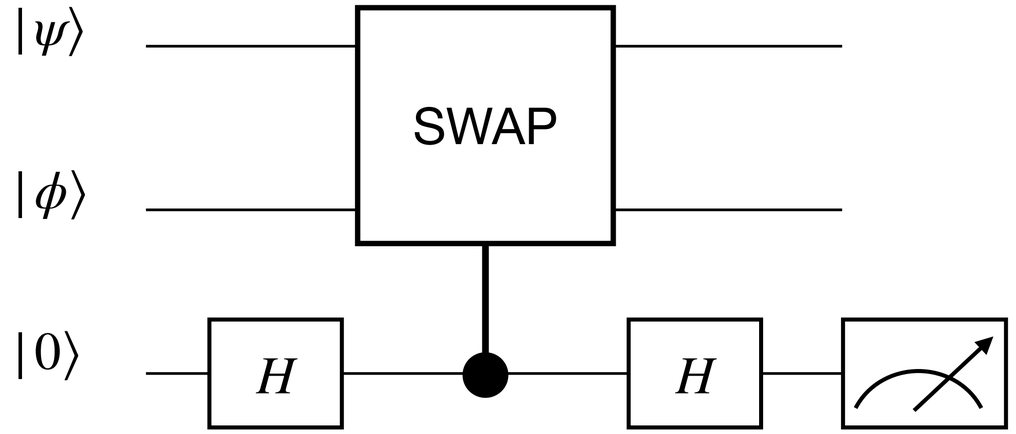
$= 0$ if $|\psi\rangle$ and $|\phi\rangle$ are orthogonal

⇒ Squared inner product = ***Closeness*** measure between state vectors

Use this property later for machine learning task

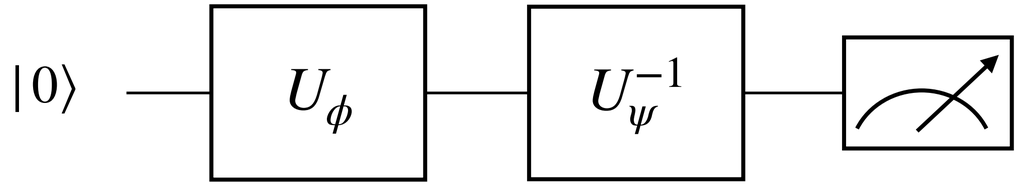
Calculation of Inner Product

Inner product by SWAP test



Squared inner product $|\langle\psi|\phi\rangle|^2 = P_0 - P_1$ obtained from the probabilities of measuring 0 and 1 on the last qubit

Inner product by inverse circuit



Squared inner product $|\langle\psi|\phi\rangle|^2 = P_0$ obtained from the probability of measuring 0

- Need to know the unitary to produce $|\psi\rangle$ and $|\phi\rangle$ from $|0\rangle$ state
- Typically more cost efficient than SWAP test

Utilize this technique in quantum machine learning

Hands-on Exercise (I)

- Quantum gates and circuits
- Single-qubit state, superposition, entangled states
- Calculation of inner products

Quantum Fourier Transform

Quantum Fourier Transform (QFT) = One of most important subroutines for quantum algorithm

A quantum state $|j\rangle$ is transformed to $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi ijk}{N}\right) |k\rangle$

$N = 2^n$

Quantum Fourier Transform

Quantum Fourier Transform (QFT) = One of most important subroutines for quantum algorithm

A quantum state $|j\rangle$ is transformed to $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi ijk}{N}\right) |k\rangle$

$N = 2^n$

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi ijk}{N}\right) |k\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{k_{n-1}=0}^{1} \sum_{k_{n-2}=0}^{1} \cdots \sum_{k_0=0}^{1} \exp\left(\frac{2\pi ij}{N} \sum_{l=1}^{n} k_{n-l} 2^{n-l}\right) |k_{n-l}\rangle$$

→ Binary representation of k

$$k = [k_{n-1} k_{n-2} \cdots k_0]$$

$$= k_{n-1} 2^{n-1} + k_{n-2} 2^{n-2} + \cdots + k_0 2^0$$

$$= \frac{1}{\sqrt{N}} \sum_{k_{n-1}=0}^{1} \sum_{k_{n-2}=0}^{1} \cdots \sum_{k_0=0}^{1} \bigotimes_{l=1}^{n} \exp\left(\frac{2\pi ijk_{n-l}}{2^l}\right) |k_{n-l}\rangle$$

$$= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left[|0\rangle + \exp\left(\frac{2\pi ij}{2^l}\right) |1\rangle \right]$$

Quantum Fourier Transform

Quantum Fourier Transform (QFT) = One of most important subroutines for quantum algorithm

A quantum state $|j\rangle$ is transformed to $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi ijk}{N}\right) |k\rangle$ $N = 2^n$

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi ijk}{N}\right) |k\rangle$$

$$= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left[|0\rangle + \exp\left(\frac{2\pi ij}{2^l}\right) |1\rangle \right]$$

$$= \frac{1}{\sqrt{N}} \left[|0\rangle + \exp\left(\frac{2\pi ij}{2}\right) |1\rangle \right] \left[|0\rangle + \exp\left(\frac{2\pi ij}{2^2}\right) |1\rangle \right] \cdots \left[|0\rangle + \exp\left(\frac{2\pi ij}{2^n}\right) |1\rangle \right]$$

$$k = [k_{n-1} k_{n-2} \cdots k_0]$$
$$= k_{n-1} 2^{n-1} + k_{n-2} 2^{n-2} + \cdots + k_0 2^0$$

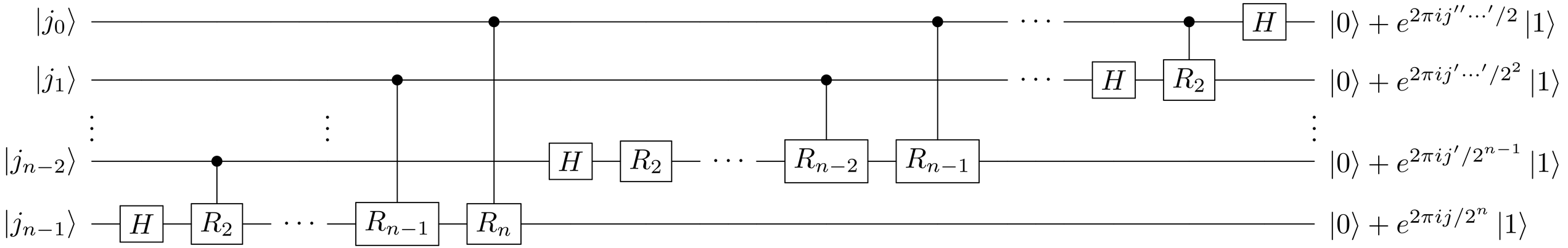
Convert a number represented as a computational base into a phase

➞ Possible to do numerical calculation by manipulating phases

Quantum Fourier Transform

Quantum circuit of QFT

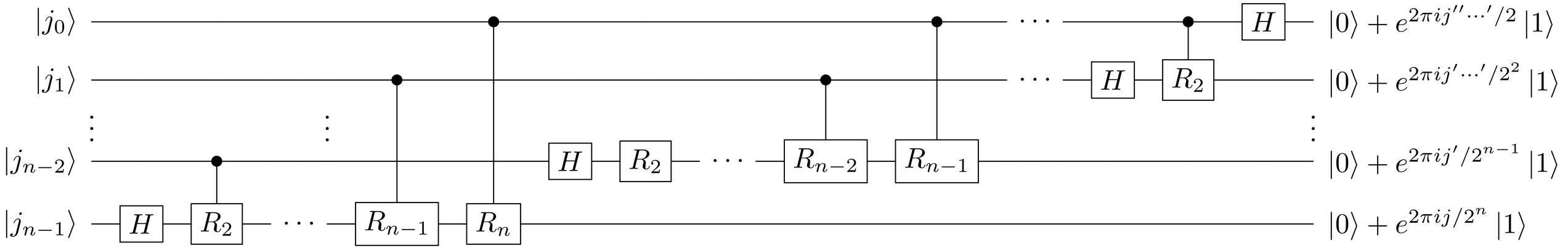
$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{bmatrix}$$ ➔ Shift phase of $|1\rangle$ state by $\exp\left(\frac{2\pi i}{2^k}\right)$



Quantum Fourier Transform

Quantum circuit of QFT

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{bmatrix}$$ ➔ Shift phase of $|1\rangle$ state by $\exp\left(\frac{2\pi i}{2^k}\right)$



$$|j_0\rangle \rightarrow |0\rangle + \exp\left[\frac{2\pi i j_0}{2^1}\right]|1\rangle = |0\rangle + \exp\left[\frac{2\pi i j''\cdots'}{2^1}\right]|1\rangle \qquad j''\cdots' = [0\cdots 0 j_0] = j_0 2^0$$

$$|j_{n-2}\rangle \rightarrow |0\rangle + \exp\left[\frac{2\pi i j_0}{2^{n-1}} + \frac{2\pi i j_1}{2^{n-2}} + \cdots + \frac{2\pi i j_{n-3}}{2^2} + \frac{2\pi i j_{n-2}}{2^1}\right]|1\rangle = |0\rangle + \exp\left[\frac{2\pi i j'}{2^{n-1}}\right]|1\rangle \quad j' = [0 j_{n-2}\cdots j_0] = j_{n-2}2^{n-2} + \cdots + j_0 2^0$$

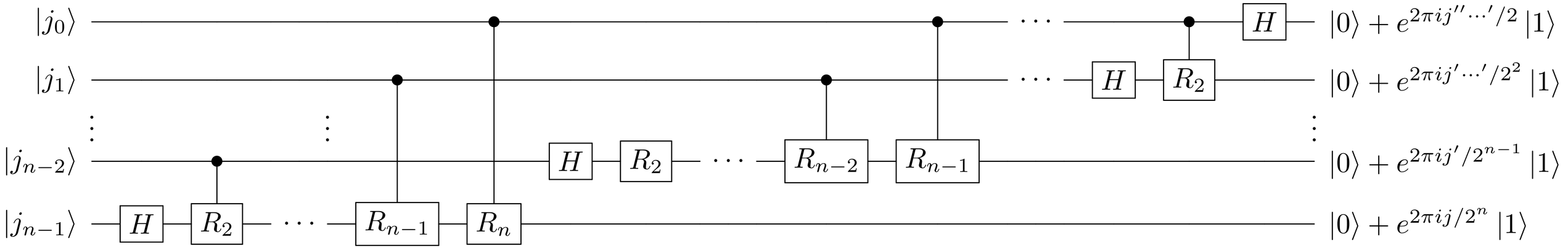
$$|j_{n-1}\rangle \rightarrow |0\rangle + \exp\left[\frac{2\pi i j_0}{2^n} + \frac{2\pi i j_1}{2^{n-1}} + \cdots + \frac{2\pi i j_{n-2}}{2^2} + \frac{2\pi i j_{n-1}}{2^1}\right]|1\rangle = |0\rangle + \exp\left[\frac{2\pi i j}{2^n}\right]|1\rangle \quad j = [j_{n-1}\cdots j_1 j_0] = j_{n-1}2^{n-1} + \cdots + j_1 2^1 + j_0 2^0$$

R_n R_{n-1} R_2 H

Quantum Fourier Transform

Quantum circuit of QFT

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{bmatrix}$$ ➔ Shift phase of $|1\rangle$ state by $\exp\left(\frac{2\pi i}{2^k}\right)$



Computational cost of Fourier transform for 2^n numbers:

- Classical Fast Fourier Transform = $\mathcal{O}(n2^n)$
- Quantum Fourier Transform = $\mathcal{O}(n^2)$ ➡ Exponential speed-up!

