Quantum Computation

Dr. Yangjun Chen

- What is a qubit?
- Bloch sphere interpretation
- About $e^{i\theta}$
- Qubit operators and circuits
- Quantum Fourier Transformation

Sept. 2023

What is a qubit?

- **In classical compuation, the fundamental concept is *bit*. A bit *b* can take one of two values 0 or 1.**
- **In quantom computation, the fundamental concept is quantom bit, *called* qubit, whose *superposition* is**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

where $|0\rangle$ represents the 0-state and $|1\rangle$ 1-state of a quantom bit. α and β are two complex numbers, satisfying $|\alpha|^2 + |\beta|^2$.

- **Assume that $\alpha = a + ib$. Then,** $|\alpha| = \sqrt{a^2 + b^2}$

called the *absolute value* (or *modulus*, or *magnitude*) of α.

What is a qubit?

Interpretation of superposition:

When the qubit is measured, the probability that its value is $|0\rangle$ is $|\alpha|^2$ and the probability that its value is $|1\rangle$ is $|\beta|^2$.

Qubit Visualization

Bloch Sphere

- **We can write $\alpha = re^{i\gamma}$ and $\beta = pe^{i\omega}$. Then, we have**

$$|\psi\rangle = re^{i\gamma}|0\rangle + pe^{i\omega}|1\rangle. \qquad (2)$$

- **Mupltiplying either side of the above equation by $e^{-i\gamma}$, we get**

$$e^{-i\gamma}|\psi\rangle = r|0\rangle + pe^{i(\omega-\gamma)}|1\rangle. \qquad (3)$$

- **Denote $e^{-i\gamma}|\psi\rangle$ by $|\psi'\rangle$, and $(\omega - \gamma)$ by φ. We can rewrite (3) as**

$$|\psi'\rangle = r|0\rangle + pe^{i\varphi}|1\rangle \qquad (4)$$

Qubit Visualization

Bloch Sphere

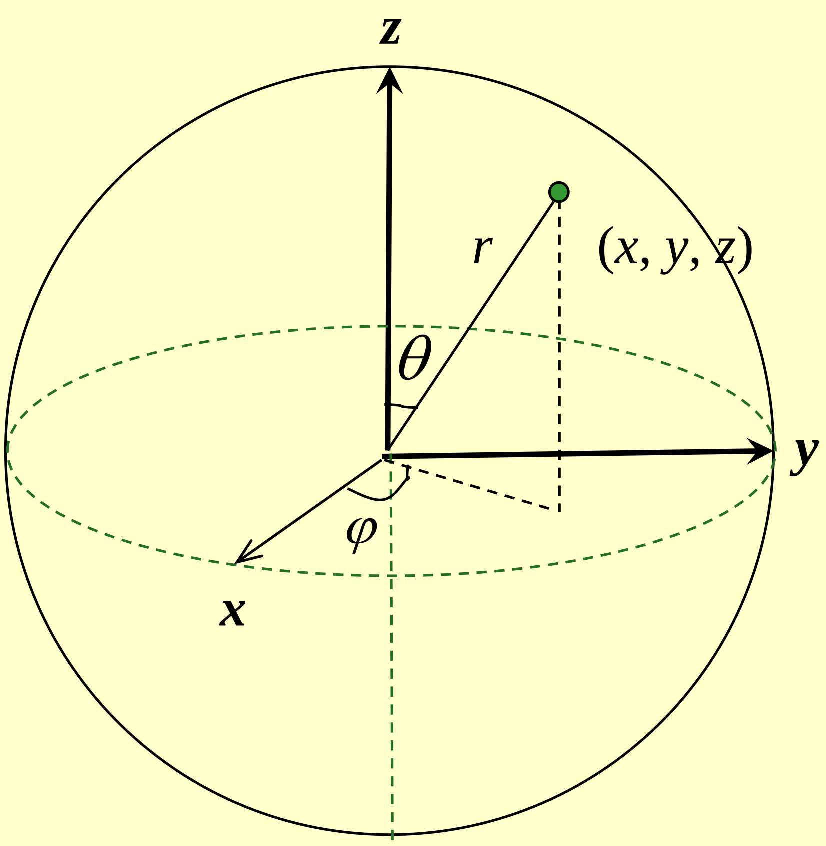
- **Rewriting $pe^{i\varphi}|1\rangle$ as $(x + iy)|1\rangle$ and renaming r as z, we have**

  $$|\psi'\rangle = z|0\rangle + (x + iy)|1\rangle, \qquad (5)$$

  satisfying $x^2 + y^2 + z^2 = 1$.

  From (5), we can see that the state of $|\psi'\rangle$ is completely determined by three values, x, y, and z.

Qubit Visualization



Cartesian coordinates are related to polar coordinates by the following equations:

$$x = r\sin(\theta)\sin(\varphi) \qquad (6)$$
$$y = r\sin(\theta)\cos(\varphi)$$
$$z = r\cos(\theta)$$

$$r = \sqrt{x^2 + y^2 + z^2}$$

For $r = 1$, we have

$$x = \sin(\theta)\sin(\varphi) \qquad (7)$$
$$y = \sin(\theta)\cos(\varphi)$$
$$z = \cos(\theta)$$

Qubit Visualization

- **In terms of (5) and (7), $|\psi'\rangle$ can be rewritten as follows:**

  $|\psi'\rangle = cos(\theta)|0\rangle + sin(\theta)(cos(\varphi) + isin(\varphi))|1\rangle.$ **(8)**

  $|\psi'\rangle = cos(\theta)|0\rangle + sin(\theta)e^{i\varphi}|1\rangle.$

- **Note that $\theta = 0 \Rightarrow |\psi'\rangle = |0\rangle$, $\theta = \pi/2 \Rightarrow |\psi'\rangle = |1\rangle$. This suggests that $0 \leq \theta \leq \pi/2$.**
- **We can map points on the upper hemisphere onto points on a sphere by defining**

  $\theta = \theta'/2 \Rightarrow \theta' = 2\theta$
- **Then, we now have**

  $|\psi'\rangle = cos(\theta'/2)|0\rangle + sin(\theta'/2)e^{i\varphi}|1\rangle.$ **(9)**

  with $0 \leq \theta' \leq \pi$, $0 \leq \varphi \leq 2\pi$, which are the coordinates of points on the Bloch sphere.

