Emory University

CS 463 Quantum Computing & Information

Learning Notes

Jiuru Lyu

April 19, 2026

Contents

1 Qubits and Quantum Circuits

1.1 Qubits

- Quantum computers manipulates qubits (quantum bits)

  1. To review, what's a classical bit (binary bit)? 0 or 1.
  2. How to represent whole numbers with 0's and 1's?

  $$(26)_{10} = 16 + 8 + 2 = (11010)_2$$

  3. Count in binary: $000, 001, 010, 011, 100, 101, 110, 111$.

- Qubits can be in superposition of $|0\rangle$ and $|1\rangle$:

  $$\alpha\,|0\rangle + \beta\,|1\rangle\,,$$

  where $|\alpha|^2 + |\beta|^2 = 1$ (normalization). α and β are called *probability amplitudes* and are complex numbers. Hence, $|\alpha|^2 = \alpha\alpha^*$.

Example 1.1.1

$A\big(\sqrt{2}\,|0\rangle + \mathrm{i}\,|1\rangle\big)$. Find A, given that the expression is in normalized state.

Solution 1.

$$\alpha = A\sqrt{2} \quad \text{and} \quad \beta = A\mathrm{i},$$

So,

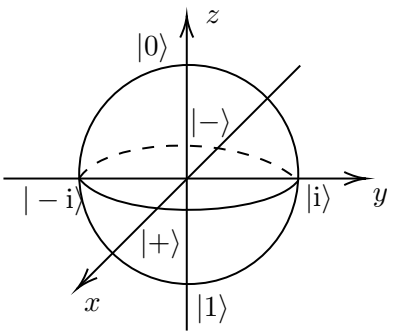
$$|\alpha|^2 = \left(A\sqrt{2}\right)^2 = 2|A|^2, \quad |\beta|^2 = (A\mathrm{i})^2 = |A|^2.$$

Then,

$$\begin{aligned} |\alpha|^2 + |\beta|^2 = 2|A|^2 + |A|^2 &= 1 \\ 3|A|^2 &= 1 \\ |A|^2 &= \frac{1}{3} \\ A &= \pm\frac{1}{\sqrt{3}}, \pm\frac{\mathrm{i}}{\sqrt{3}} = \frac{e^{\mathrm{i}\theta}}{\sqrt{3}}. \end{aligned}$$

□

- Bloch Sphere:



$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$|\pm \mathrm{i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{i}\,|1\rangle).$$

- What happens when we measure a qubit?

  We get one of the two results at opposite points of the Bloch sphere. For example, we get $|0\rangle$ or $|1\rangle$ when measuring along the z-direction of the Bloch sphere. This is called measuring the *z-basis* or *computational basis* and is our default.

- If the qubit state is $\alpha\,|0\rangle + \beta\,|1\rangle$:

  1. $|\alpha|^2 =$ probability of obtaining $|0\rangle$, and
  2. $|\beta|^2 =$ probability of obtaining $|1\rangle$.

  After the measurement, the state is $|0\rangle$ or $|1\rangle$. Measurement *collapses* the state.

Example 1.1.2 Probability of Measurement

If the initial state is $\frac{2}{3}\,|0\rangle + \frac{1-2\mathrm{i}}{3}\,|1\rangle$, then

1. probability of measuring $|0\rangle$ is $\left(\frac{2}{3}\right)^2 = \frac{4}{9}$, and
2. probability of measuring $|1\rangle$ is

$$\frac{1-2\mathrm{i}}{3} \cdot \frac{1+2\mathrm{i}}{3} = \frac{1-(2\mathrm{i})^2}{9} = \frac{5}{9}.$$

Remark. $|a+b\mathrm{i}|^2 = a^2 + b^2$.

Example 1.1.3 Change Measurement Basis

Determine probabilities of results if qubits state is $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ if this qubit is measured in the x-basis.

Solution 2.

Write the state in terms of $|+\rangle$ and $|-\rangle$: $\alpha|+\rangle + \beta|-\rangle$. Recall:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

So,

$$|+\rangle + |-\rangle = \sqrt{2}|0\rangle \quad \text{and} \quad |+\rangle - |-\rangle = \sqrt{2}|1\rangle$$
$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad \text{and} \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).$$

Then,

$$\begin{aligned}\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle &= \frac{\sqrt{3}}{2}\cdot\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) + \frac{1}{2}\cdot\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \\ &= \frac{\sqrt{3}+1}{2\sqrt{2}}|+\rangle + \frac{\sqrt{3}-1}{2\sqrt{2}}|-\rangle.\end{aligned}$$

□

- Consecutive Measurements: Hessenberg Uncertainty Principle

  A qubit $\alpha|0\rangle + \beta|1\rangle$ is measured in z-basis, then x-basis, then z-basis.

  1. z-basis: probability of $|0\rangle$ is $|\alpha|^2$; probability of $|1\rangle$ is $|\beta|^2$.
  2. x-basis: after z-basis measurement, state is either

     $$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad \text{or} \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).$$

     In either case, the probability of $|+\rangle$ is $\frac{1}{2}$, and the probability of $|-\rangle$ is $\frac{1}{2}$.
  3. z-basis: state is either

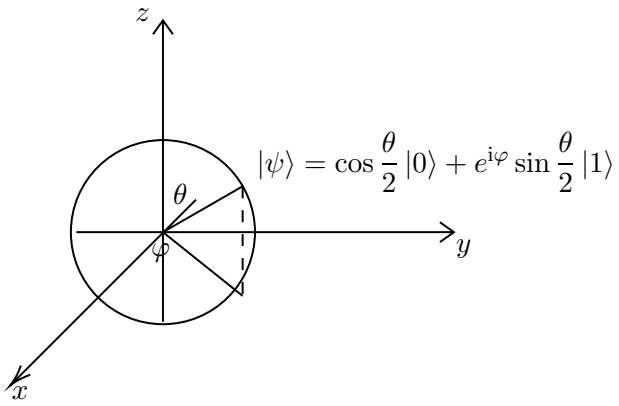
     $$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{or} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

     The probability of $|0\rangle$ is $\frac{1}{2}$, and the probability of $|1\rangle$ is $\frac{1}{2}$.

Definition 1.1.4 (Global Phase and Relative Phase).

- Global phase:
$$e^{i\gamma}(\alpha|0\rangle + \beta|1\rangle),$$
where $e^{i\gamma}$ has no measurable effects. We can ignore/drop it.
- Relative phase:
$$\alpha|0\rangle + e^{i\varphi}\beta|1\rangle,$$
where $e^{i\varphi}$ can be detected. [*For example, compare the following:* $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle$ *and* $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$]

- Map any Qubit to Bloch Sphere:



[*For example,* $|0\rangle$ *corresponds to* $\theta = 0$ *and* $\varphi = 0$*;* $|1\rangle$ *corresponds to* $\theta = \pi$ *and* $\varphi = 0$.]

Example 1.1.5

Find θ and φ for $\frac{3+i\sqrt{3}}{4}|0\rangle - \frac{1}{2}|1\rangle$.

Solution 3.

– Need coefficient of $|0\rangle$ to be real. $\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$.

– Write $\frac{3+i\sqrt{3}}{4}$ in polar form $re^{i\gamma}$ (length and angle in complex plane).

$$r = \sqrt{\frac{9}{16} + \frac{3}{16}} = \sqrt{\frac{12}{16}} = \sqrt{\frac{3}{4}} = \frac{\sqrt{3}}{2}$$
$$\sin\gamma = \frac{\sqrt{3}/4}{\sqrt{3}/2} \implies \gamma = \frac{\pi}{6}.$$

So,

$$\frac{3+\mathrm{i}\sqrt{3}}{4} = \frac{3}{2}e^{\mathrm{i}\frac{\pi}{6}}.$$

– Substitute, and factor $e^{\mathrm{i}\frac{\pi}{6}}$ as a global phase:

$$\frac{3}{2}e^{\mathrm{i}\frac{\pi}{6}}|0\rangle - \frac{1}{2}|1\rangle = e^{\mathrm{i}\frac{\pi}{6}}\left(\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}e^{-\mathrm{i}\frac{\pi}{6}}|1\rangle\right).$$

In $\cos\frac{\theta}{2}|0\rangle + e^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle$, we have "+" in front of $|1\rangle$. So, use $-1 = e^{\mathrm{i}\pi}$. Drop global phase, we have

$$\frac{\sqrt{3}}{2}|0\rangle + e^{\mathrm{i}\pi}\frac{1}{2}e^{-\mathrm{i}\frac{\pi}{6}}|1\rangle = \frac{3}{2}|0\rangle + \frac{1}{2}e^{\mathrm{i}\frac{5\pi}{6}}|1\rangle$$

– Compare expressions:

$$\begin{cases} \frac{\sqrt{3}}{2} = \cos\frac{\theta}{2} \\ \frac{1}{2} = \sin\frac{\theta}{2} \\ \frac{5\pi}{6} = \varphi \end{cases} \implies \frac{\theta}{2} = \frac{\pi}{6} \implies \theta = \frac{\pi}{3} \implies \begin{cases} \theta = \frac{\pi}{3} \\ \varphi = \frac{5\pi}{6}. \end{cases}$$

□

1.2 Quantum Gates

- Classical gates act on classical bits. [*For example, classical NOT gate*].