However, one cannot directly obtain amplitude in quantum computation

➡ How can we exploit this speed-up in quantum algorithms?

See later the case of speed-up by using QFT as a subroutine

Addition by Quantum Fourier Transform

Can utilize accumulation of phases as a means of addition

E.g, assume we want to perform $|0\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}} \rightarrow |a+b\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}}$

Addition by Quantum Fourier Transform

Can utilize accumulation of phases as a means of addition

E.g, assume we want to perform $|0\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}} \rightarrow |a+b\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}}$

1) Create equal superposition state in out register

$$|0\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}} \rightarrow \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}}$$

2) Apply P gates controlled by in1 and in2 registers to out register, making a phase shift that depends on k in out register

$$\rightarrow \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\exp\left(\frac{2\pi i(a+b)k}{2^n}\right)|k\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}}$$

3) Apply inverse QFT to out register

$$\rightarrow |a+b\rangle_{\text{out}}|b\rangle_{\text{in2}}|a\rangle_{\text{in1}}$$

Quantum Phase Estimation

Given a unitary operator U and the eigenvector $|\psi\rangle$ with $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$,

can we estimate the phase θ of the eigenvalue $e^{2\pi i\theta}$?

➡ Quantum Phase Estimation **(QPE)**

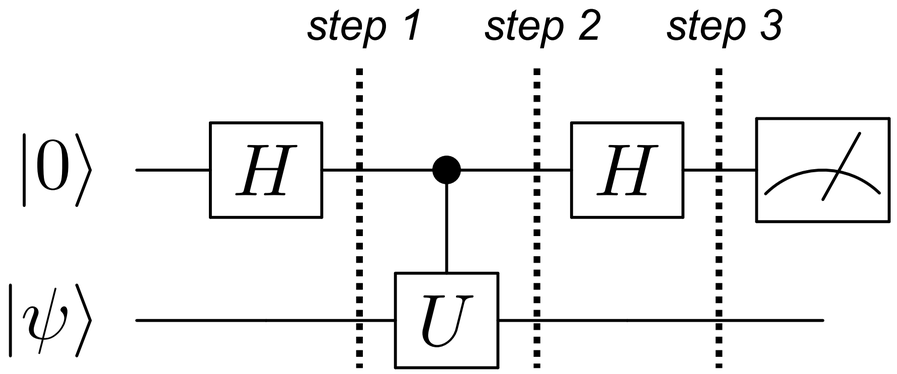
Quantum Phase Estimation

Given a unitary operator U and the eigenvector $|\psi\rangle$ with $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$,

can we estimate the phase θ of the eigenvalue $e^{2\pi i\theta}$?

➡ Quantum Phase Estimation **(QPE)**

Single-qubit QPE corresponds to the following circuit:



step 1 $\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle\right)$

step 2 $\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle e^{2\pi i\theta}|\psi\rangle\right)$

step 3 $\frac{1}{2}\left[(1+e^{2\pi i\theta})|0\rangle + (1-e^{2\pi i\theta})|1\rangle\right]|\psi\rangle$

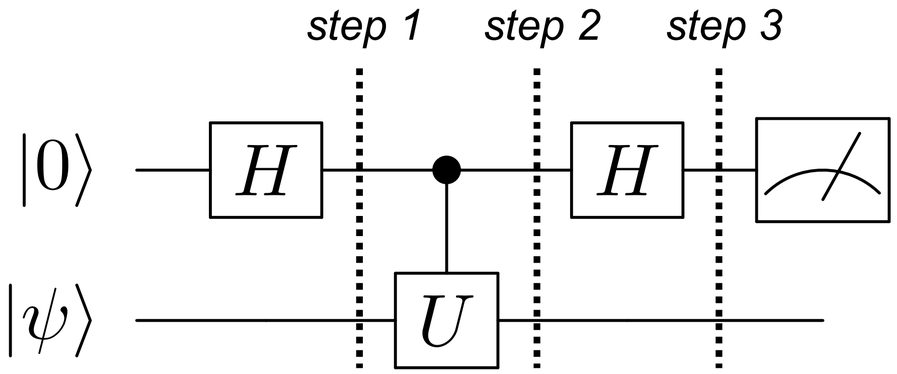
Quantum Phase Estimation

Given a unitary operator U and the eigenvector $|\psi\rangle$ with $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$,

can we estimate the phase θ of the eigenvalue $e^{2\pi i\theta}$?

➡ Quantum Phase Estimation **(QPE)**

Single-qubit QPE corresponds to the following circuit:



step 1 $\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle\right)$

step 2 $\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle e^{2\pi i\theta}|\psi\rangle\right)$

step 3 $\frac{1}{2}\left[(1+e^{2\pi i\theta})|0\rangle + (1-e^{2\pi i\theta})|1\rangle\right]|\psi\rangle$

When measuring the first qubit, the probabilities of measuring 0 and 1 give information about the phase θ

Probability of measuring $m = \{0,1\}$:

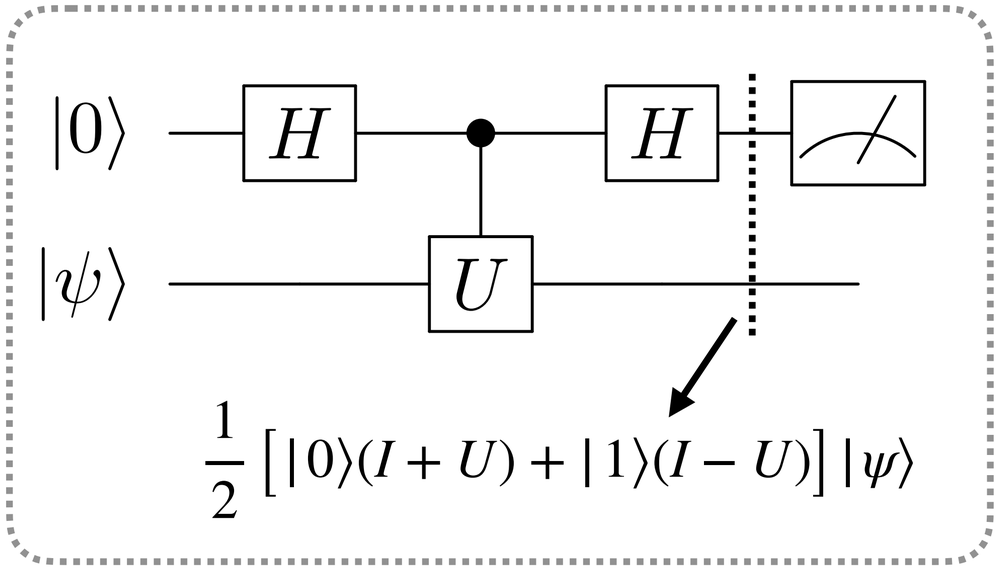
$$P_m = \left|\frac{1+(-1)^m e^{2\pi i\theta}}{2}\right|^2 = \frac{1+(-1)^m\cos(2\pi\theta)}{2}$$

$P_{0(1)}$ is very close to $1(0)$ when $\theta \ll 1$

➡ Need many measurements to extract θ value

Hadamard Test

Single-qubit QPE considered as an extension of **Hadamard Test**



If $|\psi\rangle$ is a general 1-qubit state, the probabilities of measuring 0 and 1 on the first qubit is given as follows:

Probability of measuring $m = \{0,1\}$:

$$P_m = \frac{1 + (-1)^m \,\mathrm{Re}\,\langle\psi|\,U\,|\psi\rangle}{2}$$

Assuming the state $|\psi\rangle$ is decomposed with eigenstates $|\phi_\pm\rangle$ with eigenvalues ± 1 for U

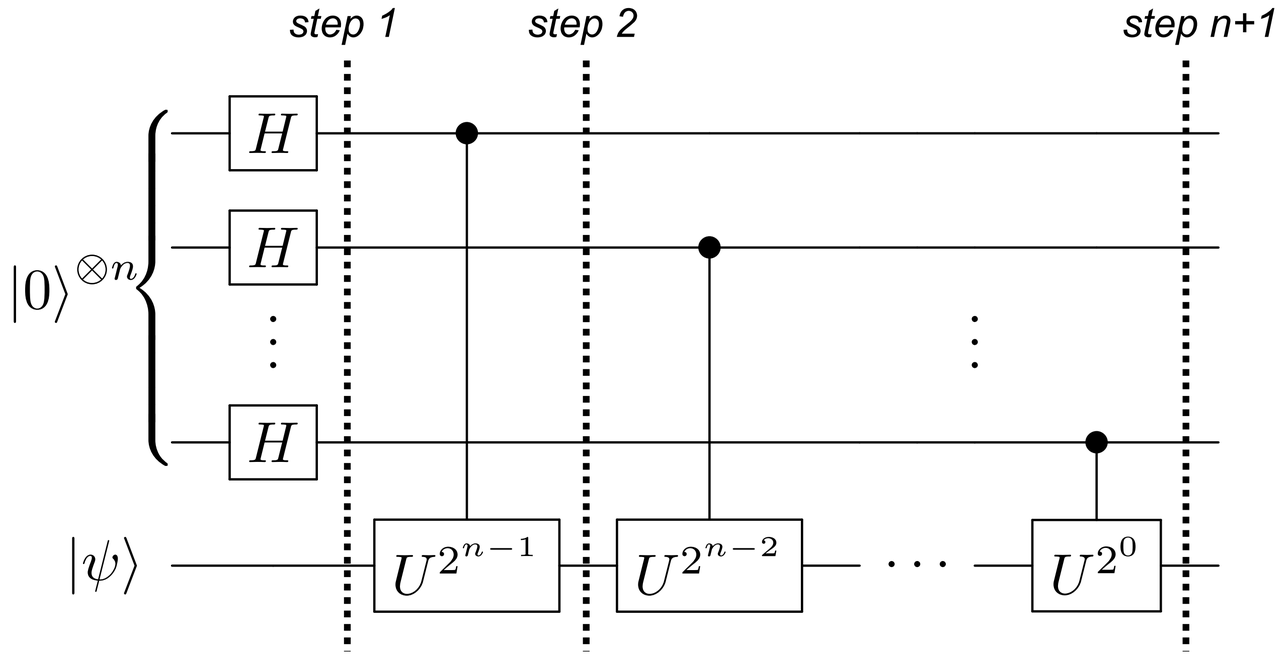
$$|\psi\rangle = c_+|\phi_+\rangle + c_-|\phi_-\rangle \quad (c_\pm \in \mathbb{C})$$