Qubit Visualization

- $|\psi'\rangle$ can be considered as a vector in a two-dimentional space V, in which two vectors

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

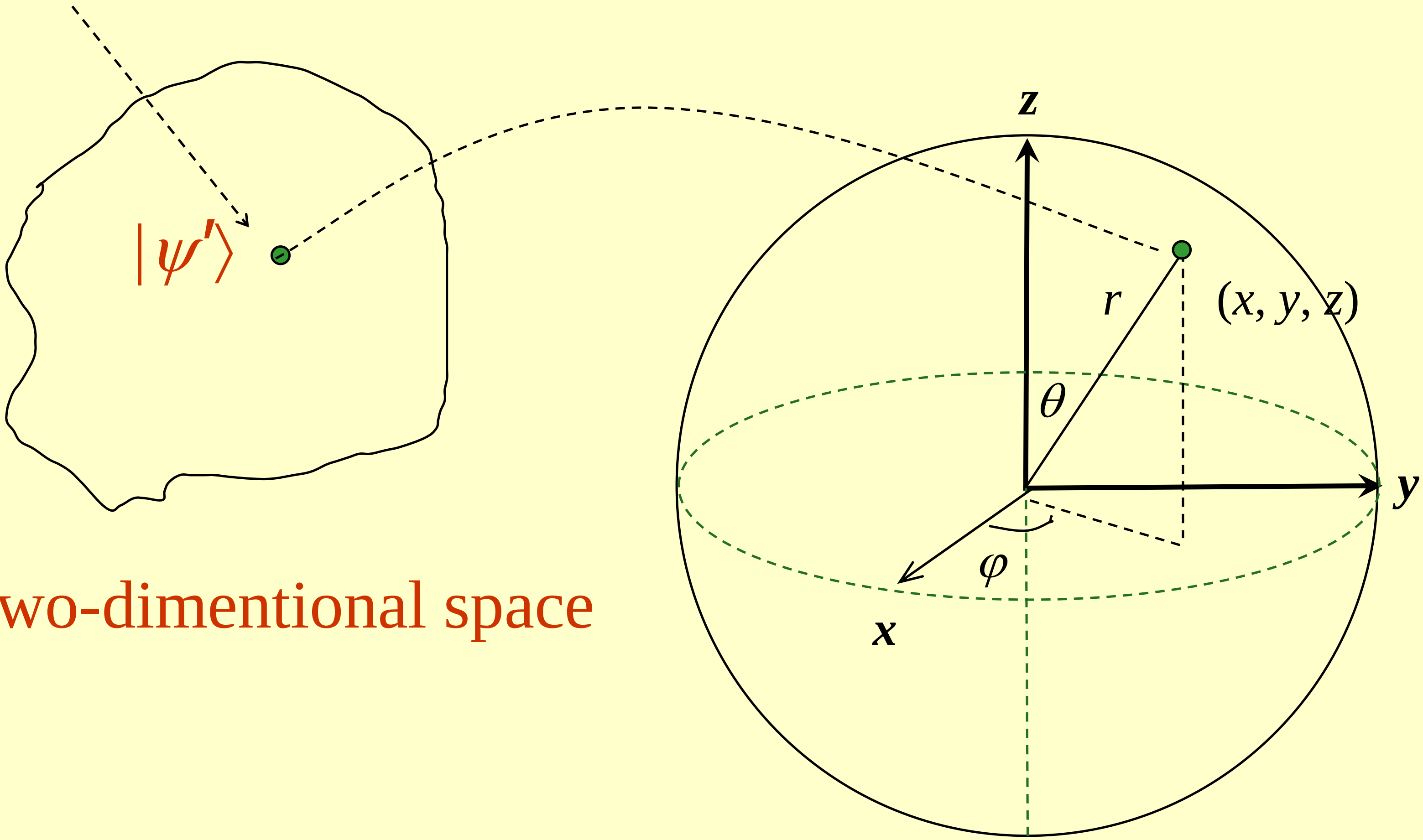
make up an orthonomal.

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|\psi'\rangle = \begin{pmatrix} cos(\frac{\theta'}{2}) \\ sin(\frac{\theta'}{2})e^{i\varphi} \end{pmatrix}$$