  Quantum gates act on qubits.

Example 1.2.1

Define gate U by its action on basis states:

$$U|0\rangle = \frac{\sqrt{2}-\mathrm{i}}{2}|0\rangle - \frac{1}{2}|1\rangle \quad \text{and} \quad U|1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{2}+\mathrm{i}}{2}|1\rangle.$$

One can confirm: U keeps normalization and linearity.

Quantum gates are *linear*:

$$U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle.$$

Definition 1.2.2 (Classical Reversible Gates). Gates that can determine inputs from outputs. [*e.g., the classical NOT gate*]. If a gate is a classical reversible gate, then we can make it quantum.

Example 1.2.3

Quantum NOT gate: The X gate:

$$X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle .$$

Then,

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle .$$

Example 1.2.4 Classical Irreversible Gates

Consider the classical gate that maps all inputs to 0. Trying to make it quantum:

$$\text{Gate}|0\rangle = |0\rangle \quad \text{and} \quad \text{Gate}|1\rangle = |0\rangle .$$

Then,

$$\text{Gate}(\alpha|0\rangle + \beta|1\rangle) = \alpha\,\text{Gate}|0\rangle + \beta\,\text{Gate}|1\rangle = (\alpha+\beta)|0\rangle .$$

Assume $|\alpha|^2 + |\beta|^2 = 1$. Check

$$\begin{aligned} |a+\beta|^2 &= (\alpha+\beta)(\alpha^*+\beta^*) \\ &= \alpha\alpha^* + \beta\beta^* + \alpha\beta^* + \alpha^*\beta \\ &= |\alpha|^2 + |\beta|^2 + \alpha\beta^* + \alpha^*\beta \\ &= 1 + \alpha\beta^* + \alpha^*\beta \neq 1. \end{aligned}$$

So, this gate does not keep normalization.

Classical irreversible gates cannot be transformed into quantum gates.

- Common Quantum Gates:

  1. Identity: $I|0\rangle = |0\rangle , \quad I|1\rangle = |1\rangle$.
  2. Pauli X Gate (NOT): $X|0\rangle = |1\rangle , \quad X|1\rangle = |0\rangle$
     Rotates 180° about x-axis.
     $X^2 = I$. ($X^2|0\rangle = X(X|0\rangle) = X|1\rangle = |0\rangle , \quad X^2|1\rangle = X(X|1\rangle) = X|0\rangle = |1\rangle$.)
  3. Pauli Y Gate: $Y|0\rangle = \mathrm{i}|1\rangle , \quad Y|1\rangle = -\mathrm{i}|1\rangle$
     Rotates 180° about y-axis.
  4. Pauli Z Gate: $Z|0\rangle = |0\rangle , \quad Z|1\rangle = -|1\rangle$
     Rotates 180° about z-axis.
  5. Phase Gate: $S|0\rangle = |0\rangle , \quad S|1\rangle = \mathrm{i}|1\rangle$.
     $S^2 = Z$.

6. T Gate: $T|0\rangle = |0\rangle\,, \quad T|1\rangle = e^{i\pi/4}|1\rangle$.
   $T^2 = S$.
7. Hadamard Gate: convert $|0\rangle$ and $|1\rangle$ into superpositions.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$
$$H^2 = I$$

Rotates 180° about $x+z$-axis.

Example 1.2.5

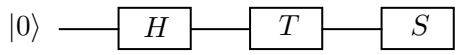
$$\begin{aligned} H|+\rangle &= \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + \cancel{|1\rangle}) + \frac{1}{\sqrt{2}}(|0\rangle - \cancel{|1\rangle})\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{2}{\sqrt{2}}|0\rangle\right) \\ &= |0\rangle\,. \end{aligned}$$

Similarly, $H|-\rangle = |1\rangle$.

- Sequence of Gates:

$$S(T(H|0\rangle)) = STH|0\rangle\,.$$

In quantum circuits diagram:



2 Linear Algebra

2.1 Qubits and Column Vectors

- Note that
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$
Therefore, we can represent a general qubit
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$
$$|\mathrm{i}\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{\mathrm{i}}{\sqrt{2}}\,|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix}.$$
- Transpose and Conjugate Transpose (Hermitian):
$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}^{\top} = \begin{pmatrix} \alpha & \beta \end{pmatrix}$$
$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}^{\dagger} = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$$

Definition 2.1.1 (Dual). If $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, then the *dual vector* of $|\psi\rangle$ is
$$\langle\psi| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} = |\psi\rangle^{\dagger}.$$
Note that ⟨brac|ket⟩. So, we call $\langle\cdot|$ a brac, and $|\cdot\rangle$ a ket.

Example 2.1.2
$$\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^{\dagger} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$
$$\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}^{\dagger} = \begin{pmatrix} 0 & 1 \end{pmatrix}$$
$$\langle \mathrm{i}| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix}^{\dagger} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -\mathrm{i} \end{pmatrix} = \frac{1}{\sqrt{2}}\langle 0| - \frac{\mathrm{i}}{\sqrt{2}}\langle 1|.$$

Definition 2.1.3 (Inner Products). Given $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ and $|\varphi\rangle = \begin{pmatrix}\gamma\\ \delta\end{pmatrix}$, the *inner product* is

$$\langle\psi|\,|\varphi\rangle = \langle\psi|\varphi\rangle = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \alpha^*\gamma + \beta^*\delta.$$

Note: inner products are not commutative:

$$\langle\varphi|\psi\rangle = \begin{pmatrix}\gamma^* & \delta^*\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \gamma^*\alpha + \delta^*\beta = \langle\psi|\varphi\rangle^*.$$

Definition 2.1.4 (Normalization). If $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ is *normalized*, then its norm

$$\text{norm} := \sqrt{\langle\psi|\psi\rangle} = 1.$$

Note:

$$\langle\psi|\psi\rangle = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha^*\alpha + \beta^*\beta = |\alpha|^2 + |\beta|^2 = 1.$$

Definition 2.1.5 (Orthogonality). If inner product of two vectors is 0, then the two states are *orthogonal* to each other. For example,

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

If each state is also normalized, we call them *orthonormal*. All basis are orthonormal.

- Notice that if $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, then

$$\langle 0|\psi\rangle = \alpha\,\langle 0|0\rangle + \beta\,\langle 0|1\rangle = \alpha$$
$$\langle 1|\psi\rangle = \alpha\,\langle 1|0\rangle + \beta\,\langle 1|1\rangle = \beta.$$

So,

$$|\psi\rangle = \langle 0|\psi\rangle\,|0\rangle + \langle 1|\psi\rangle\,|1\rangle\,.$$

Example 2.1.6

$|\psi\rangle = \dfrac{\sqrt{3}}{2}\,|0\rangle + \dfrac{1}{2}\,|1\rangle.$

1. Measure in computational basis (z-basis):

$$\text{probability of } |0\rangle = \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4}$$
$$\text{probability of } |1\rangle = \left(\frac{1}{2}\right)^2 = \frac{1}{4}.$$

2. Measure in x-basis: $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ and $|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$.

$$|\psi\rangle = \langle+|\psi\rangle\,|+\rangle + \langle-|\psi\rangle\,|-\rangle$$
$$\text{probability of } |+\rangle = |\langle+|\psi\rangle|^2 = \left(\frac{1}{\sqrt{2}}\cdot\frac{\sqrt{3}}{2} + \frac{1}{\sqrt{2}}\cdot\frac{1}{2}\right)$$
$$= \left(\frac{\sqrt{3}+1}{2\sqrt{2}}\right)^2 = \frac{3+1+2\sqrt{3}}{8} = \frac{2+\sqrt{3}}{4}.$$
$$\text{probability of } |-\rangle = |\langle-|\psi\rangle|^2 = \left(\frac{1}{\sqrt{2}}\cdot\frac{\sqrt{3}}{2} - \frac{1}{\sqrt{2}}\cdot\frac{1}{2}\right)^2$$
$$= \left(\frac{\sqrt{3}-1}{2\sqrt{2}}\right)^2 = \frac{3+1-2\sqrt{3}}{8} = \frac{2-\sqrt{3}}{4}.$$

- Generally, probability of $|\varphi\rangle$ if original state is $|\psi\rangle$:

$$|\langle\varphi|\psi\rangle|^2.$$

2.2 Gates are Matrices

- If $U|0\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix}a\\b\end{pmatrix}$ and $U|1\rangle = c|0\rangle + d|1\rangle = \begin{pmatrix}c\\d\end{pmatrix}$, then

$$U = \begin{pmatrix}a & c\\ b & d\end{pmatrix}.$$

Proof 1.

$$U|0\rangle = \begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix} \quad \text{and} \quad U|1\rangle = \begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}c\\d\end{pmatrix}.$$

Q.E.D. ■

- If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$, then

$$U|\psi\rangle = \begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}a\alpha + c\beta\\ b\alpha + d\beta\end{pmatrix} = \begin{pmatrix}a\alpha\\ b\alpha\end{pmatrix} + \begin{pmatrix}c\beta\\ d\beta\end{pmatrix} = \alpha\begin{pmatrix}a\\ b\end{pmatrix} + \beta\begin{pmatrix}c\\ d\end{pmatrix} = \alpha U|0\rangle + \beta U|1\rangle.$$

- Unitarity:

  Quantum gates preserve total probability. i.e., it preserves norm:

$$U|\psi\rangle \quad \text{has the same norm as} \quad |\psi\rangle.$$

  1. Define $|U\psi\rangle = U|\psi\rangle$. Show: $\langle U\psi| = |U\psi\rangle^\dagger = (U|\psi\rangle)^\dagger = \langle\psi|U^\dagger$.