➡ After measuring the first qubit, $|\psi\rangle$ becomes an eigenstate depending on the measurement outcome

$$|\psi\rangle \to |\psi'\rangle = c_+|\phi_+\rangle \text{ for } m = 0 \text{ or } c_-|\phi_-\rangle \text{ for } m = 1$$

Quantum Phase Estimation

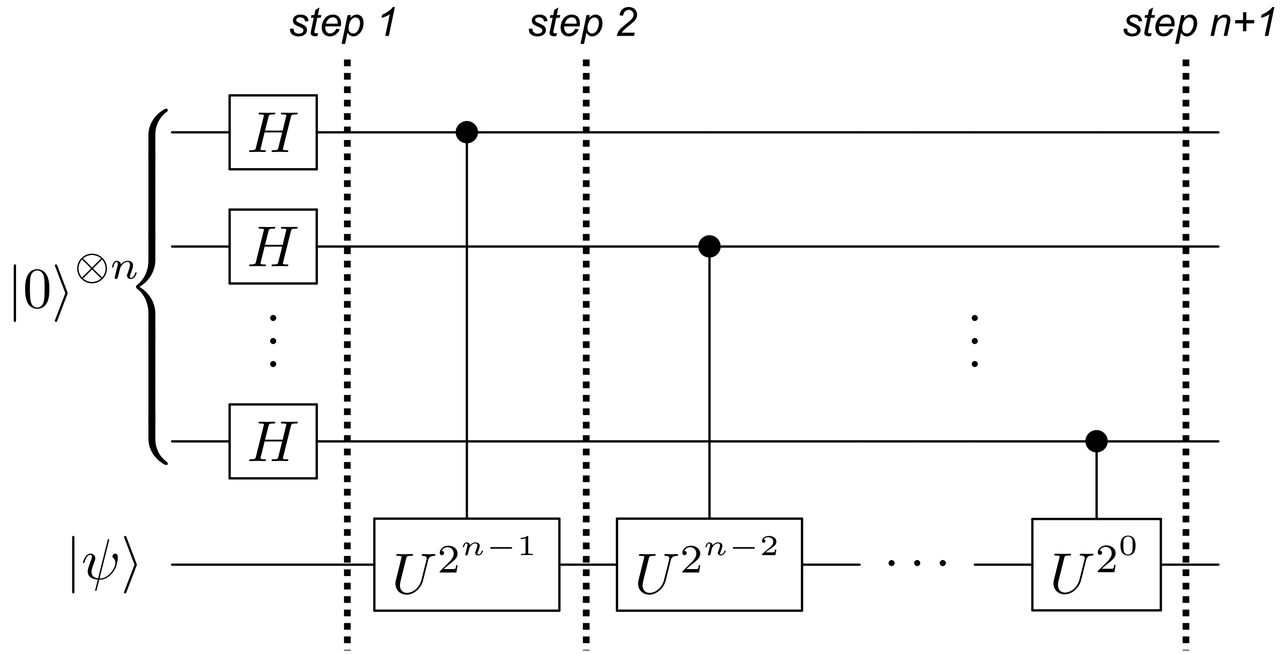
Extending to n-qubit QPE



Quantum Phase Estimation

Extending to n-qubit QPE

$$
\begin{aligned}
U^{2^x}|\psi\rangle &= U^{2^x-1}U|\psi\rangle \\
&= U^{2^x-1}e^{2\pi i\theta}|\psi\rangle \\
&= U^{2^x-2}e^{2\pi i\theta 2}|\psi\rangle \\
&= \cdots \\
&= e^{2\pi i\theta 2^x}|\psi\rangle
\end{aligned}
$$



step 1 $\dfrac{1}{\sqrt{2^n}}\left(|0\rangle|+|1\rangle\right)^{\otimes n}|\psi\rangle$

step 2 $\dfrac{1}{\sqrt{2^n}}\left(|0\rangle+e^{2\pi i\theta 2^{n-1}}|1\rangle\right)\left(|0\rangle+|1\rangle\right)^{\otimes n-1}|\psi\rangle$

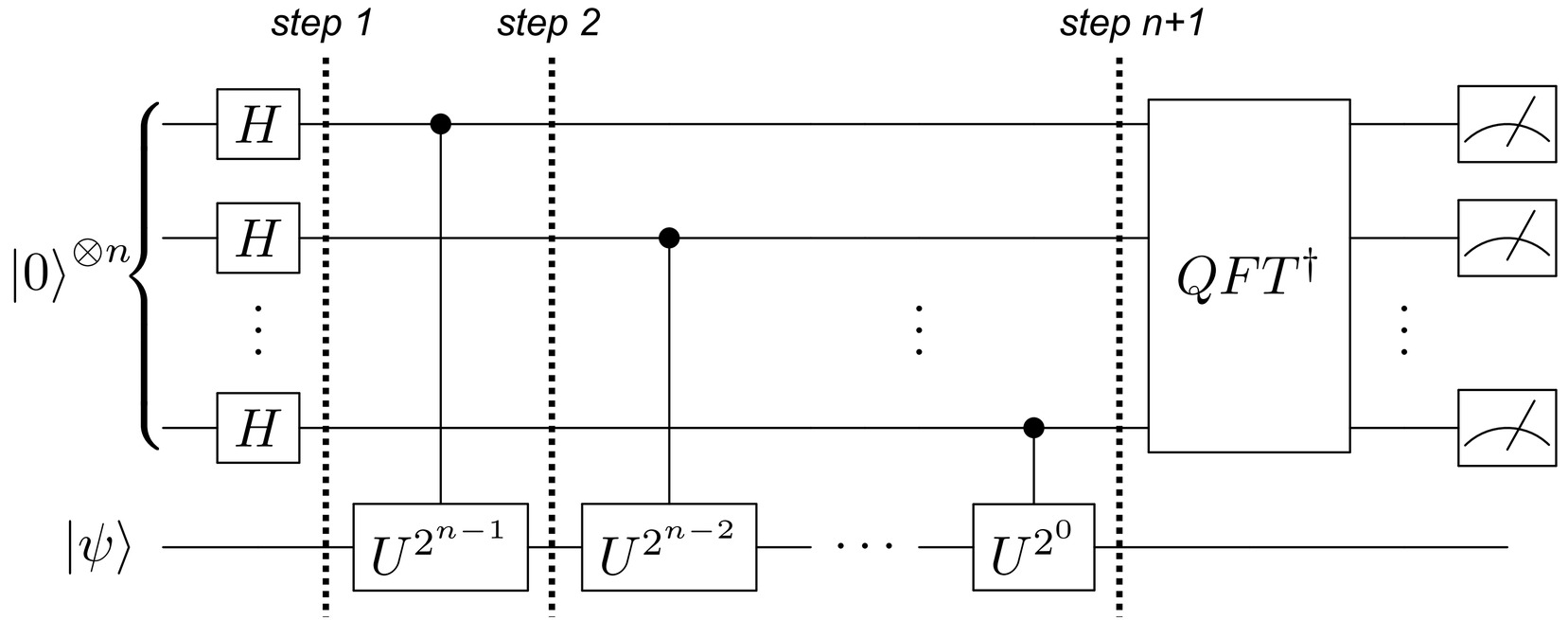
step n+1 $\dfrac{1}{\sqrt{2^n}}\left(|0\rangle+e^{2\pi i\theta 2^{n-1}}|1\rangle\right)\left(|0\rangle+e^{2\pi i\theta 2^{n-2}}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i\theta 2^{0}}|1\rangle\right)|\psi\rangle$

→ Equivalent to QFT with j replaced by $2^n\theta$

Quantum Phase Estimation

Extending to n-qubit QPE

$$
\begin{aligned}
U^{2^x}|\psi\rangle &= U^{2^x-1}U|\psi\rangle \\
&= U^{2^x-1}e^{2\pi i\theta}|\psi\rangle \\
&= U^{2^x-2}e^{2\pi i\theta 2}|\psi\rangle \\
&= \cdots \\
&= e^{2\pi i\theta 2^x}|\psi\rangle
\end{aligned}
$$



step 1 $\frac{1}{\sqrt{2^n}}\left(|0\rangle|+|1\rangle\right)^{\otimes n}|\psi\rangle$

step 2 $\frac{1}{\sqrt{2^n}}\left(|0\rangle+e^{2\pi i\theta 2^{n-1}}|1\rangle\right)\left(|0\rangle+|1\rangle\right)^{\otimes n-1}|\psi\rangle$

step n+1 $\frac{1}{\sqrt{2^n}}\left(|0\rangle+e^{2\pi i\theta 2^{n-1}}|1\rangle\right)\left(|0\rangle+e^{2\pi i\theta 2^{n-2}}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i\theta 2^{0}}|1\rangle\right)|\psi\rangle$

→ Equivalent to QFT with j replaced by $2^n\theta$

➡ Can obtain $|2^n\theta\rangle$ by inverse QFT

➔ Measure the circuit output to get $2^n\theta$!!

Precision improved with increasing number of qubits, though so does the computational cost

Hands-on Exercise (II)

- Quantum Fourier Transform
- Addition by QFT
- Quantum Phase Estimation

More details on circuit building, transpilation, error mitigations, etc. at IBM Quantum Learning page, e.g, overview of how to use Qiskit

Backup

Shor's Algorithm

Shor's algorithm Peter Shor, 1994

- Factorize a positive composite number N into two prime numbers
- No <u>efficient</u> factorization algorithm is known in classical computation

  Computational resource increasing exponentially in $N \sim \exp\left[\Theta(N^{1/3}(\log N)^{2/3}\right]$

- Shor's algorithm can solve the problem in a polynomial resource $\sim \mathcal{O}\left(N^2(\log N)(\log\log N)]\right)$

  ➡ Exponential speed-up!