Qubit Visualization

a vector representing an qubit



two-dimentional space

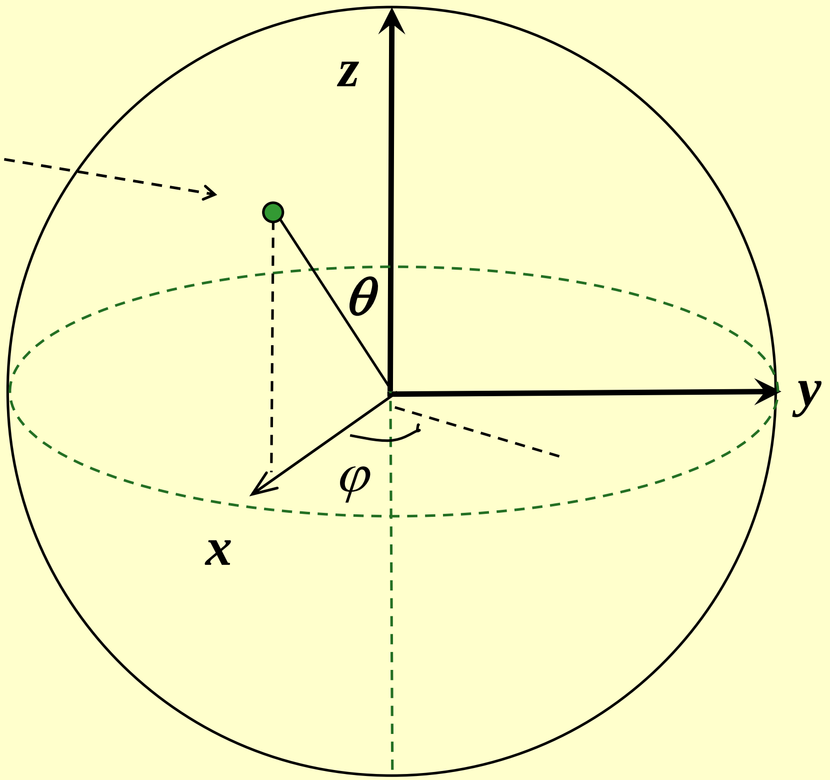
Qubit Visualization

$$|\psi'\rangle = \cos(\theta'/2)|0\rangle + \sin(\theta'/2)e^{i\varphi}|1\rangle$$

$$|0\rangle = \cos(0)|0\rangle + \sin(0)e^{i0}|1\rangle$$

$$\cos(\pi/4)|0\rangle + \sin(\pi/4)e^{i0}|1\rangle$$

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



$$|1\rangle = \cos(\pi)|0\rangle + \sin(\pi)e^{i0}|1\rangle$$

About $e^{i\varphi}$

- $e = \lim\limits_{n\to\infty} (1 + 1/n)^n$
- $e^{i\varphi} = \lim\limits_{n\to\infty} (1 + i\dfrac{\varphi}{m})^m$
- $e^{i\varphi} = cos(\varphi) + isin(\varphi)$

$$e^{i\varphi} = 1 + i\varphi - \frac{\varphi^2}{2!} - i\frac{\varphi^3}{3!} + \frac{\varphi^4}{4!} + i\frac{\varphi^5}{5!} \;\ldots\;\ldots$$

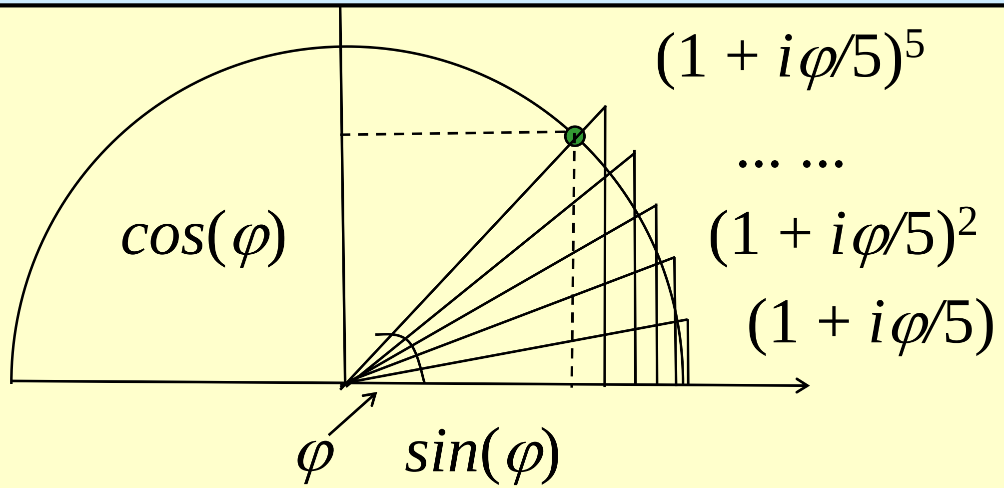
$$= (1 - \frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} \ldots) + i(\varphi - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!} \ldots)$$

$$= cos(\varphi) + isin(\varphi)$$

About $e^{i\varphi}$

- **Intuitive expalanation**

  Consider $(1 + i\varphi/5)^5$.



From the figure, we can see that as m increases,

$$(1 + i\frac{\varphi}{m})^m$$ gets closer to $cos(\varphi) + isin(\varphi)$.

Notations for basic operations

notation	description
z^*	Complex conjugate of the complex number z. $(1 + i)^* = 1 - i$
$\|\psi\rangle$	Vector. Also known as a *ket*. $\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle = (\alpha, \beta)^T$
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*. $\langle\psi\| = (\alpha^*, \beta^*)$
$\langle\psi\|\varphi\rangle$	Inner product between $\|\varphi\rangle$ and $\langle\|\psi$. Also known as *braket*. So $\langle\psi\|$ is called *bra* and $\|\varphi\rangle$ is called *ket*. For $\|\varphi\rangle = \alpha\|0\rangle + \beta\|1\rangle$ and $\langle\psi\| = (\alpha^*, \beta^*)$, $\langle\psi\|\varphi\rangle = (\alpha^*, \beta^*)(\alpha, \beta)^T = \alpha^*\alpha + \beta^*\beta$.
$\|\varphi\rangle\langle\psi\|$	Cartisian product between $\|\varphi\rangle$ and $\langle\psi\|$.
$\|\varphi\rangle\otimes\|\psi\rangle$	Tensor product between $\|\varphi\rangle$ and $\langle\psi\|$.
$\|\varphi\rangle\|\psi\rangle$	Abreviated notation for $\|\varphi\rangle\otimes\|\psi\rangle$, as also be written as $\|\varphi\psi\rangle$.
A^*	Complex conjugate of the matrix *A*.
A^T	Transpose of the matrix *A*.