     Proof 2. If $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ and $U = \begin{pmatrix}a & c\\ b & d\end{pmatrix}$, then

$$U|\psi\rangle = \begin{pmatrix}a\alpha + c\beta\\ b\alpha + d\beta\end{pmatrix}.$$

     Meanwhile,

$$\langle\psi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix} \quad \text{and} \quad U^\dagger = \begin{pmatrix}a^* & c^*\\ b^* & d^*\end{pmatrix}.$$

     Then,

$$\langle\psi|U^\dagger = \begin{pmatrix}\alpha^*a^* + \beta^*c^* & \alpha^*b^* + \beta^*d^*\end{pmatrix}$$
$$(U|\psi\rangle)^* = \begin{pmatrix}\alpha^*a^* + \beta^*c^* & \alpha^*b^* + \beta^*d^*\end{pmatrix}.$$

     Q.E.D. ■

  2. Preserve norm:

$$\langle\psi|\psi\rangle = \langle U\psi|U\psi\rangle = \langle\psi|U^\dagger U|\psi\rangle.$$

     So, it must be that $U^\dagger U = I$. Then, $U^\dagger = U^{-1}$.

     [*Implication: all quantum gates are reversible.*]

- *Outer products* are matrices/gates.

  If $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ and $|\varphi\rangle = \begin{pmatrix}\gamma\\ \delta\end{pmatrix}$, then

$$|\psi\rangle\langle\varphi| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\begin{pmatrix}\gamma^* & \delta^*\end{pmatrix} = \begin{pmatrix}\alpha\gamma^* & \alpha\delta^*\\ \beta\gamma^* & \beta\delta^*\end{pmatrix}.$$

Example 2.2.1

Let $U = |1\rangle\langle 0| + |0\rangle\langle 1|$ act on $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Solution 3.

Method 1

$$\begin{aligned} U|\psi\rangle &= (|1\rangle\langle 0| + |0\rangle\langle 1|)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|1\rangle\underbrace{\langle 0|0\rangle}_{=1} + \beta|1\rangle\underbrace{\langle 0|1\rangle}_{=0} + \alpha|0\rangle\underbrace{\langle 1|0\rangle}_{=0} + \beta|0\rangle\underbrace{\langle 1|1\rangle}_{=1} \\ &= \alpha|1\rangle + \beta|0\rangle. \end{aligned}$$

So, U is the Pauli X (NOT) gate.

Method 2

$$\begin{aligned} U = |1\rangle\langle 0| + |0\rangle\langle 1| &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

$$U|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}.$$

□

3 Multiple Qubits

- Two qubits, both in state $|0\rangle$:

$$|0\rangle |0\rangle = |00\rangle = |0\rangle \otimes |0\rangle ,$$

where $\otimes$ is called a tensor/Kronecker product.

The computational basis for two qubits is

$$\{|00\rangle , |01\rangle , |10\rangle , |11\rangle\} = \{|0\rangle , |1\rangle , |2\rangle , |3\rangle\}.$$

Generate state of two qubits:

$$c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle = c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle = \sum_{j=0}^{3} c_j |j\rangle .$$

- General state of three qubits:

$$\sum_{j=0}^{7} c_j |j\rangle .$$

Generate state of n qubits:

$$\sum_{j=0}^{N-1} c_j |j\rangle , \quad \text{where } N = 2^n.$$

Normalization:

$$\sum_{j=0}^{N-1} |c_j|^2 = 1.$$

Example 3.0.1 Many Ways to Represent the Same Thing

1. n qubits, each in state $|0\rangle$:

$$|0\rangle^{\otimes n} = \underbrace{|0\rangle |0\rangle \cdots |0\rangle}_{n} = \underbrace{|00\cdots 0\rangle}_{n} = \underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{n} = |0^n\rangle .$$

2. Also work with $\langle\cdot|$:

$$\langle 0| \otimes \langle 0| = \langle 0| \langle 0| = \langle 00| .$$

- Inner products obtained by matching qubits:

$$\langle 01|00\rangle = \langle 0|0\rangle \langle 1|0\rangle = 1 \cdot 0 = 0.$$
$$\langle 3|2\rangle = \langle 11|10\rangle = \langle 1|1\rangle \langle 1|0\rangle = 1 \cdot 0 = 0.$$

So, general expression: Kronecker-δ:

$$\delta_{jk} = \langle j|k\rangle = \begin{cases} 0, & j \neq k \\ 1, & j = k. \end{cases}$$

Definition 3.0.2 (Kronecker Product). Multiply each term of the first matrix (vector) by the entire second matrix (vector).

Example 3.0.3

- $$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

  $$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

  Similarly,

  $$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

- NOT Gate:

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

  So, $X \otimes X \neq X^2 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

- General state:

  $$c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}.$$

- Three qubits:

$$\sum_{j=0}^{7} c_j |j\rangle = c_0 |0\rangle + c_1 |1\rangle + \cdots + c_7 |7\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_7 \end{pmatrix}.$$

- General case: $N = 2^n$, and

$$|\psi\rangle = \sum_{j=0}^{N-1} c_j |j\rangle = c_0 |0\rangle + \cdots + c_{N-1} |N-1\rangle = \begin{pmatrix} c_0 \\ \vdots \\ c_{N-1} \end{pmatrix}.$$

- $$\langle 00| = \langle 0| \otimes \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1(1 & 0) & 0(1 & 0) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}.$$

- $$\langle \psi| = |\psi\rangle^\dagger = \begin{pmatrix} c_0^* & c_1^* & \cdots & c_{N-1}^* \end{pmatrix}.$$

Measuring Individual Qubits Consider $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{2} |01\rangle + \frac{\sqrt{3}}{4} |10\rangle + \frac{1}{4} |11\rangle$. What happens if we measure only the first (left) qubit?

$$\begin{aligned} \text{probability of } |0\rangle &= \text{probability of } |00\rangle + \text{probability of } |01\rangle \\ &= \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{3}{4} \end{aligned}$$

The state collapses to terms where the first qubit is $|0\rangle$:

$$|00\rangle \quad \text{and} \quad |01\rangle .$$

So, it becomes

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{2} |01\rangle .$$

But we need to re-normalize it. Assume A is the normalization constant:

$$A\left(\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{2} |01\rangle\right).$$

So,

$$\left(\frac{A}{\sqrt{2}}\right)^2 + \left(\frac{A}{2}\right)^2 = \frac{A^2}{2} + \frac{A^2}{4} = 1 \implies \frac{3}{4}A^2 = 1 \implies A^2 = \frac{4}{3} \implies A = \frac{2}{\sqrt{3}}.$$

On the other hand,

$$\begin{aligned}\text{probability of } |1\rangle &= \text{probability of } |10\rangle + \text{probability of } |11\rangle \\ &= \left(\frac{\sqrt{3}}{4}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{1}{4}.\end{aligned}$$

The states collapses to

$$B\left(\frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle\right) \implies \frac{1}{4}B^2 = 1 \implies B^2 = 4 \implies B = 2.$$

Definition 3.0.4 (Product State). *Product state* can be written as product of state of individual qubits.

- $$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |+\rangle\,|-\rangle\,.$$
- $\frac{1}{2\sqrt{2}}\left(\sqrt{3}\,|00\rangle - \sqrt{3}\,|01\rangle + |10\rangle - |11\rangle\right)$.
  Assume

$$\begin{aligned}|\psi_1\rangle\,|\psi_0\rangle &= (\alpha_1\,|0\rangle + \beta_1\,|1\rangle)(\alpha_0\,|0\rangle + \beta_0\,|1\rangle) \\ &= \alpha_1\alpha_0\,|00\rangle + \alpha_1\beta_0\,|01\rangle + \beta_1\alpha_0\,|10\rangle + \beta_1\beta_0\,|11\rangle\,.\end{aligned}$$

So,

$$\begin{cases}\alpha_1\alpha_0 = \dfrac{\sqrt{3}}{2\sqrt{2}} & \implies \alpha_1 = \dfrac{\sqrt{3}}{2\alpha_0\sqrt{2}} \\ \alpha_1\beta_0 = -\dfrac{\sqrt{3}}{2\sqrt{2}} & \implies \dfrac{\sqrt{3}}{2\alpha_0\sqrt{2}}\beta_0 = -\dfrac{\sqrt{3}}{2\sqrt{2}} \implies \beta_0 = -\alpha_0 \\ \beta_1\alpha_0 = \dfrac{1}{2\sqrt{2}} & \implies \beta_1 = \dfrac{1}{2\alpha_0\sqrt{2}} \\ \beta_1\beta_0 = -\dfrac{1}{2\sqrt{2}} & \implies \dfrac{1}{2\alpha_0\sqrt{2}}(-\alpha_0) = -\dfrac{1}{2\sqrt{2}} \implies -\dfrac{1}{2\sqrt{2}} = -\dfrac{1}{2\sqrt{2}}\end{cases}$$

So, this is a product state:

$$\begin{aligned}|\psi_1\rangle\,|\psi_0\rangle &= \left(\frac{\sqrt{3}}{2\alpha_0\sqrt{2}}|0\rangle + \frac{1}{2\alpha_0\sqrt{2}}|1\rangle\right)(\alpha_0\,|0\rangle - \alpha_0\,|1\rangle) \\ &= \left(\frac{\sqrt{3}}{2\sqrt{2}}|0\rangle + \frac{1}{2\sqrt{2}}|1\rangle\right)(|0\rangle - |1\rangle) \\ &= \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).\end{aligned}$$

Definition 3.0.5 (Entangled State). *Entangled state* cannot be factored into product state.