<u>Nielsen & Chuang</u>

Security of RSA cryptosystem based on the difficulty of prime factorization

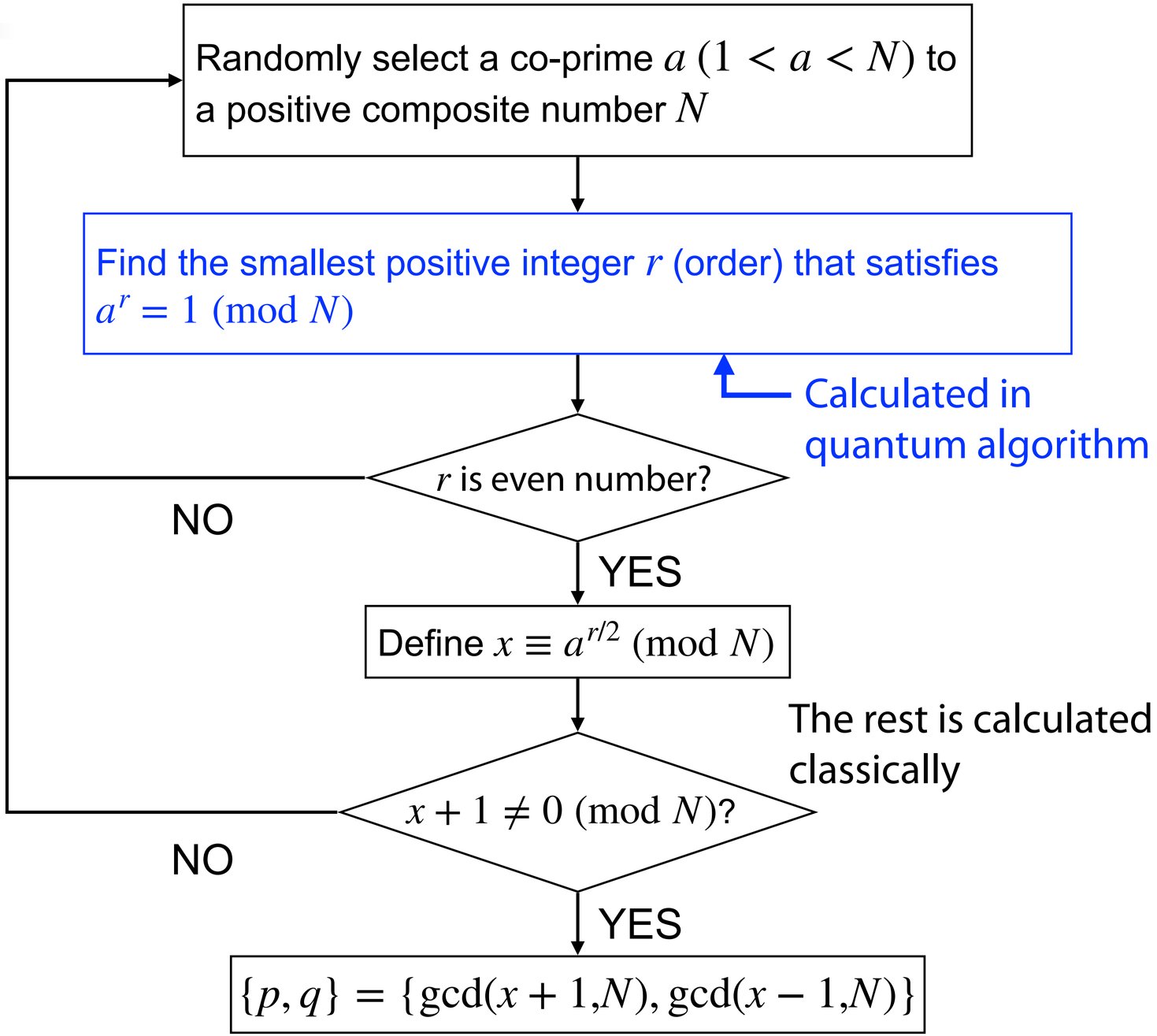
Shor's Algorithm

Factorize a positive composite number N into primes $N = pq$?

If y is a remainder of dividing an integer x by 3

x	0	1	2	3	4	5	6	…
y	0	1	2	0	1	2	0	…

➡ $x = y \pmod 3$



An Example

Factorization of $N = 15$

$15 = [1111]$ (4-bit integer)

For example, if we take $a = 7$

x	0	1	2	3	4	5	6	…
$7^x \pmod{15}$	1	7	4	13	1	7	4	…

Smallest integer r that satisfies

$7^r = 1 \pmod{15}$ ➡ $r = 4$

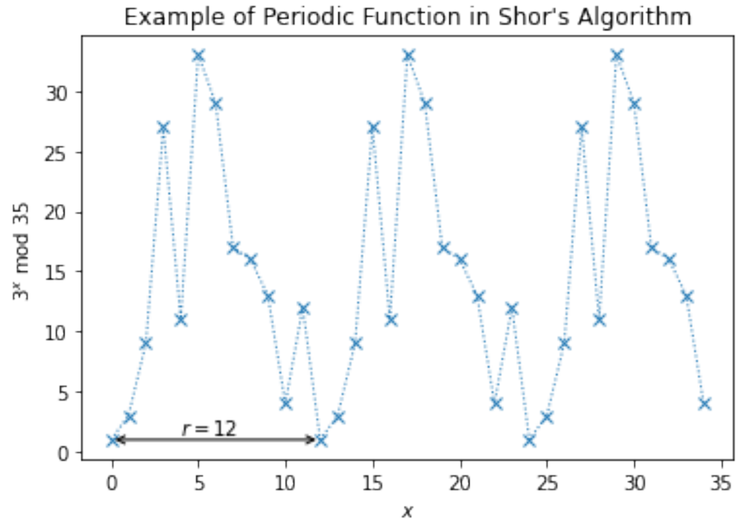
$x \equiv 7^{4/2} \pmod{15} = 4$

$x + 1 = 5 \neq 0 \pmod{15}$, therefore

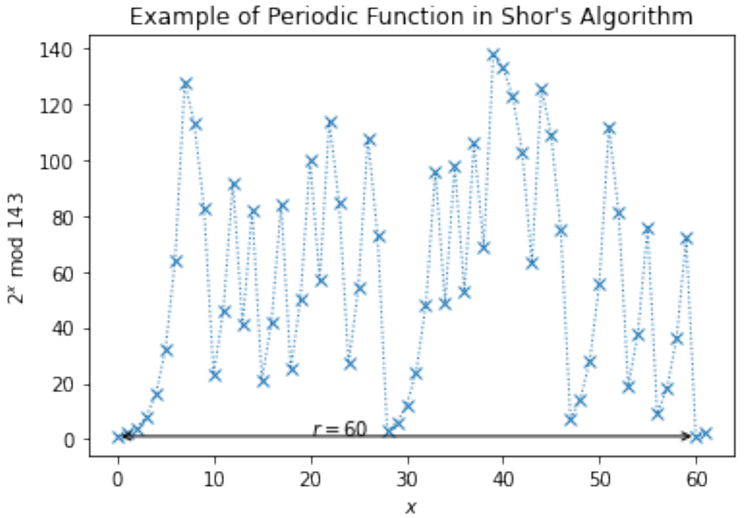
$\{p, q\} = \{\gcd(5,15), \gcd(3,15)\} = \{5,3\}$

➡ 5 and 3!!

Why is the problem "Find the smallest positive integer (order) that satisfies $a^r = 1 \pmod{N}$" so difficult?



$3^x \pmod{35}$

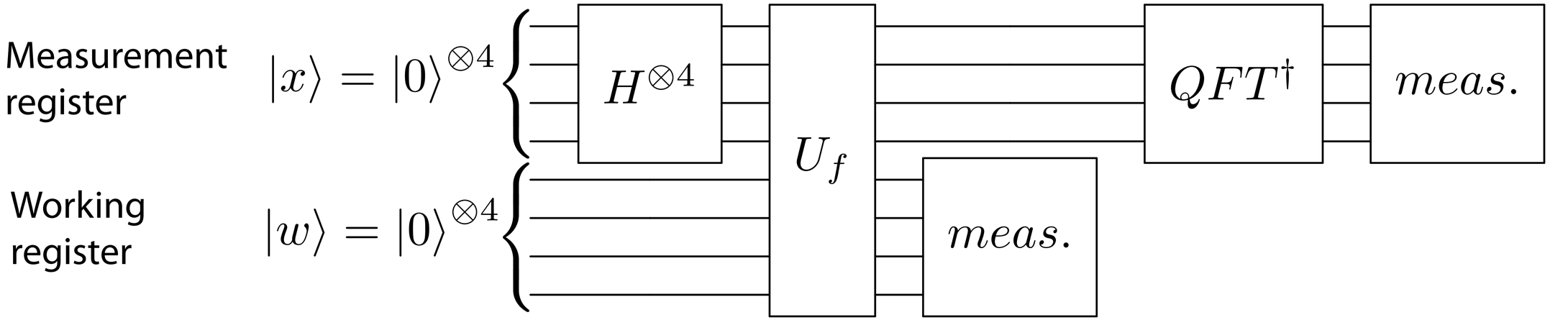


$2^x \pmod{143}$

Finding period is getting more difficult as the number becomes larger

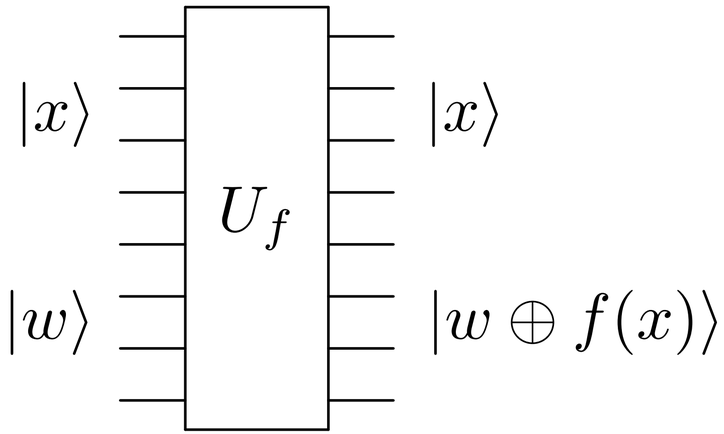
Quantum Circuit for Shor's Algorithm

Quantum circuit for factorization of $N = 15$



Oracle for $|x\rangle|w\rangle \rightarrow |x\rangle|w \oplus f(x)\rangle$

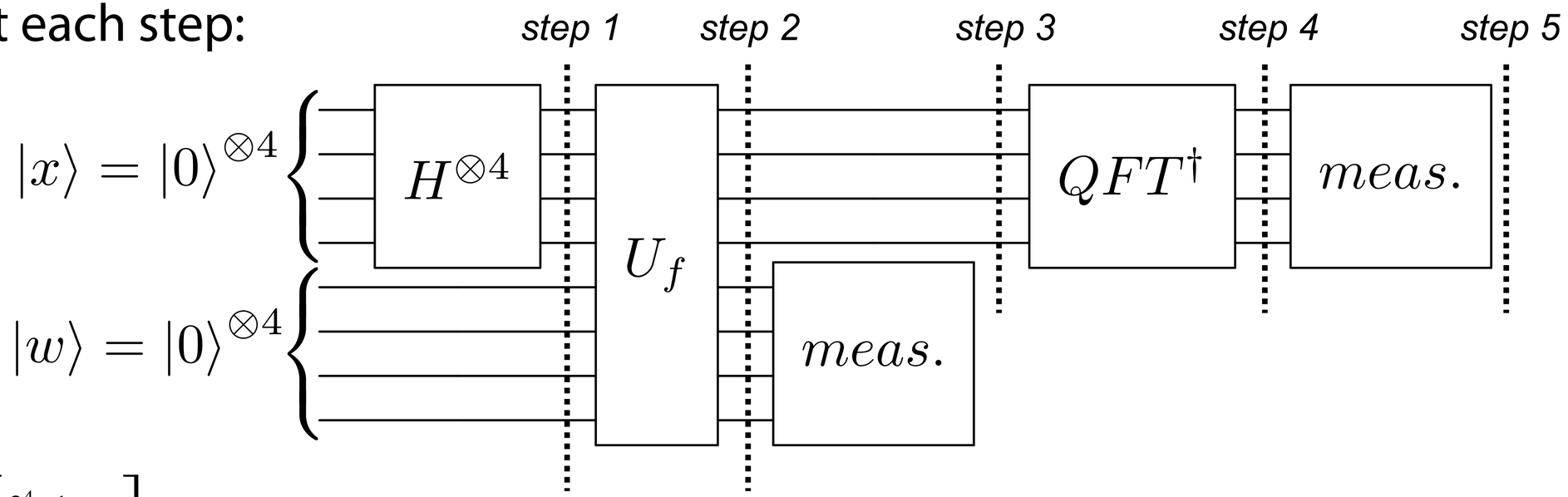
$f(x) \equiv a^x \pmod N$



Utilizing quantum parallelism with superposition states

Quantum Circuit for Shor's Algorithm

Quantum states at each step:



step 1 $$\frac{1}{\sqrt{2^4}}\left[\sum_{j=0}^{2^4-1}|j\rangle\right]|0\rangle^{\otimes 4} = \frac{1}{4}\left[|0\rangle + |1\rangle + |2\rangle + \cdots + |15\rangle\right]|0\rangle^{\otimes 4}$$

step 2 $$\frac{1}{4}\left[|0\rangle|0 \oplus 7^0 \,(\mathrm{mod}15)\rangle + |1\rangle|0 \oplus 7^1 \,(\mathrm{mod}15)\rangle + \cdots + |15\rangle|0 \oplus 7^{15} \,(\mathrm{mod}15)\rangle\right]$$

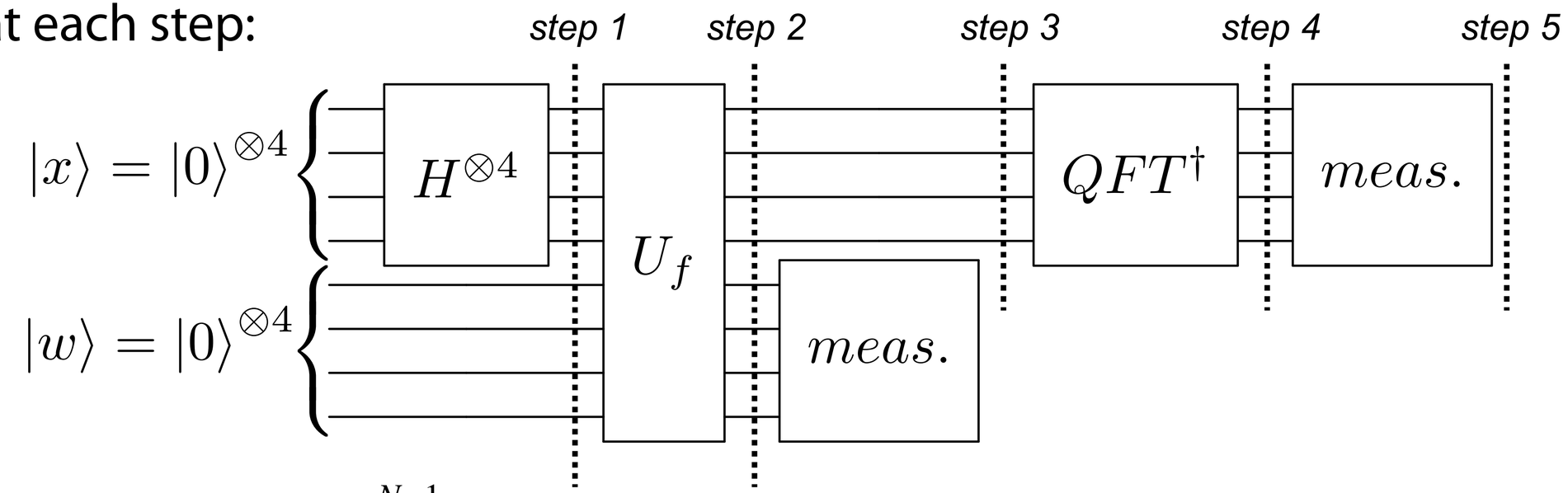
$$= \frac{1}{4}\left[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + \cdots + |15\rangle|13\rangle\right]$$

For example, if we get 13 by measuring the working register w

step 3 $$= \frac{1}{2}\left[|3\rangle + |7\rangle + |11\rangle + |15\rangle\right]$$

Quantum Circuit for Shor's Algorithm

Quantum states at each step:



Applying inverse QFT : $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{-2\pi ijk}{N}} |k\rangle$

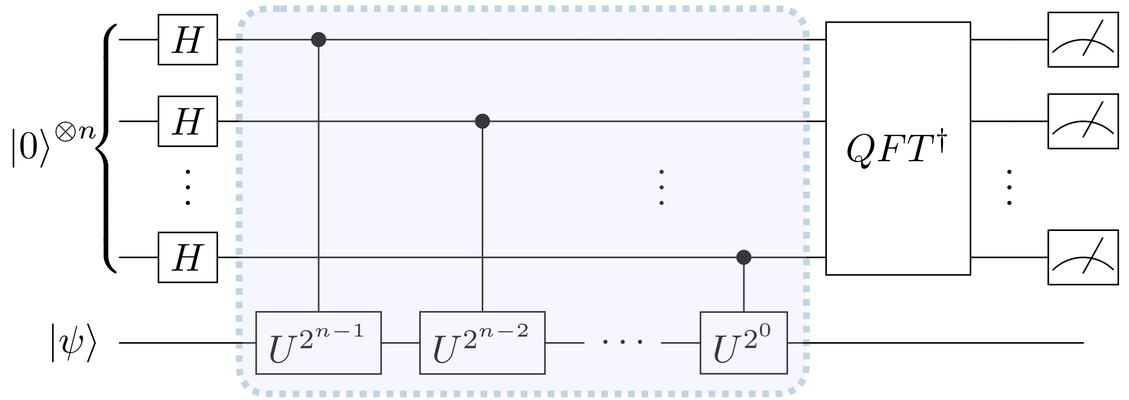
step 4 $= \frac{1}{2} QFT^\dagger \left[|3\rangle + |7\rangle + |11\rangle + |15\rangle \right] = \frac{1}{2} \frac{1}{\sqrt{2^4}} \sum_{k=0}^{2^4-1} \left[e^{\frac{-2\pi i \cdot 3k}{2^4}} + e^{\frac{-2\pi i \cdot 7k}{2^4}} + e^{\frac{-2\pi i \cdot 11k}{2^4}} + e^{\frac{-2\pi i \cdot 15k}{2^4}} \right] |k\rangle$

$= \frac{1}{8} \left[4|0\rangle + 4i|4\rangle - 4|8\rangle - 4i|12\rangle \right]$

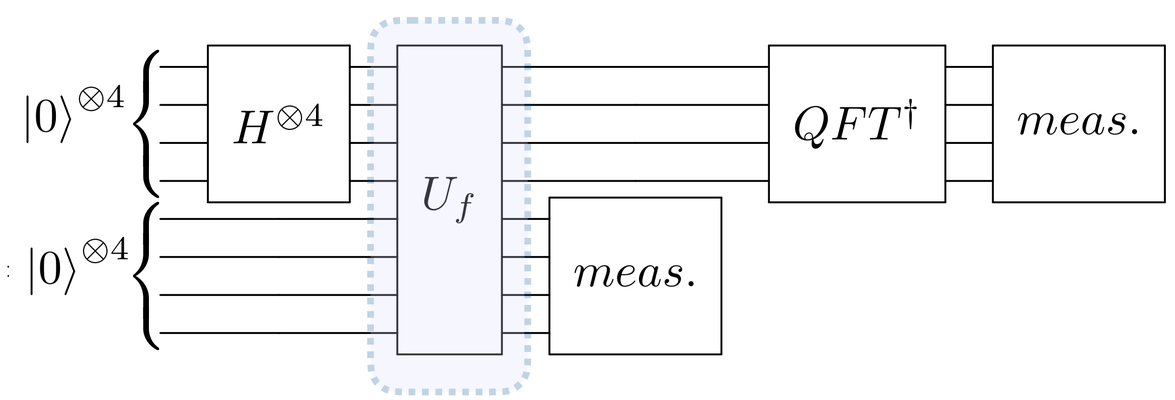
step 5 Measuring the measurement register x, we will get 0, 4, 8 and 12 each with probability 1/4

Quantum Circuit for Shor's Algorithm

Circuit of Quantum Phase Estimation



Circuit of Shor's algorithm (order finding)



Similarity to QPE circuit ➡

If the Oracle U_f of Shor's circuit is designed to work the same as in QPE circuit,

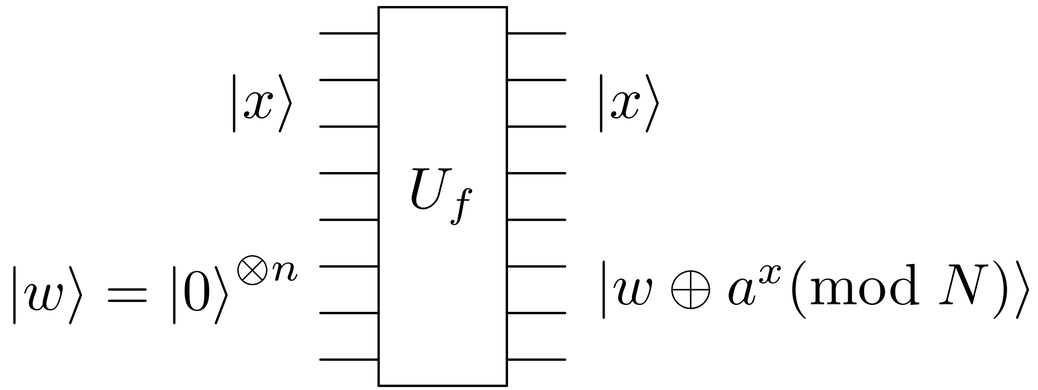
we will get $2^n\theta$ by measuring the measurement register ($n = 4$、θ is the phase of eigenvalue $e^{2\pi i\theta}$)

For example, if we get 4, the phase value is $\theta = 4/2^n = 0.25$

➞ What does this phase mean?