Notations for basic operations

notation	description
A†	Hermitian conjugate or adjoint of the matrix A, A† = $(A^T)^*$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between A†$\|\varphi\rangle$ and $\|\psi\rangle$.

For $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$, we have

$$|\varphi\rangle\langle\psi| = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}(\alpha', \beta')^* = \begin{pmatrix}\alpha\alpha'^* & \alpha\beta'^* \\ \beta\alpha'^* & \beta\beta'^*\end{pmatrix} \qquad |\varphi\rangle\otimes\langle\psi| = \begin{pmatrix}\alpha\begin{pmatrix}\alpha' \\ \beta'\end{pmatrix} \\ \beta\begin{pmatrix}\alpha' \\ \beta'\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha\alpha' \\ \alpha\beta' \\ \beta\alpha' \\ \beta\beta'\end{pmatrix}$$

For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we have $A† = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.

- **Single qubits can be realized in many ways:**
  - **as the two different polarizations of a photon,**
  - **as the alignment of a nuclear spin in a uniform magnetic field,**
  - **as two states of an electron orbiting a single atom. The electron can exist in either the so-called 'ground' or 'excited' states, which we'll call $|0\rangle$ and $|1\rangle$, respectively. By shining light on the atom, with appropriate energy and for an appropriate length of time, it is possible to move the electron from the $|0\rangle$ state to the $|1\rangle$ state and vice versa.**
  - **Quantum wires are extremely narrow structures where electron transport is possible only in a very few transverse modes.**

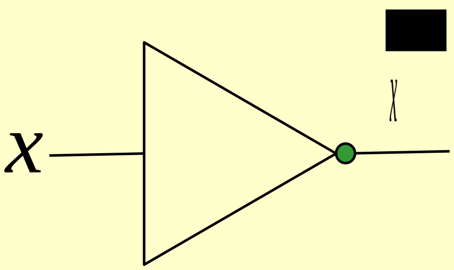
Single qubit operators

- A matrix U is called a unitary matrix if $U^\dagger U = I$. (I is an identity matrix.)
- Any (valid) single qubit operator is represented as a 2 × 2 unitary matrix.

$$\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = U \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

Single qubit operators



classical NOT gate

$$\alpha|0\rangle + \beta|1\rangle \;-\boxed{X}-\; \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;-\boxed{Y}-\; -i\beta|0\rangle + i\alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;-\boxed{Z}-\; \alpha|0\rangle - \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;-\boxed{H}-\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$\alpha|0\rangle + \beta|1\rangle \;-\boxed{S}-\; \alpha|0\rangle + i\beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;-\boxed{T}-\; \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

Single qubit operators

- Any 2×2 unitary matrix represents a single qubit operator
- An arbitrary 2×2 unitary matrix may be decomposed as

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta} & 0 \\ 0 & e^{i\beta} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

Multiple qubits

- **A pair of qubits can also exist in superpositions of four states, so the quantum state of two qubits involves associating a complex coefficient – sometimes called an amplitude – with each computational basis state, such that the state vector describing the two qubits is**

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

where the *normalization condition* is satisfied, that is

$$\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2} = 1$$

Multiple qubit

- **For a two qubit system, we could measure just a subset of the qubits, say the first qubit, and you can probably guess how this works: measuring the first qubit alone gives 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, leaving the post-measurement state**

$$|\psi'\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

- **Mmeasuring the first qubit alone gives 1 with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$, leaving the post-measurement state**

$$|\psi'\rangle = \frac{\alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

Multiple qubit

Example: *Bell state* or *EPR pair* (Enstain-Podolsky-Rosen)

$$|\varphi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- **The Bell state has the propertythat upon measuring the first qubit, one obtains two possible results: 0 with probability 1/2, leaving the post-measurement state $|\varphi\rangle = |00\rangle$, and 1 with probability 1/2, leaving $|\varphi\rangle = |11\rangle$.**
- **As a result, a measurement of the second qubit always gives the same result as the measurement of the first qubit. That is, the measurement outcomes are correlated.**
- **Quantom teleportation, superdense coding, entanglement.**

Multiple qubit gates

- **CNOT gate (or controlled-not gate)**

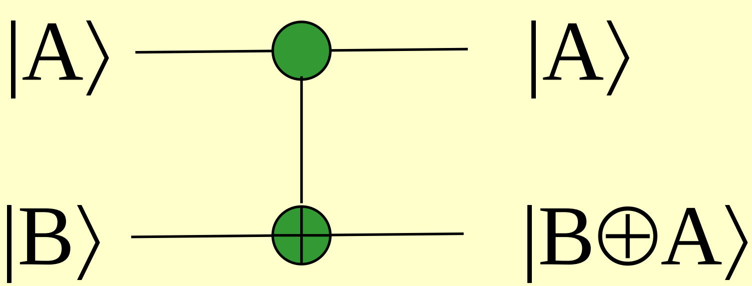
This gate has two input qubits, known as the control qubit and the target qubit, respectively. If the control qubit is set to 0, then the target qubit is left unchanged. If the control qubit is set to 1, then the target qubit is flipped. In equations:

$|00\rangle \rightarrow |00\rangle;\ |01\rangle \rightarrow |01\rangle;\ |10\rangle \rightarrow |11\rangle;\ |11\rangle \rightarrow |10\rangle.$

Circuit representation of a CNOT gate:

control qubit:

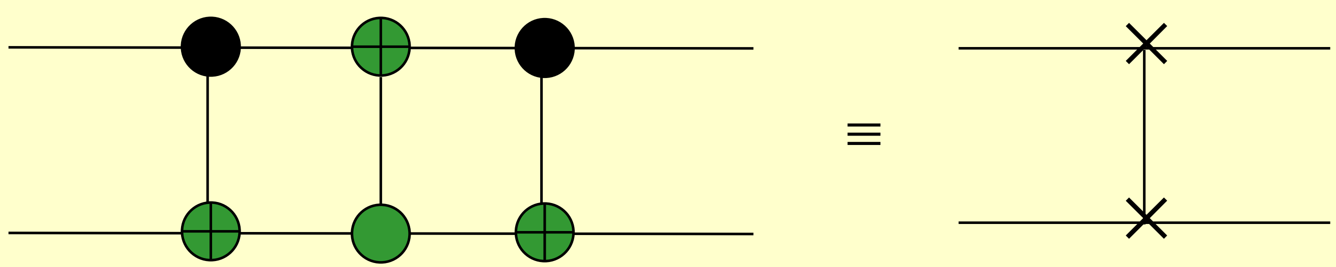
target qubit:



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

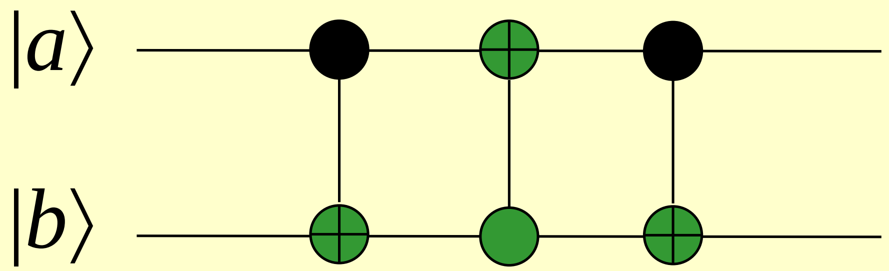
Quantom circuits

- A quantom circuit contains several gates connected through wires.wire does not necessarily
- A wire does not necessarilycorrespond to a physical wire; it may correspond instead to the passage of time, or perhaps to a physical particle such as a photon – a particle of light – moving from one location to another through space.



Quantum circuits

- The function of this circuit is to swaps the states of the two qubits.
- To see this, consider input $|a, b\rangle$



control qubit

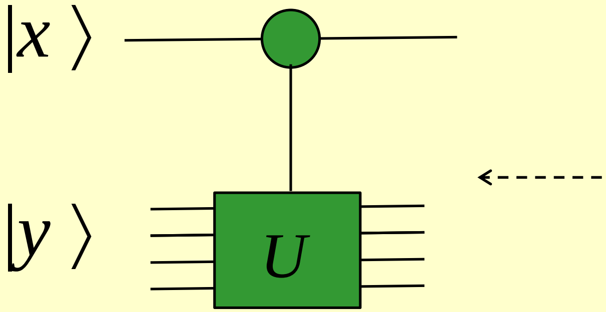
- The effect of the circut on input $|a, b|\rangle$

$$
\begin{aligned}
|a, b\rangle &\longrightarrow |a, b\oplus a\rangle \\
&\longrightarrow |a\oplus(b\oplus a), b\oplus a\rangle = |b, b\oplus a\rangle \\
&\longrightarrow |b, (b\oplus a)\oplus b\rangle = |b, a\rangle
\end{aligned}
$$

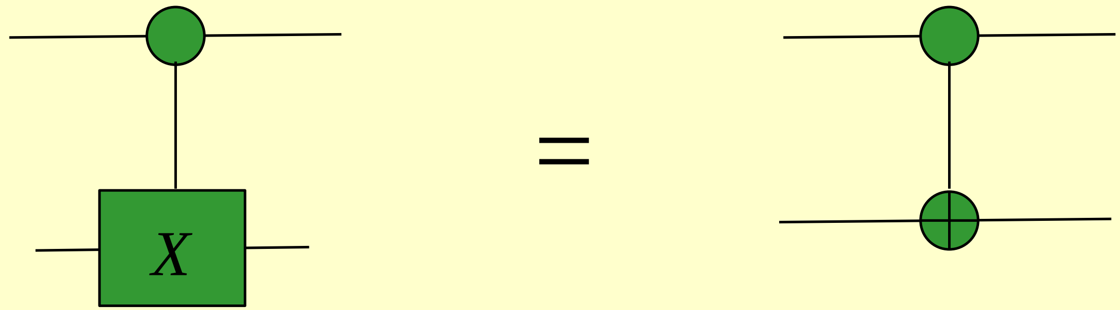
Quantum circuits

- **A convention**
  - **Suppose *U* is any unitary matrix acting on some number *n* of qubits, so *U* can be regarded as a quantum gate on those qubits. Then we can define a controlled-*U* gate which is a natural extension of the controlled- gate.**
  - **If the control qubit is set to 0 then nothing happens to the target qubits. If the control qubit is set to 1 then the gate *U* is applied to the target qubits.**

Quantum circuits



This circuit maps $|0\rangle|y\rangle$ to $|0\rangle|y\rangle$, and $|1\rangle|y\rangle$ to $|1\rangle(U|y\rangle)$. That is, for input $|x\rangle|y\rangle$, the output is $|x\rangle(U^x|y\rangle)$. (Note that $U^0 = I, U^1 = U$.)



For quantom Fourier Transformation, a kind of matrices of the following form is used:

$$U = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{bmatrix}$$

Quantum Fourier Transformation

- **Discrete Fourier transform**

In the usual mathematical notation, the discrete Fourier transform takes as input a vector of complex numbers, $x_0, \ldots, x_{N-1}$ where the length N of the vector is a fixed parameter. It outputs the transformed data, a vector of complex numbers $y_0, \ldots, y_{N-1}$, defined by

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j e^{2\pi ijk/N}$$

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} \, |k\rangle \qquad \sum_{j=0}^{N-1} x_j \, |j\rangle = \sum_{k=0}^{N-1} y_k \, |k\rangle$$

Quantum Fourier Transformation

- **The quantum Fourier transform is exactly the same transformation, although the conventional notation for the quantum Fourier transform is somewhat different. The quantum Fourier transform on an orthonormal basis $|0\rangle$, ..., $|N-1\rangle$ is defined to be a linear operator with the following action on the basis states:**

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} \, |k\rangle$$

- **Equivalently, the action on an arbitrary state may be written**

$$\sum_{j=0}^{N-1} x_j \, | \, j\rangle = \sum_{k=0}^{N-1} y_k \, |k\rangle$$

where the amplitudes y_k are the discrete Fourier transform of the amplitudes x_j.