Consider $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Assume

$$\begin{aligned}\left|\Phi^+\right\rangle = |\psi_1\rangle\,|\psi_0\rangle &= (\alpha_1\,|0\rangle + \beta_1\,|1\rangle)(\alpha_0\,|0\rangle + \beta_0\,|1\rangle) \\ &= \alpha_1\alpha_0\,|00\rangle + \alpha_1\beta_0\,|01\rangle + \beta_1\alpha_0\,|10\rangle + \beta_1\beta_0\,|11\rangle\,.\end{aligned}$$

So,

$$\begin{cases} \alpha_1\alpha_0 = \frac{1}{\sqrt{2}} & \implies \alpha_1 = \frac{1}{\alpha_0\sqrt{2}} \implies \alpha_0, \alpha_1 \neq 0 \\ \alpha_1\beta_0 = 0 & \implies \beta_0 = 0 \\ \beta_1\alpha_0 = 0 & \implies \beta_1 = 0 \\ \beta_1\beta_0 = \frac{1}{\sqrt{2}} & \implies \beta_1\beta_0 = \frac{1}{\sqrt{2}} \neq 0. \end{cases}$$

So, $|\Phi^+\rangle$ is not a product state. It is an entangled state.

3.1 Quantum Circuit Diagrams

Start with $|0\rangle\,|0\rangle$, act on the left qubit with H, act on the right qubit with X: $H\,|0\rangle\,X\,|0\rangle$.

- How to draw the circuit? Two conventions:

  1. Left qubit on bottom (Ours):

     Note: $\oplus = \boxed{X}$

     $|0\rangle$ ——⊕

     left qubit $\to$ $|0\rangle$ ——$\boxed{H}$

  2. Left qubit on top (Everyone else).

- Three ways to analyze the circuits:

  1. Each gate acts on own qubit:

$$H\,|0\rangle\,X\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

  2. Separate matrix for each gate:

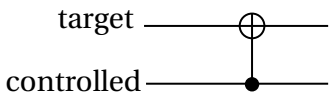
$$\begin{aligned} H\,|0\rangle \otimes X\,|0\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}\end{aligned}$$

3. Kronecker product:

$$\begin{aligned} H|0\rangle \otimes X|0\rangle &= (H \otimes X)(|0\rangle \otimes |0\rangle) \\ &= \left[\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right]\left[\begin{pmatrix}1\\ 0\end{pmatrix} \otimes \begin{pmatrix}1\\ 0\end{pmatrix}\right] \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1 & 0 & 1\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\\ 0\\ 0\end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}0\\ 1\\ 0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle). \end{aligned}$$

- Common Quantum Gates on Two Qubits:

1. Controlled NOT (CNOT): Applied NOT to the target unit if the controlled unit is $|1\rangle$.



$$\begin{aligned} \text{CNOT}\,|\text{control}\rangle\,|\text{target}\rangle: \quad & \text{CNOT}\,|00\rangle = |00\rangle \\ & \text{CNOT}\,|01\rangle = |01\rangle \\ & \text{CNOT}\,|10\rangle = |11\rangle \\ & \text{CNOT}\,|11\rangle = |10\rangle\,. \end{aligned}$$

Note that

$$\text{CNOT}\,|a\rangle\,|b\rangle = |a\rangle\,|a \oplus b\rangle\,,$$

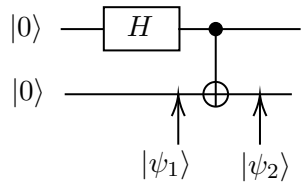
where $\oplus$ standard for exclusive or (XOR) operation.

a	b	$a \oplus b$ (XOR)
0	0	0
0	1	1
1	0	1
1	1	0

If the circuit diagram can also place the controlled at top and target at bottom, which gives

$$\text{CNOT}\,|a\rangle\,|b\rangle = |a \oplus b\rangle\,|b\rangle\,.$$

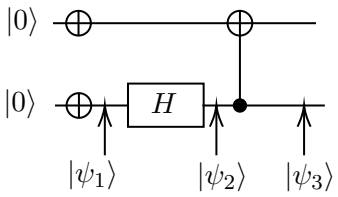
2. For example,



$$|\psi_1\rangle = |0\rangle\, H\, |0\rangle = |0\rangle\, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$
$$|\psi_2\rangle = \text{CNOT}\, \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Note that $|\psi_2\rangle$ is an entangled state.

3. Other controlled gate: If the controlled is $|1\rangle$, we apply the gate to the target unit.



$$|\psi_1\rangle = X\, |0\rangle\, X\, |0\rangle = |1\rangle\, |1\rangle$$
$$|\psi_2\rangle = H\, |1\rangle\, |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\, |1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$$
$$|\psi_3\rangle = \text{CNOT}\, |\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

4. Note that

$$\begin{aligned} H\, |0\rangle\, |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) \\ &= \frac{1}{2}\sum_{j=0}^{3} |j\rangle\,. \end{aligned}$$

We can generalize this further:

$$H\, |0\rangle\, H\, |0\rangle\, H\, |0\rangle = \frac{1}{\sqrt{8}}\sum_{j=0}^{7} |j\rangle\,.$$

4 Quantum Adder

Goal: Design a quantum circuit that adds two 4-bit numbers.

Firstly, let's review binary addition:

carry	1	1	1	0	0
		1	0	1	1
$+$		1	1	1	0
sum	1	1	0	0	1

This calculation represents $11 + 14 = 25$ in base 10. In general,

carry	c_4	c_3	c_2	c_1	$c_0 \equiv 0$
		a_3	a_2	a_1	a_0
$+$		b_3	b_2	b_1	b_0
sum	$c_4 \equiv s_4$	s_3	s_2	s_1	s_0

For each column, we need sum bit and carry bit:

$$(c_0, a_i, b_i) \mapsto (c_{i+1}, s_i).$$

c_i	a_i	b_i	c_{i+1}	s_i
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

- $s_i = 1$ if 1 input or 3 inputs are 1:

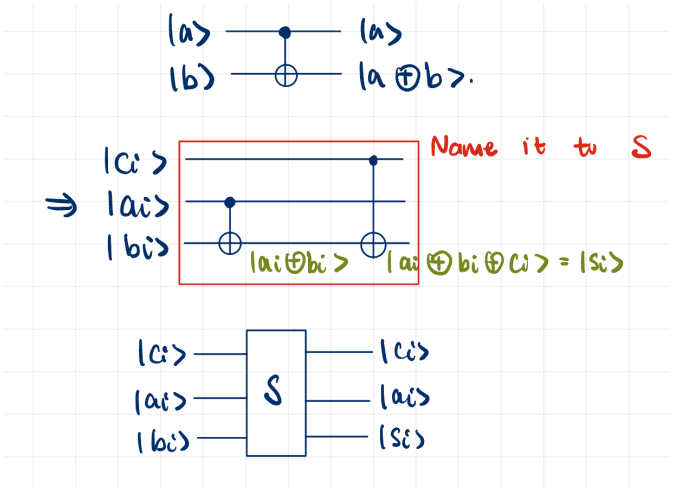
$$s_i = c_i \oplus a_i \oplus b_i$$

- $c_{i+1} = 1$ if at least 2 inputs are 1:

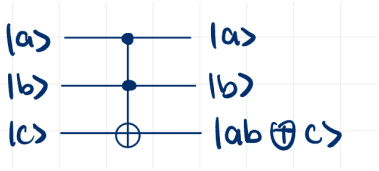
$$\begin{aligned} c_{i+1} &= a_i \wedge b_i \oplus c_i \wedge (a_i \oplus b_i) \\ &= a_i b_i \oplus c_i (a_i \oplus b_i). \end{aligned}$$

Now, let's make everything quantum.

4.1 CNOT for $|s_i\rangle$

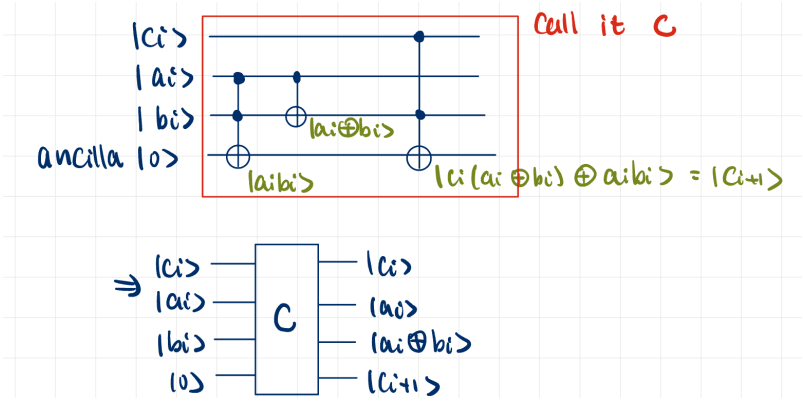


4.2 Toffoli Gate and the Carry Gate

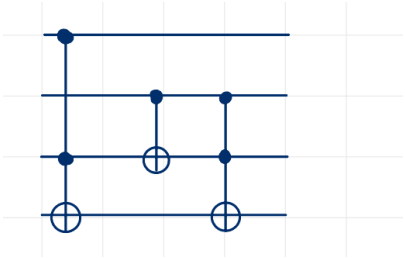


Both controls have to be 1 in order to have the NOT gate act on target.