Implementation of Order-Finding Circuit

We have considered the following circuit to implement Shor's order-finding algorithm



The Oracle can be implemented with the unitary U:

$$U|m\rangle = \begin{cases} |am \pmod N\rangle & 0 \le m \le N-1 \\ |m\rangle & N \le m \le 2^n - 1 \end{cases}$$

$$U|1\rangle = |a \pmod N\rangle$$

$$\Rightarrow U_f|x\rangle|0\rangle = |x\rangle|a^x \pmod N\rangle$$

$$= U^x|x\rangle|1\rangle$$

With the following state $|\psi_s\rangle$:

$$|\psi_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} |a^k \pmod N\rangle$$

(s is an integer within $0 < s < r-1$)

$$\Rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle$$

$\Rightarrow |\psi_s\rangle$ is the eigenvector of U with the eigenvalue $e^{2\pi is/r}$

$$U|\psi_s\rangle = e^{2\pi is/r}|\psi_s\rangle$$

Orcale U_f for Shor's order-finding algorithm

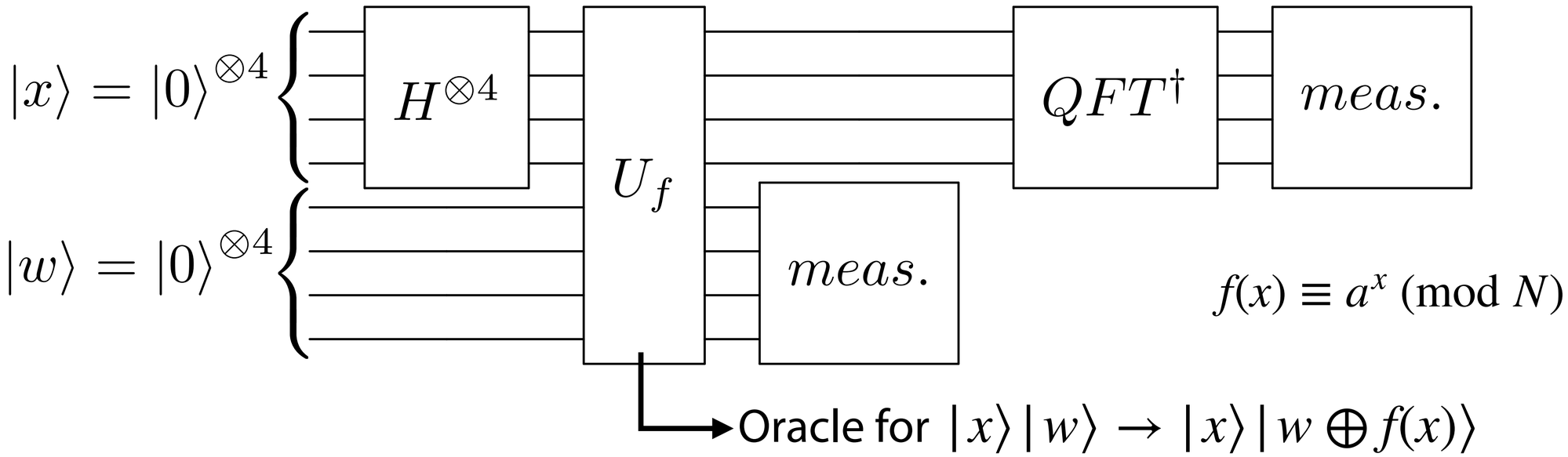
➡ Equivalent to applying U x times to $|1\rangle$, which is the superposition of $|\psi_s\rangle$ with eigenvalue $e^{2\pi is/r}$

Phase obtained by Shor's order finding

➡ (Integer multiples of) s/r

Summary of Order-Finding Circuit

Quantum circuit for factorization of $N = 15$

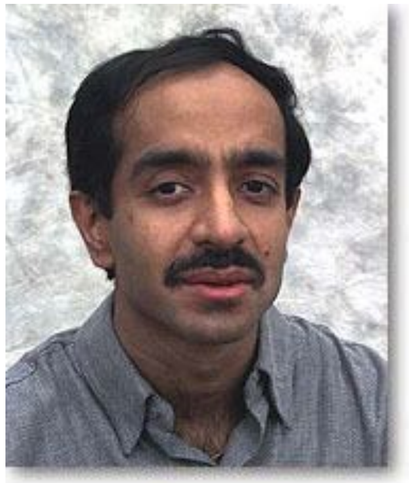


Phase obtained by measuring the measurement register = (Integer multiples of) s/r

The rest of Shor's algorithm is carried out using classical computation

Analyze the measured result using *continued fraction expansion* to get the fraction s/r, which is the closest to phase θ, and obtain the order r

Grover's Algorithm



Grover's algorithm Lov Grover, 1996

- Search for element in unstructured (non-indexed) database
- Classical search requires full scan, thus computational cost growing linearly in N (number of elements)
- Grover's algorithm enables to solve the same problem with $\mathcal{O}(\sqrt{N})$ cost
  - ➡ Quadratic speed-up （theoretically proved）

Very popular subroutine to enhance amplitudes for certain quantum states

Preparation

Consider an oracle of phase flip : $U|x\rangle = (-1)^{f(x)}|x\rangle$

$$f(x) = \begin{cases} 1 & \text{if } x = w \\ 0 & \text{else} \end{cases}$$

Oracle U_w to flip phase of the solution w

$$U_w : |w\rangle \to -|w\rangle \qquad |x\rangle \to |x\rangle \;\; \forall x \neq w \quad \Rightarrow \quad U_w = I - 2|w\rangle\langle w|$$

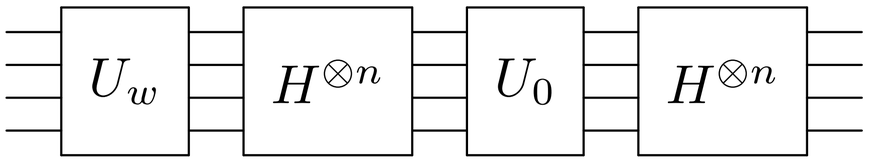
$$f_0(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{else} \end{cases}$$

Unitary U_0 to flip phase of non-0 states

$$U_0 : |0\rangle^{\otimes n} \to |0\rangle^{\otimes n} \qquad |x\rangle \to -|x\rangle \;\; \forall x \neq 0 \quad \Rightarrow \quad U_0 = 2|0\rangle\langle 0|^{\otimes n} - I$$

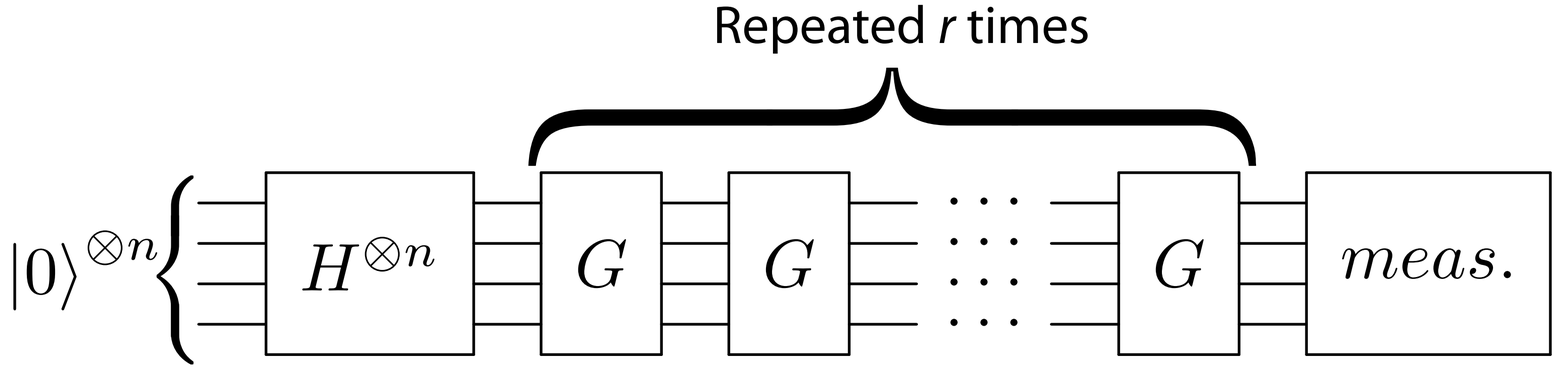
Quantum circuit for Grover's algorithm

$G =$



➡ Called Grover iteration

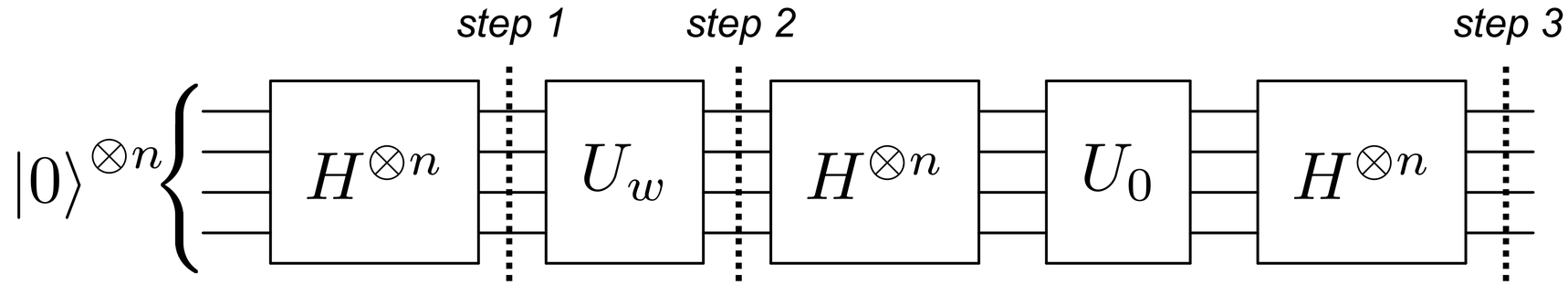
Repeated *r* times



Quantum Circuit for Grover's Algorithm

Consider the case of finding a single solution w in a database of $N(=2^n)$ data

A single Grover iteration circuit



step 1 $|s\rangle := H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

Geometrically represent $|s\rangle$ to understand by intuition

➡ Consider in 2-dimensional space spanned by the solution state $|w\rangle$ and its orthogonal state $|w^{\perp}\rangle$

Define $|w\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ $|w^{\perp}\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq w}|x\rangle = \begin{bmatrix}1\\0\end{bmatrix}$

Superposition state $|s\rangle$ represented as

$$|s\rangle = \sqrt{\frac{N-1}{N}}|w^{\perp}\rangle + \sqrt{\frac{1}{N}}|w\rangle$$