Quantum Fourier Transformation

- **We take $N = 2^n$, where n is some integer, and the basis $|0\rangle,\ldots, |2^{n-1}\rangle$ is the computational basis for an n qubit quantum computer. It is helpful to write the state $|j\rangle$ using the binary representation $j = j_1 j_2 \ldots j_n$ ($j_i \in \{0, 1\}$). More formally, $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$. It is also convenient to adopt the notation $0.j_l j_{l+1} \ldots j_m$ to represent the binary fraction $j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$.**

$$|j_1 \ldots j_n\rangle \rightarrow$$

$$\frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.j_1 \ldots j_{n-1}j_n}|1\rangle)}{2^{n-1}}$$

Quantum Fourier Transformation

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

$$|j_1 \ldots j_n\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi i(\sum_{l=1}^{n} k_l 2^{-l})} |k_1 \ldots k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi ijk_1/2^1} |k_1\rangle \otimes e^{2\pi ijk_2/2^2} |k_n\rangle \otimes \ldots \otimes e^{2\pi ijk_n/2^n} |k_n\rangle$$

$$= \frac{1}{2^{n/2}} (\sum_{k_1=0}^{1} e^{2\pi ijk_1/2^1} |k_1\rangle) \otimes \ldots \otimes (\sum_{k_n=0}^{1} e^{2\pi ijk_n/2^n} |k_n\rangle)$$

$$= \frac{1}{2^{n/2}} \otimes_{l=1}^{n} (|0\rangle + e^{2\pi ij 2^{-l}} |1\rangle)$$

Quantum Fourier Transformation

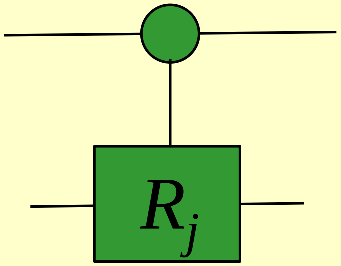
- **In terms of the above formula, an quantom algorithm for Fourier transformation is proposed, in which a Hadamard gate**

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

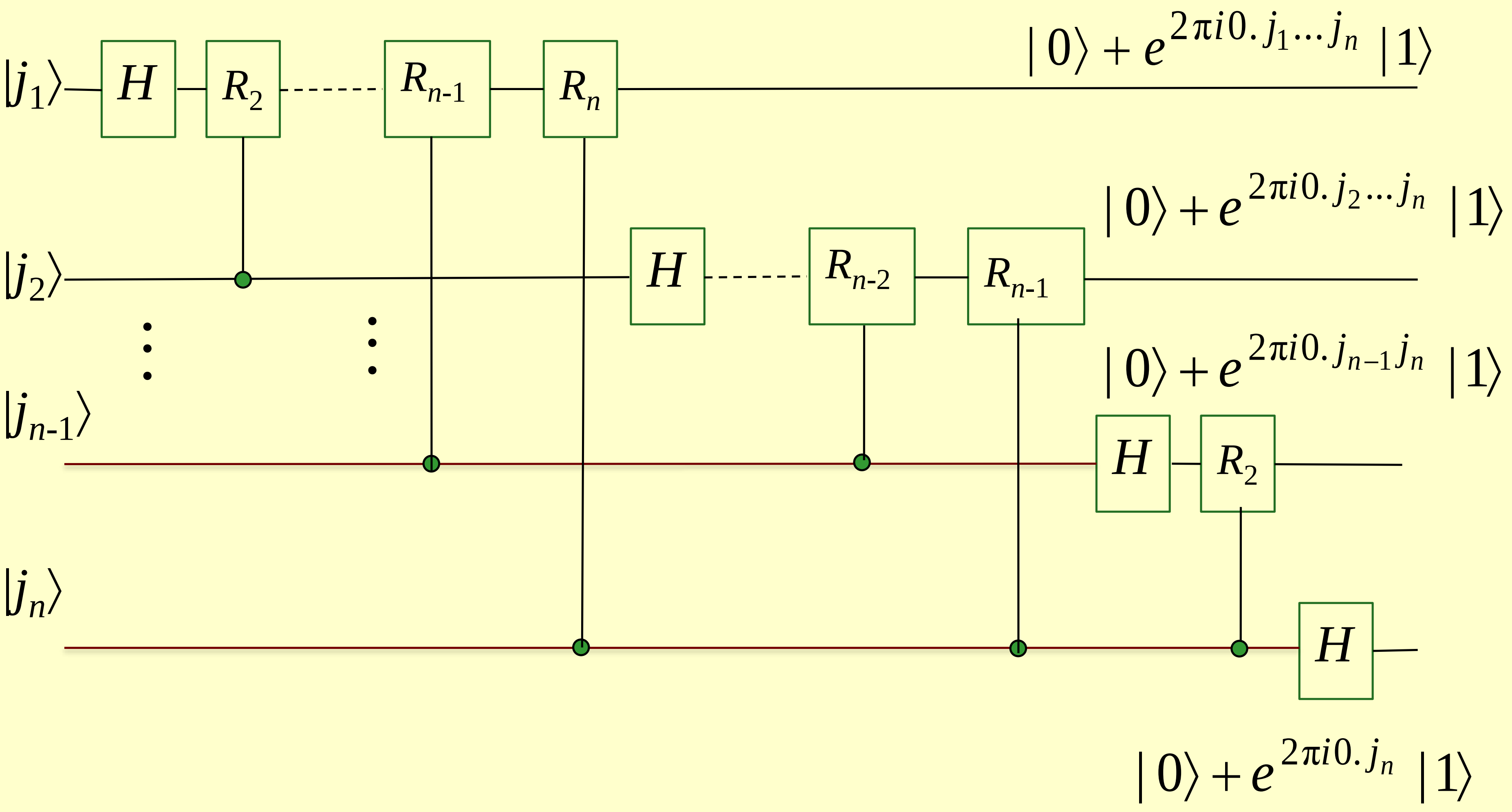
a series of gates of the following form

$$R_j = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^j} \end{bmatrix} \quad \text{for } j = 1, \ldots, n.$$