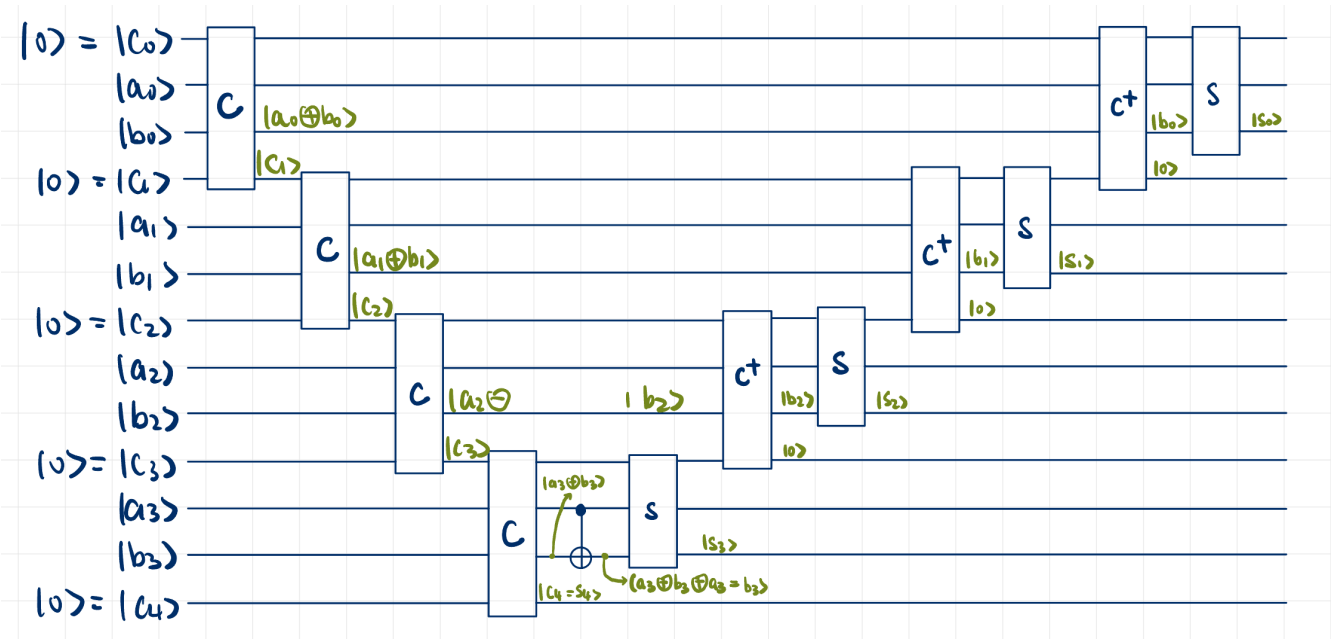
- $c \to \overline{c} \iff ab = 1$.
- Construct $|c_{i+1}\rangle$:



- In the adder, we also need $C^{-1} = C^\dagger$:



4.3 The Complete Quantum Adder



5 Quantum Entanglement: Bell/CHSH Inequality

5.1 Bell Inequality

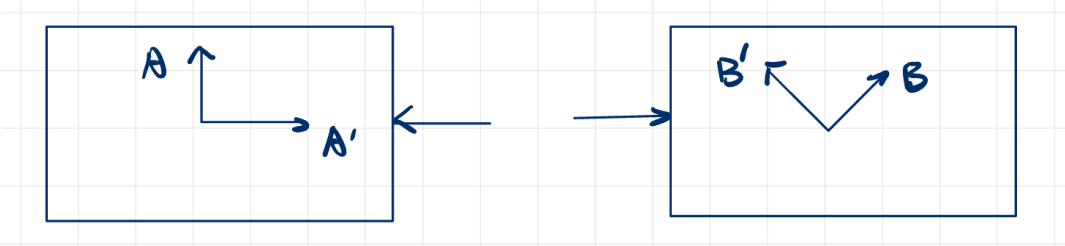
Common Sense Assumption

- Objective have properties even if we are not observing them.
- The measurement of one object doesn't affect the other object.

However, quantum mechanics can disobey the common senses.

Deriving a Bell Inequality Synopsis of an experiment:

- A pair of particles is created.
- One files to Alice and one files to Bob.
- Alice's detector has two settings: She measures either A or A'
- Bob measures either B or B'
- In all cases, each detector displays one of the two results: $+1$ or -1.



- Alice measures A, and Bob measures B.
- They multiply their results together, AB, which is either $+1$ or -1.
- They do this for many pairs of particles and calculate the average of AB. For example,

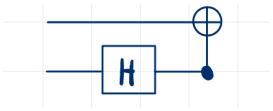
A	B	AB
$+1$	$+1$	$+1$
$+1$	-1	-1
-1	-1	$+1$

- For each particle arriving at Alice's detector, she measures A or A', not both. Common sense says that they both exist regardless.
- Similarly, for each particle arriving at Bob's detector, he measures B or B', not both. Common sense says that they both exist regardless.

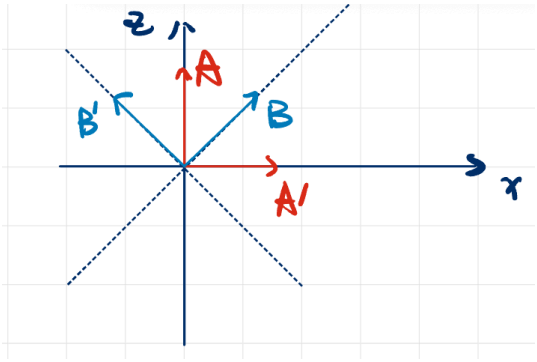
- Define
$$S = AB + AB' + A'B - A'B'$$
or sometimes, we would subtract AB'
- Common sense says that each pair of particles has an S value.
- S must be $+2$ or -2. The average of S must be between $+2$ or -2. This is exactly the *Bell inequality* (or, *CHSH inequality*).
- However, experiments show that average of S can be greater than $+2$.
- So, it was wrong to assume that S exists for each pair of particles.
- At least one of our common sense assumptions must be wrong:
  1. A, A', B, and B' *all* exist even if we don't measure them, or
  2. The measurement of one particle will not affect the other.

5.2 How to Test CHSH Inequality?

- Create an entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

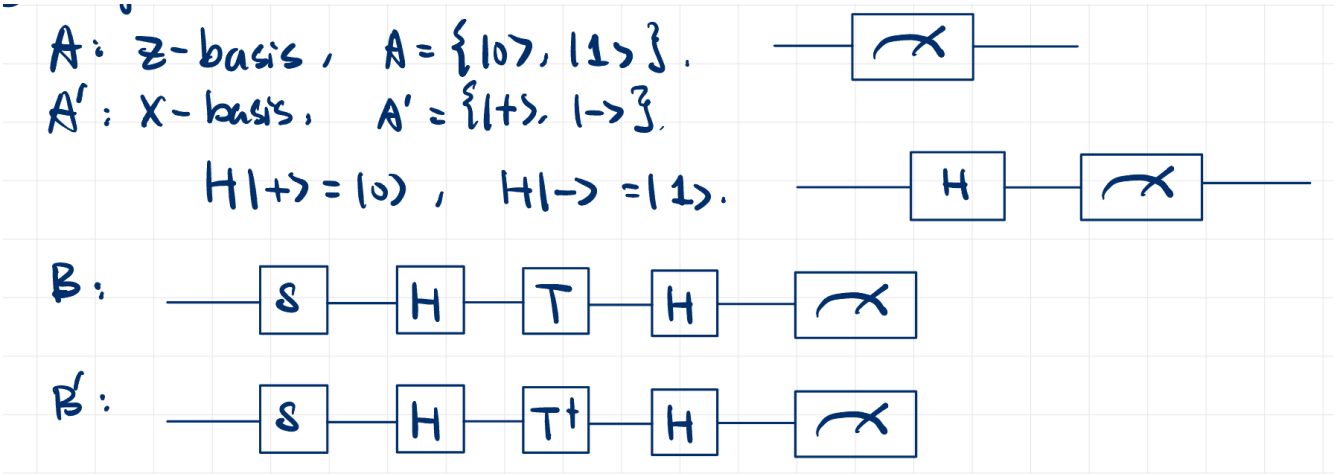


- Create 4 kinds of measurements: A, A', B, and B'. (Different measurement direction on Bloch's sphere).