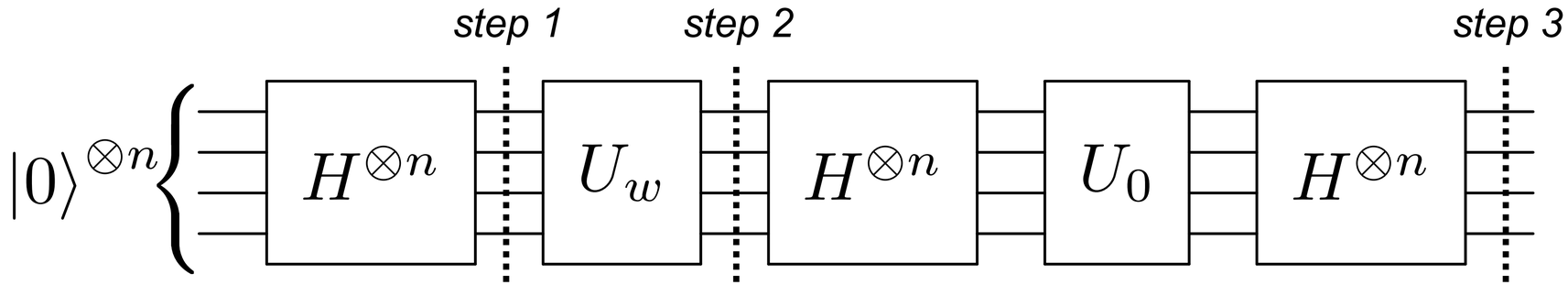
$$=: \cos\frac{\theta}{2}|w^{\perp}\rangle + \sin\frac{\theta}{2}|w\rangle = \begin{bmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{bmatrix}$$

$$\theta = 2\arcsin\frac{1}{\sqrt{N}}$$

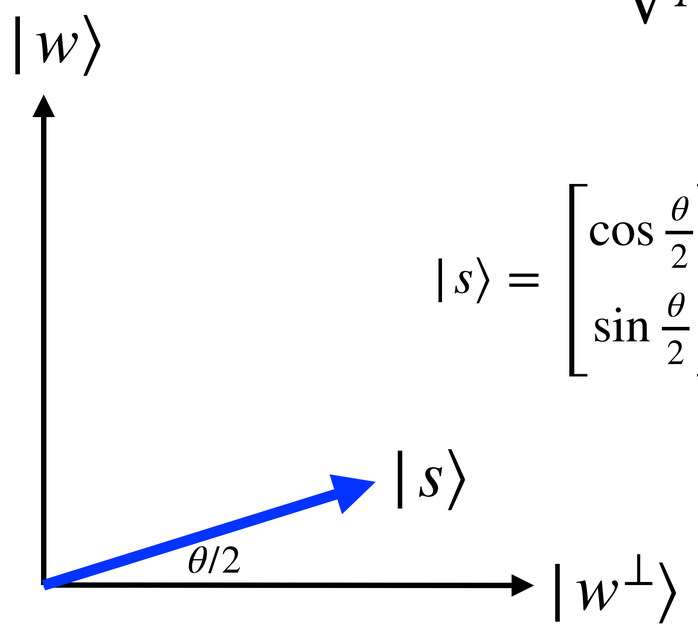
Quantum Circuit for Grover's Algorithm

Consider the case of finding a single solution w in a database of $N(=2^n)$ data

A single Grover iteration circuit



step 1 $|s\rangle := H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

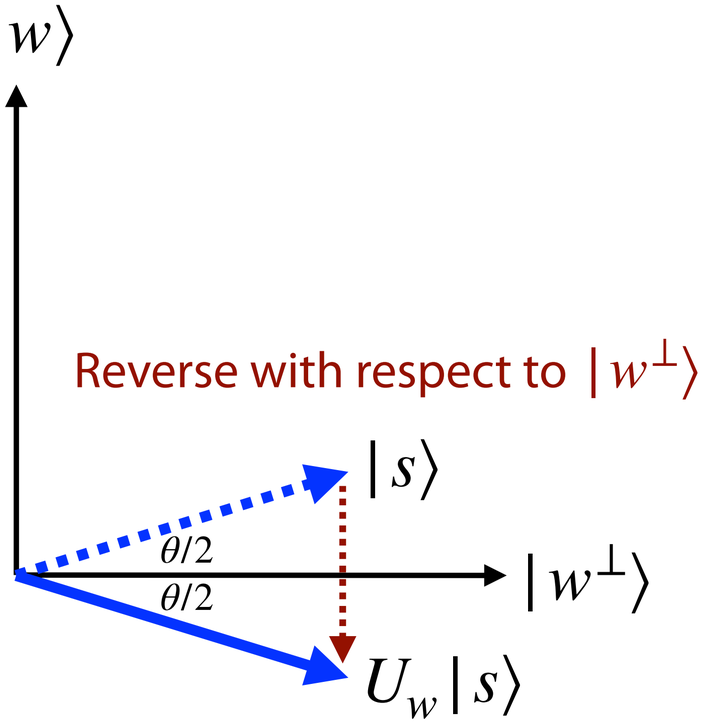


$$|s\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{bmatrix}$$

step 2

$$U_w = I - 2|w\rangle\langle w| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

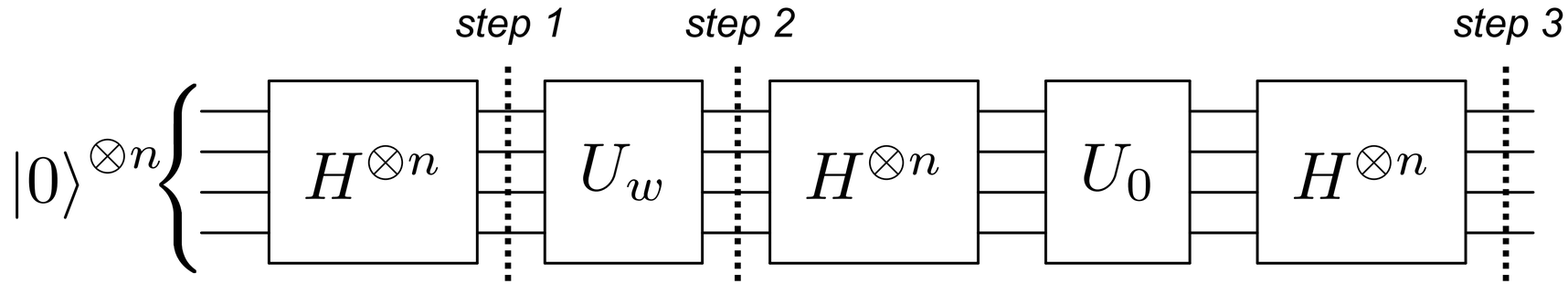
$$U_w|s\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ -\sin\frac{\theta}{2} \end{bmatrix}$$



Quantum Circuit for Grover's Algorithm

Consider the case of finding a single solution w in a database of $N(=2^n)$ data

A single Grover iteration circuit



$$U_0 = 2|0\rangle\langle 0|^{\otimes n} - I$$

Define $U_s = H^{\otimes n} U_0 H^{\otimes n}$

$$U_s = 2(H^{\otimes n}|0\rangle^{\otimes n})(\langle 0|^{\otimes n} H^{\otimes n}) - H^{\otimes n} H^{\otimes n}$$

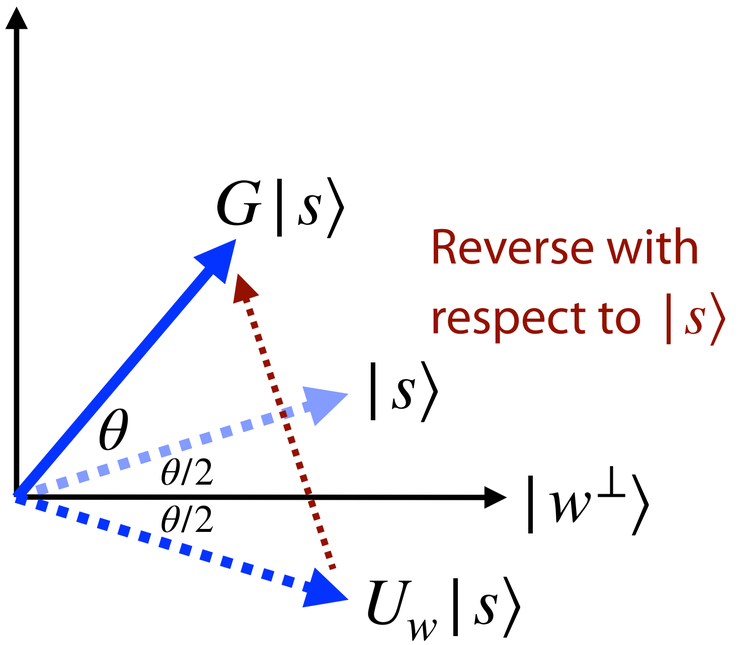
$$= 2|s\rangle\langle s| - I$$

$$= \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

step 3 $U_s U_w |s\rangle = \begin{bmatrix} \cos\frac{3}{2}\theta \\ \sin\frac{3}{2}\theta \end{bmatrix}$

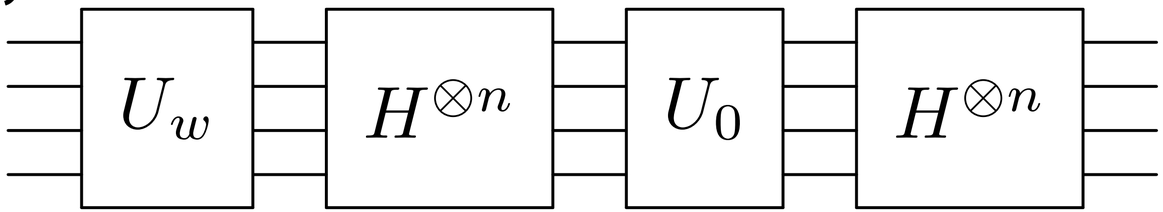
$$U_s U_w = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

→ Rotation of angle θ



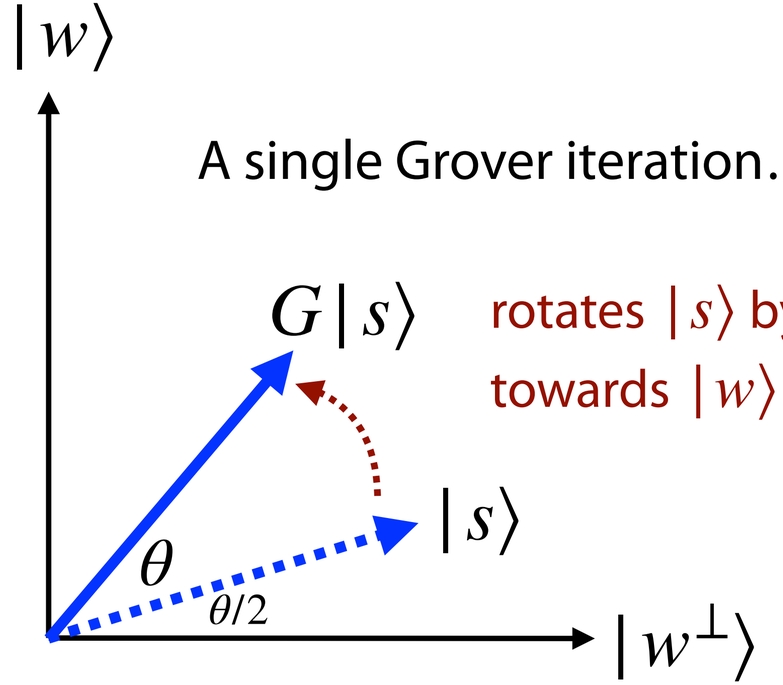
Quantum Circuit for Grover's Algorithm

In summary

$G =$ 

$$G = U_s U_w = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

A state after applying the G r times $\quad G^r |s\rangle = \begin{bmatrix} \cos\frac{2r+1}{2}\theta \\ \sin\frac{2r+1}{2}\theta \end{bmatrix}$



A single Grover iteration…

$G|s\rangle$ rotates $|s\rangle$ by θ towards $|w\rangle$

➡ In order to reach $|w\rangle$,

need to rotate r times so that $\frac{2r+1}{2}\theta \approx \frac{\pi}{2}$

If θ is small enough, $\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \approx \frac{\theta}{2}$

➡ $r \approx \frac{\pi}{4}\sqrt{N}$

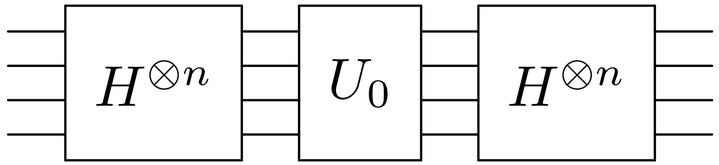
Reach the solution w by $\mathcal{O}(\sqrt{N})$ operations!!