and a series of controlled-*R* circuits are used.



Quantum Fourier Transformation



Quantum Fourier Transformation

- **The circuit operates as follows. We start with an *n*-qubit input state $|j_1 j_2 \ldots j_n\rangle$.**

1. **After the first Hadamard gate on qubit 1, the state is transformed from the input state to**

$$|j_1 j_2 \ldots j_n\rangle \rightarrow \frac{1}{2^{1/2}}[|0\rangle + e^{2\pi i 0.j_1}|1\rangle] \otimes |j_2 \ldots j_n\rangle$$

since $e^{2\pi i 0.j_1} = -1$ when $j_1 = |1\rangle$, and is +1 otherwise.

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

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

Quantum Fourier Transformation

2. **After the R_2 gate on qubit 1 controlled by qubit 2, the state is transformed to**

$$\frac{1}{2^{1/2}}[|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle] \otimes |j_2 \ldots j_n\rangle$$

3. **We continue applying the controlled-R_3, R_4 through R_n gates, each of which adds an extra bit to the phase of the co-efficient of the first $|1\rangle$. At the end of this procedure we have the state**

$$\frac{1}{2^{1/2}}[|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle] \otimes |j_2 \ldots j_n\rangle$$

Quantum Fourier Transformation

4. Next, we perform a similar procedure on the second qubit. The Hadamard gate puts us in the state

$$\frac{1}{2^{2/2}}[|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle][|0\rangle + e^{2\pi i 0.j_2}|1\rangle]\otimes|j_3 \ldots j_n\rangle$$

5. Continually, the controlled-R_2 through R_{n-1} gates yield the state

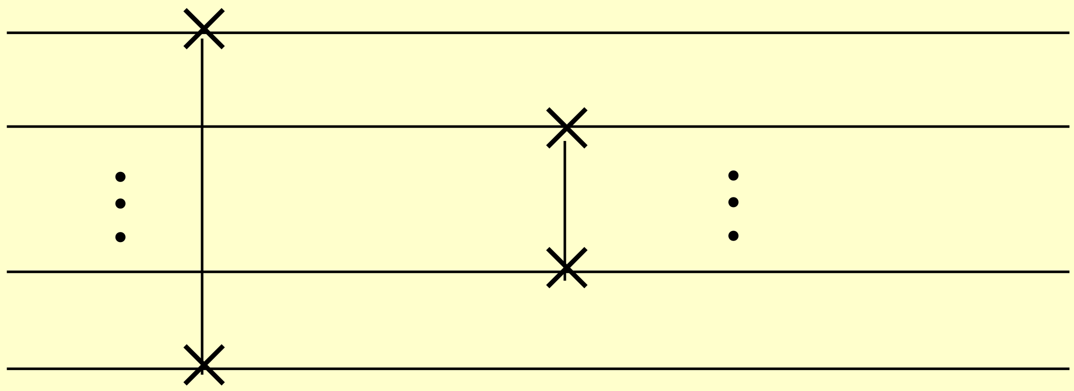
$$\frac{1}{2^{2/2}}[|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle][|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle]\otimes|j_3 \ldots j_n\rangle$$

Quantum Fourier Transformation

6. **Continually, the controlled-R_2 through R_{n-1} gates yield the state**

$$\frac{1}{2^{n/2}}[|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle][|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle]\ldots[|0\rangle + e^{2\pi i 0.j_n}|1\rangle]$$

7. Awap gates.



$$\frac{1}{2^{n/2}}[|0\rangle + e^{2\pi i 0.j_n}|1\rangle]\ldots[|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle][|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle]$$

Quantum Fourier Transformation

- **How many gates does this circuit use? We start by doing a Hadamard gate and $n - 1$ conditional rotations on the first qubit – a total of n gates. This is followed by a Hadamard gate and $n - 2$ conditional rotations on the second qubit, for a total of $n + (n - 1)$ gates.**
- **Continuing in this way, we see that $n + (n - 1) + \cdots + 1 = n(n+1)/2$ gates are required.**
- **Finally, the number of the gates involved in the swaps is $3n/2$.**
  - At most $n/2$ swaps are required, and
  - each swap can be accomplished using three controlled-gates.
- **Therefore, this circuit provides a $\Theta(n^2)$ algorithm for performing the quantum Fourier transform.**

Quantum Fourier Transformation

- **In contrast, the best classical algorithms for computing the discrete Fourier transform on 2^n elements are algorithms such as the Fast Fourier Transform (FFT), which compute the discrete Fourier transform using $\Theta(n2^n)$ gates. That is, it requires exponentially more operations to compute the Fourier transform on a classical computer than it does to implement the quantum Fourier transform on a quantum computer.**