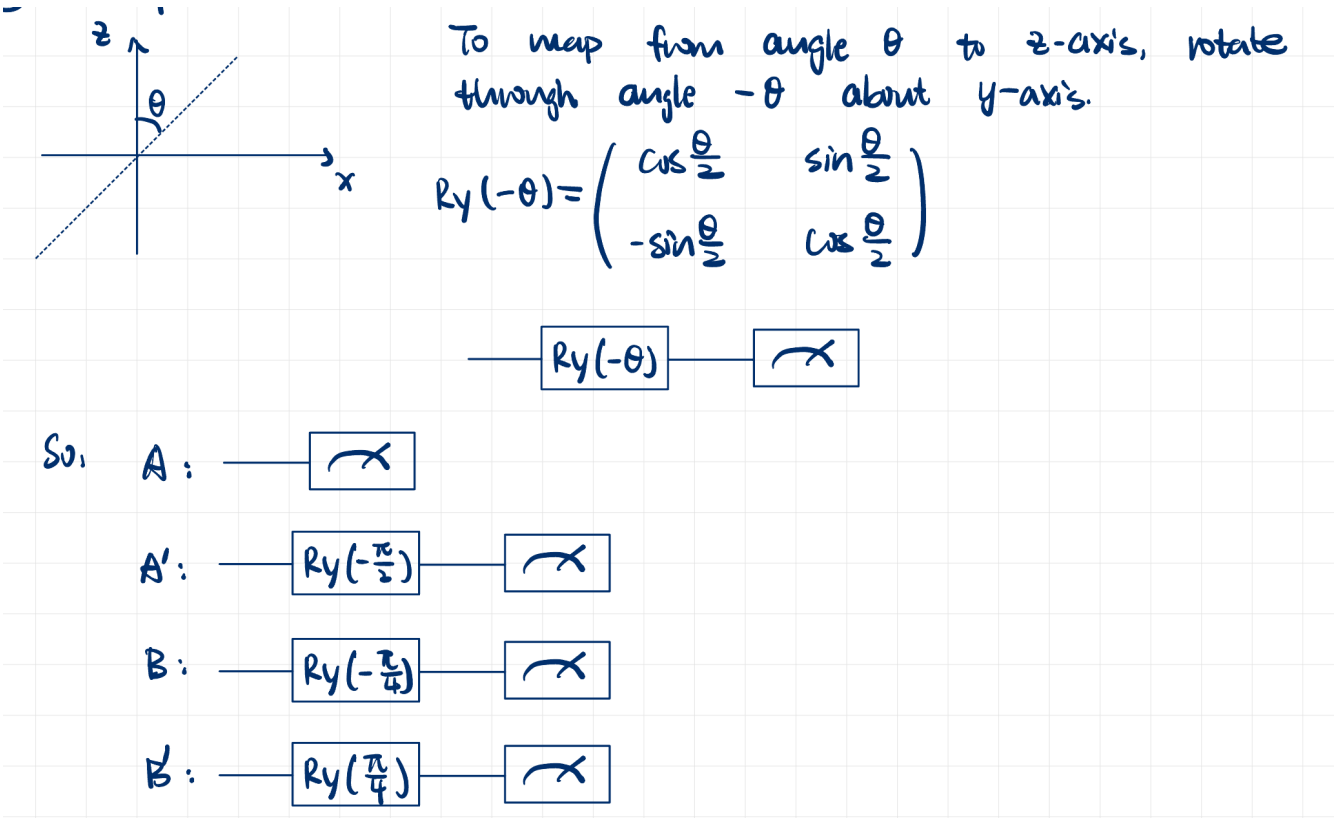


There

1. Wong's circuit:



2. A simpler alternative:



- How to compute averages of AB, AB', $A'B$, and $A'B'$?

1. Measured results is histogram: fractional distribution of 4 possible results $(00,\ 01,\ 10,\ 11)$, which approximates probabilities $\mathbf{P}_{00}, \mathbf{P}_{01}, \mathbf{P}_{10}, \mathbf{P}_{11}$.
2. Alice and Bob's results were ± 1, not 0 and 1. So, map $0 \to +1$ and $1 \to -1$:

	A	B	AB
00	$+1$	$+1$	$+1$
01	$+1$	-1	-1
10	-1	$+1$	-1
11	-1	-1	$+1$

3. Average of AB:

$$\mathbf{E}(AB) = \mathbf{P}_{00} + \mathbf{P}_{11} - \mathbf{P}_{01} - \mathbf{P}_{10}$$

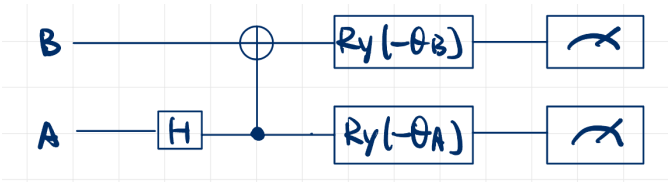
4. We run 4 circuits (for AB, $A'B$, AB', and $A'B'$) to compute average of S:

$$\mathbf{E}(S) = \mathbf{E}(AB) + \mathbf{E}(A'B) + \mathbf{E}(AB') - \mathbf{E}(A'B')$$

The CHSH Inequality

$$|\mathbf{E}(S)| \leq 2.$$

- Derive Quantum Prediction: The circuits are:



where θ_A and θ_B are given as follows:

	θ_A	θ_B
AB	0	$\pi/4$
AB'	0	$-\pi/4$
$A'B$	$\pi/2$	$\pi/4$
$A'B'$	$\pi/2$	$-\pi/4$.

Before measurement, the state is

$$\big[R_y(-\theta_A) \otimes R_y(-\theta_B)\big] \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \begin{pmatrix} \cos\frac{\theta_A}{2}\cos\frac{\theta_B}{2} & * & * & \sin\frac{\theta_A}{2}\sin\frac{\theta_B}{2} \\ -\cos\frac{\theta_A}{2}\sin\frac{\theta_B}{2} & * & * & \sin\frac{\theta_A}{2}\cos\frac{\theta_B}{2} \\ -\sin\frac{\theta_A}{2}\cos\frac{\theta_B}{2} & * & * & \cos\frac{\theta_A}{2}\sin\frac{\theta_B}{2} \\ \sin\frac{\theta_A}{2}\sin\frac{\theta_B}{2} & * & * & \cos\frac{\theta_A}{2}\cos\frac{\theta_B}{2} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

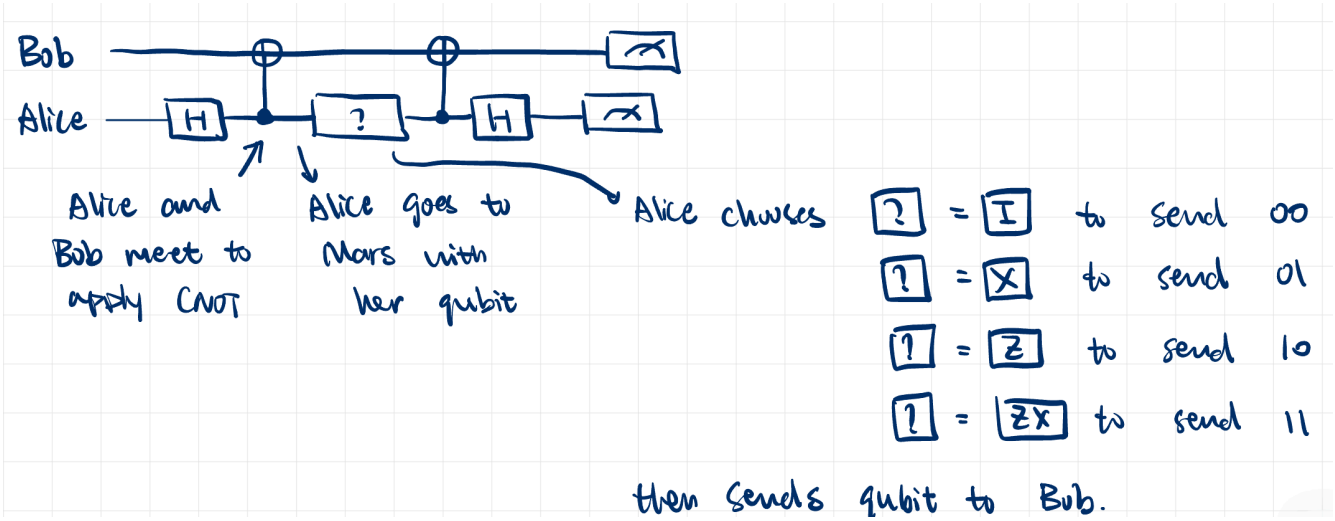
With some work, one can show

$$\mathbf{E}(S) = 2\sqrt{2}.$$

6 Quantum Protocol

6.1 Superdense Coding

Alice wants to send 2 bits (00, 01, 10, or 11) to Bob by sending a single qubit.