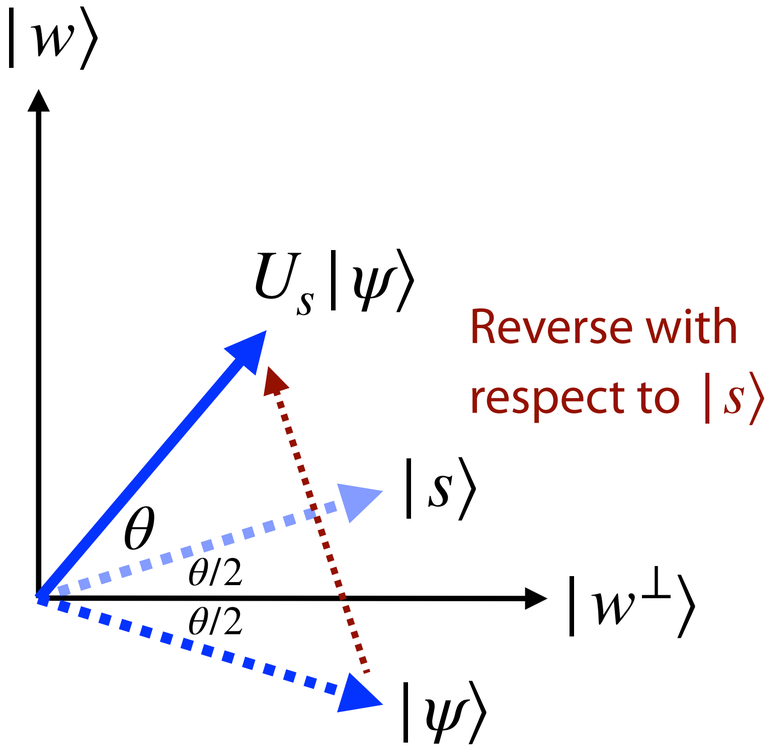
Diffuser

$U_s = H^{\otimes n} U_0 H^{\otimes n} = 2|s\rangle\langle s| - I$ is called **Diffuser**

$U_0 = 2|0\rangle\langle 0|^{\otimes n} - I$

U_s =





Expanding $|\psi\rangle$ with some bases $|\psi\rangle := \sum_k a_k |k\rangle$

$$(2|s\rangle\langle s| - I)|\psi\rangle = \frac{2}{N}\sum_i |i\rangle \cdot \sum_{j,k} a_k \langle j|k\rangle - \sum_k a_k |k\rangle$$

$$= 2\frac{\sum_i a_i}{N}\sum_k |k\rangle - \sum_k a_k |k\rangle$$

$$= \sum_k (2\langle a\rangle - a_k)|k\rangle \qquad \langle a\rangle \equiv \frac{\sum_i a_i}{N}$$

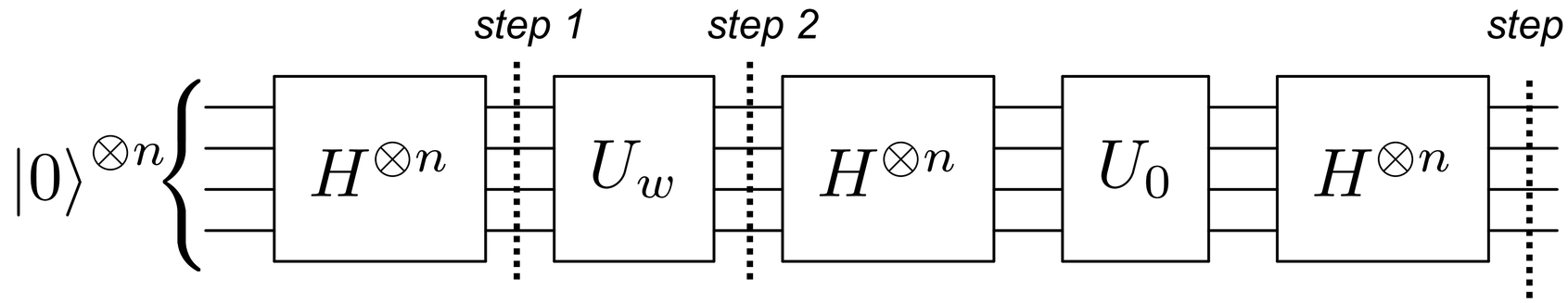
If a_k is represented as $a_k = \langle a\rangle - \Delta$, then

$2\langle a\rangle - a_k = \langle a\rangle + \Delta$

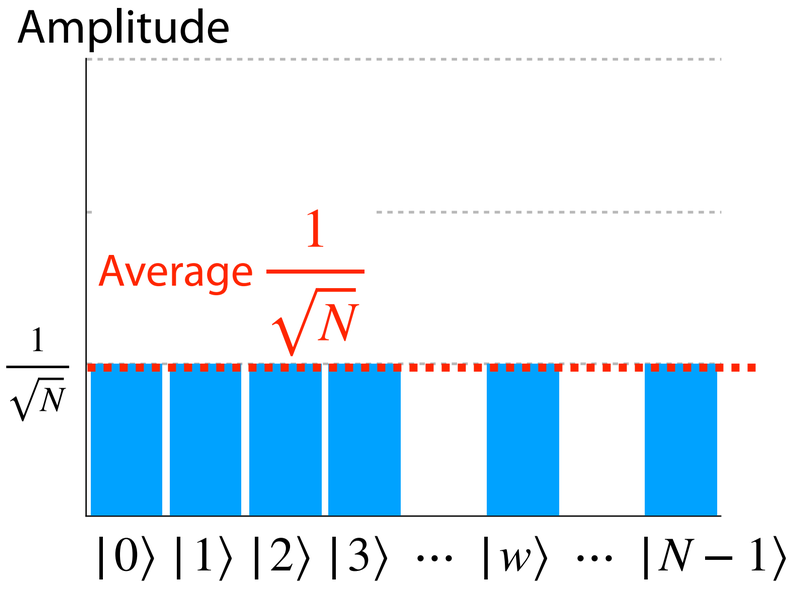
➡ Reversing with respect to the average $\langle a\rangle$

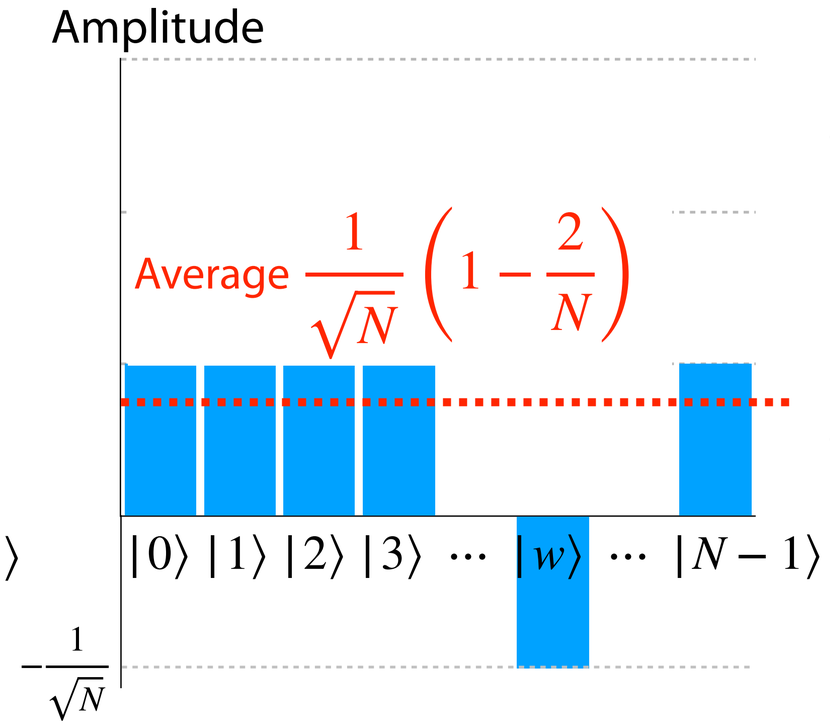
Amplitude Amplification

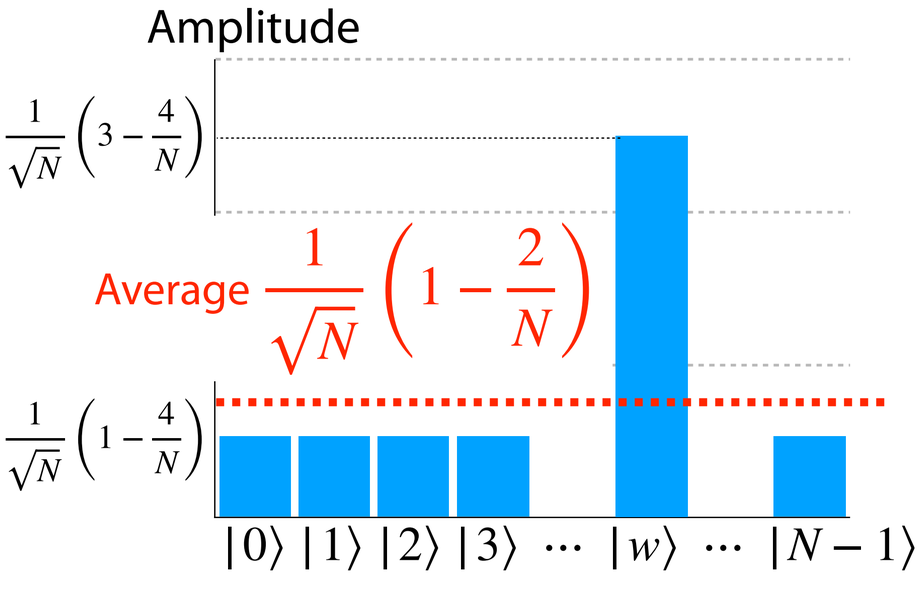
A single Grover iteration circuit



step 1 Create superposition states → *step 2* Reverse a solution state → *step 3* Reverse all states with respect to the average







Amplitude of solution state increases by repeating G