Phase Estimation

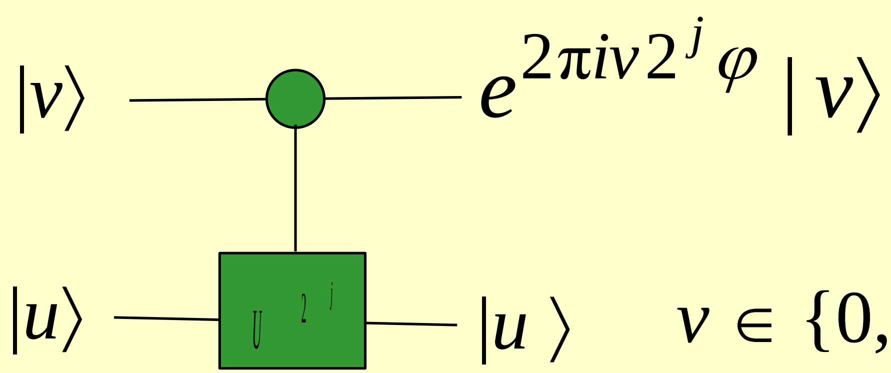
Problem: Suppose an unitary operator (matrix) has an eigen vector $|u\rangle$ with eigen value $e^{2\pi i\varphi}$, where φ is unknown.

Goal: Estimate φ. Note that φ is a real number. We intend to eastimate it to a t-bits value, that is

$$\varphi \approx Q_0 Q_1 \ldots Q_{t-1} = \tilde{\varphi}.$$

Input: The eigen vector $|u\rangle$ and controlled-U^k operator, where $k = 2^j$ for some non-negative integer j.

controlled-U^k operator:



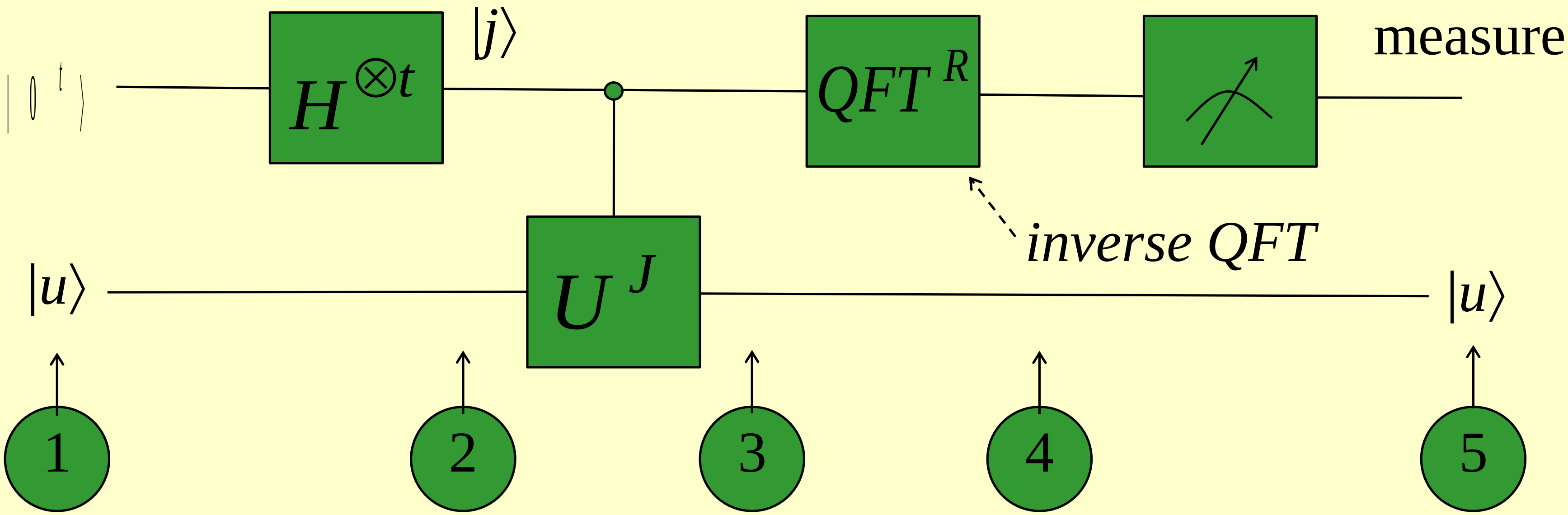
$v \in \{0, 1\}$

Phase Estimation

Suppose there is a black-box that applies U^J where the control state is $|j\rangle$ and j is a t-bit number.

$$|j\rangle|u\rangle \xrightarrow{U^J} |j\rangle U^J|u\rangle = e^{2\pi i\varphi J}|j\rangle|u\rangle$$

Then, schematic of the phase estimation can be show as



Phase Estimation

procedure:

1 $|0^t\rangle|u\rangle$ initialization

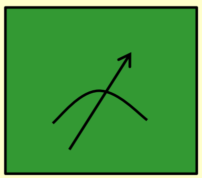
2 $\xrightarrow{H^{\otimes t}} \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$ superposition

3 $\xrightarrow{\text{controlled}-U^J} \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^J|u\rangle$ apply black box

$$= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi iJ\varphi}|j\rangle|u\rangle$$ result of black box

Phase Estimation

4 $\xrightarrow{\quad QFT^R \quad} |\tilde{\varphi}\rangle |u\rangle$ apply *inverse QFT*



5 $\longrightarrow |\tilde{\varphi}\rangle$ measure

Note that $$|\tilde{\varphi}\rangle \underset{QFT^R}{\overset{QFT}{\rightleftarrows}} \sum_{j=0}^{2^t-1} e^{2\pi i j \tilde{\varphi}} |j\rangle$$

Phase Estimation

How do we imolement the black box?

We want to black box apply U^J on $|u\rangle$ when the control qubits are $|j\rangle$ where $j = j_0 j_1 \ldots j_{t\text{-}1}$.

This can be obtained if j_l controls U^{2^l} indipendantly, and the output of U^{2^l} is the input of $U^{2^{l+1}}$.

Phase Estimation