Example 6.1.1

Alice sends 01: After ther first CNOT, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

After $\boxed{?} = \boxed{X} = \oplus$,

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

After the second CNOT:

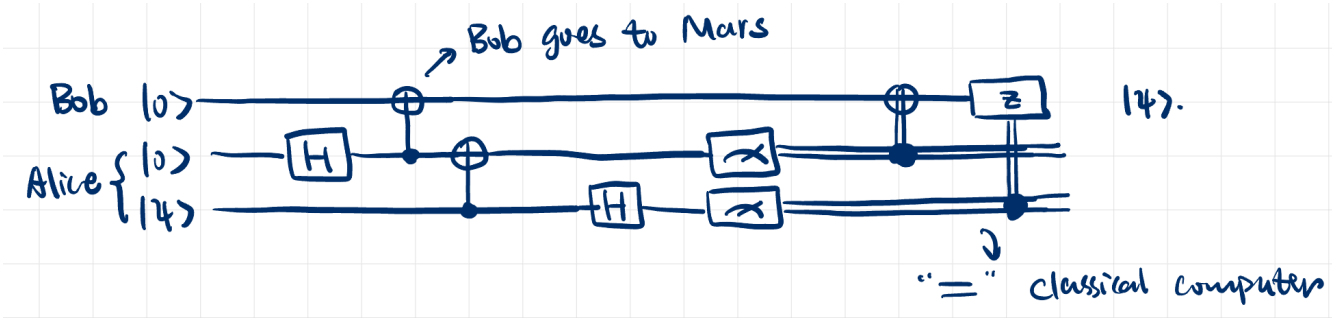
$$\frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) + \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)|1\rangle = \frac{1}{\sqrt{2}}|+\rangle|1\rangle.$$

After the final $\boxed{H}$: $|0\rangle|1\rangle$.

[$H|0\rangle = |+\rangle$, *and* $|0\rangle = HH|0\rangle = H|+\rangle$.]

6.2 Quantum Teleportation

Alice wants to send Bob unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.



After the first CNOT:

$$|\psi\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

After the second CNOT:

$$\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle).$$

After H,

$$\begin{aligned}&\frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle)\\ &\quad = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]\end{aligned}$$

After Alice's measurement, Bob's qubit is:

- $00 \to \alpha|0\rangle + \beta|1\rangle$
- $01 \to \alpha|1\rangle + \beta|0\rangle \xrightarrow{\text{Apply } \oplus} \alpha|0\rangle + \beta|1\rangle$
- $10 \to \alpha|0\rangle - \beta|1\rangle \xrightarrow{\text{Apply } \boxed{Z}} \alpha|0\rangle + \beta|1\rangle$
- $11 \to \alpha|1\rangle - \beta|0\rangle \xrightarrow[\text{Apply } \boxed{Z}]{\text{Apply } \oplus} \alpha|0\rangle + \beta|1\rangle$.

6.3 Scheme for Instantaneous Communication

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle).$$

- Alice chooses the measure in z-basis or x-basis.
- Bob clones his qubit 100 times (not actually possible) and measures in z-basis.
- If Alice measured in z-basis, qubit state is $|00\rangle$ or $|11\rangle$, and Bob gets same result every time.
- If Alice measured in x-basis, the state is $|{+}{+}\rangle$ or $|{-}{-}\rangle$, and Bob gets $|0\rangle \sim 50\%$ and $|1\rangle \sim 50\%$.

6.4 No-Cloning Theorem

We want to clone $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ onto qubit, initially in state $|\varphi\rangle$.

$$|\psi\rangle|\varphi\rangle \to |\psi\rangle|\psi\rangle.$$

Is there an operator U that does this?

$$\begin{aligned}U|\psi\rangle|\varphi\rangle = |\psi\rangle|\psi\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)\\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle\end{aligned}$$

Must work if $|\psi\rangle$ is $|0\rangle$ or $|1\rangle$: So, $U|0\rangle|\varphi\rangle = |00\rangle$, and $U|1\rangle|\varphi\rangle = |11\rangle$, which means

$$\begin{aligned} U|\psi\rangle|\varphi\rangle &= U(\alpha|0\rangle + \beta|1\rangle)|\varphi\rangle \\ &= \alpha U|0\rangle|\varphi\rangle + \beta U|1\rangle|\varphi\rangle \\ &= \alpha|00\rangle + \beta|11\rangle . \end{aligned}$$

Since the two expressions do not match each other, we reach a contradiction, and such U that clones a qubit does not exist.

6.5 Quantum Cryptography – Quantum Key Distribution

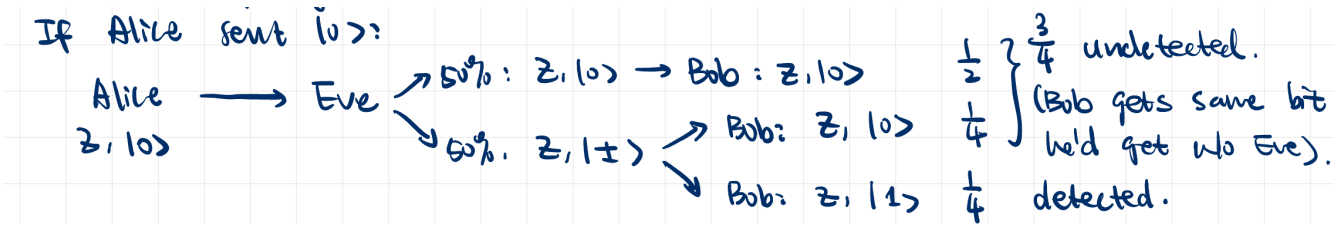
Alice wants to generate a secret sequence of bits, known only to her and Bob, that they can use to encrypt data they send to each other:

message		0	1	1	0
key	$\oplus$	1	1	0	1
cipher (encrypted message)		1	0	1	1

- Alice randomly picks a bit (0 or 1) and basis (z or x), then sends qubit to Bob. Bob randomly pick measurement basis:

Alice's bit	0	1	0	1	1	0	1	1	1
Alice's bases	z	z	x	z	x	x	x	z	z
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$
Bob's bases	z	x	x	z	z	x	z	x	z
bob's measurement	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's bit	0	1	0	1	0	0	1	0	1

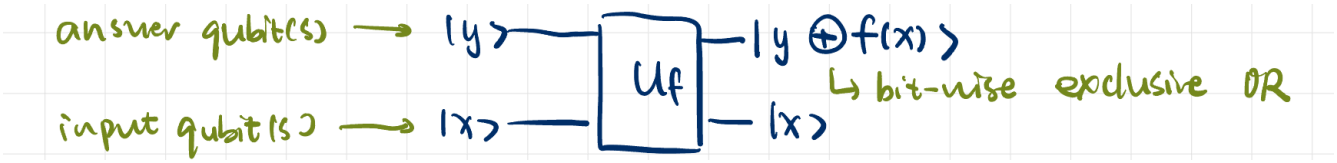
- Alice and Bob publicly reveal the basis used for each qubit. When their bases were the same, their bits have to be the same: secrete key is 00101.
- To determine if Eve eavesdropped, they publicly reveal (and eliminate from their key) some bits (when they both used the same basis) to see if they agree.



7 Deutsch's Algorithm

7.1 Quantum Oracle

- *Quantum Oracle* is a quantum gate/operator that incorporates a function $f(x)$.



$x, y, f(x)$ are all binary numbers.

$$|x\rangle |y\rangle \xrightarrow{U_f} |x\rangle |y \oplus f(x)\rangle ,$$

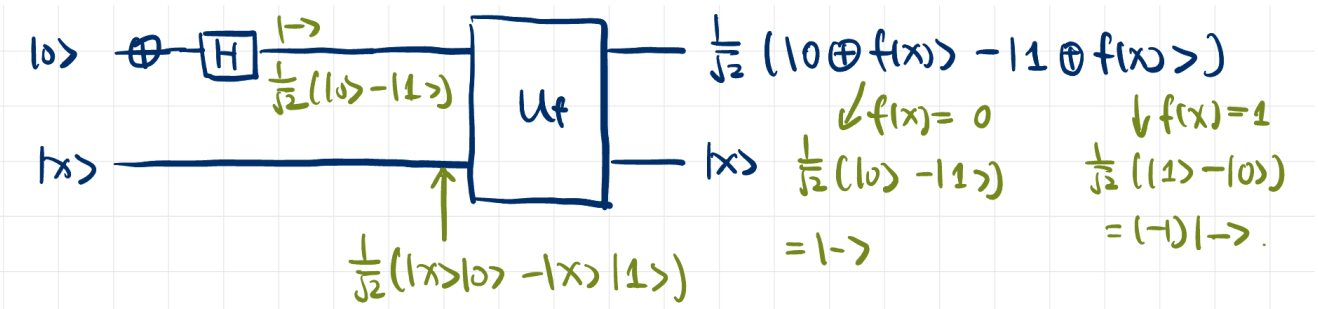
where $\oplus$ is the bit-wise exclusive OR operator.

Let $x, y, f(x)$ each be 1 bit for now (they could have more bits in reality).

- To determine $f(0)$ and $f(1)$, we can set $y = 0$:

$$|0\rangle |0\rangle \xrightarrow{U_f} |0\rangle |f(0)\rangle$$
$$|1\rangle |0\rangle \xrightarrow{U_f} |1\rangle |f(1)\rangle .$$

Let's try



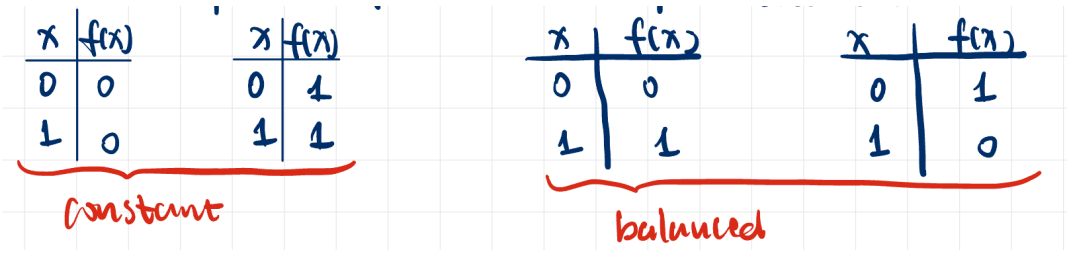
The final state is $\underbrace{(-1)^{f(x)}}_{\text{phase kickback}} |x\rangle |-\rangle$.

- Phase Oracle:

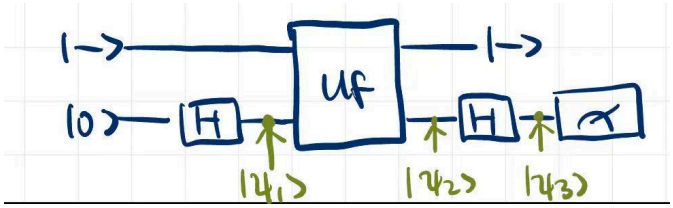
$$|x\rangle \xrightarrow{\boxed{U_f}} (-1)^{f(x)} |x\rangle .$$

7.2 Deutsch's Algorithm

- Consider all possible functions that input one bit and output one bit:



Task: Determine if $f(x)$ is constant or balanced.



Recall:

$$|x\rangle\,|-\rangle \xrightarrow{U_f} (-1)^{f(x)}\,|x\rangle\,|-\rangle\,.$$

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|-\rangle + |1\rangle\,|-\rangle)\\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}\Big[(-1)^{f(0)}\,|0\rangle\,|-\rangle + (-1)^{f(1)}\,|1\rangle\,|-\rangle\Big]\\
&= \frac{1}{\sqrt{2}}(-1)^{f(0)}\Big[|0\rangle + (-1)^{f(1)-f(0)}\,|1\rangle\Big]\,|-\rangle
\end{aligned}$$

1. Constant case: $f(0) = f(1)$:

$$(-1)^{f(0)}\,|+\rangle\,|-\rangle$$

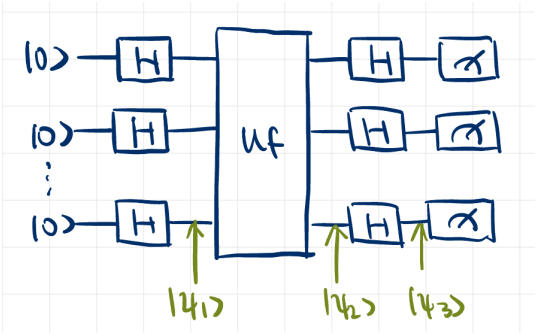
2. Balanced cases: $f(0) \neq f(1)$:

$$(-1)^{f(0)}\,|-\rangle\,|-\rangle$$

$$|\psi_3\rangle = \begin{cases} |0\rangle\,, & \text{if } f(0) = f(1)\\ |1\rangle\,, & \text{if } f(0) \neq f(1)\end{cases}$$

- Extended to Multiple Qubits: Deutsch-Jozsa Algorithm

  Consider: n bit X, $f(X)$ is still one bit.



Recall (phase) oracle:

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle .$$

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\cdots(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}}(|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2^n}}\left[(-1)^{f(00\cdots0)}|00\cdots0\rangle + (-1)^{f(00\cdots1)}|00\cdots1\rangle + (-1)^{f(11\cdots1)}|11\cdots1\rangle\right] \end{aligned}$$

1. If $f(X) =$ constant,

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}(-1)^{f(X)} \underbrace{[|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle]}_{\text{unchanged from } |\psi_1\rangle \text{ (neglecting global phase)}}$$

   So, $U_f = I$. Since $H^2 = I$, $|\psi_3\rangle = |00\cdots0\rangle$ if $f(X)$ is constant.

2. Prove that if $f(X)$ is balanced, $\mathbf{P}(|\psi_3\rangle = |00\cdots0\rangle) = 0$.

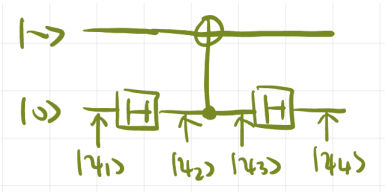
$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}}\left[(-1)^{f(00\cdots)}H|0\rangle H|0\rangle\cdots H|0\rangle + (-1)f(00\cdots1)\right]H|0\rangle H|0\rangle\cdots H|1\rangle + \cdots$$

   Keep track only of $|00\cdots0\rangle$ terms:

$$\frac{1}{\sqrt{2^n}}\left[(-1)^{f(00\cdots0)}|00\cdots0\rangle + (-1)^{f(00\cdots1)}|00\cdots0\rangle + \cdots\right] \underbrace{\frac{1}{\sqrt{2^n}}}_{\text{from } \boxed{H}}$$

   If $f(X)$ is balanced, just as many exponents $= 0$ as 1. So, just as many $(-1)^0 = 1$ as $(-1)^1 = -1$ in sum. Hence, the sum $= 0$.

Example 7.2.1



Solution 1.

$$\begin{aligned} |\psi_1\rangle &= |0\rangle|-\rangle = |0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned}$$

$$
\begin{aligned}
|\psi_3\rangle &= \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= |-\rangle\,|-\rangle \\
|\psi_4\rangle &= |1\rangle\,|-\rangle\,.
\end{aligned}
$$

□

8 Grover's Search Algorithm

Motivation: In a phonebook with a million names, listed alphabetically, find the name of the person with a specific phone number.

- Classical computer: no choice but brute-force search. On average, we will succeed after $500,000$ steps.
- Grover's algorithm will succeed after ~ 1000 steps (queries).

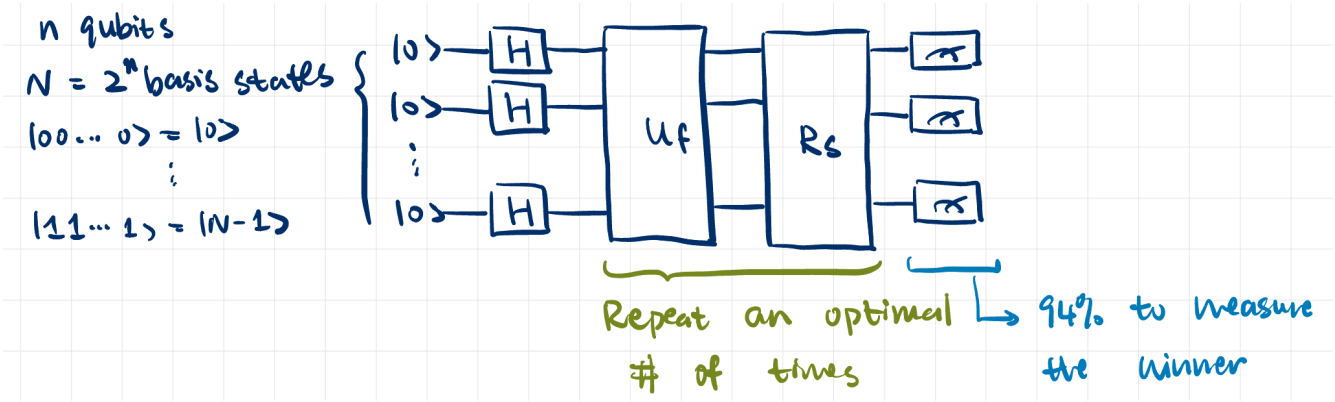
Set-Up: The function

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

So, the oracle that "flags" the winner is given by

$$U_f = (-1)^{f(x)} |x\rangle = \begin{cases} -|x\rangle & \text{if } x = w \\ |x\rangle & \text{o/w.} \end{cases}$$

8.1 Grover's Circuit



Recall:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} = |s\rangle \quad [\textit{equally weighted superposition of basis vectors}]$$

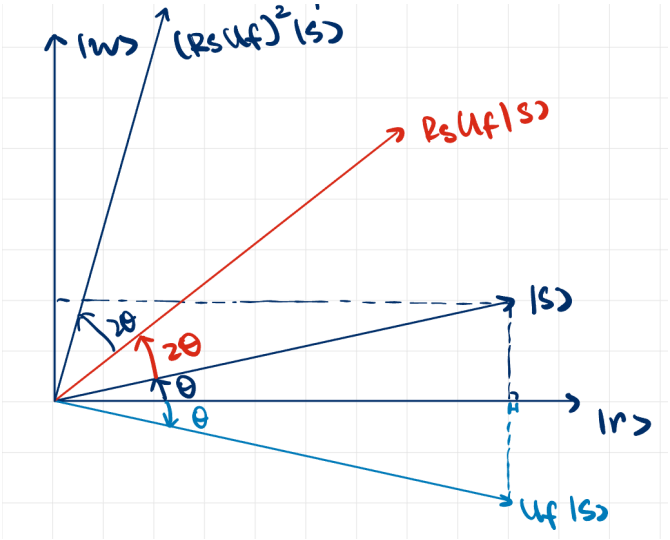
$$= \frac{1}{\sqrt{N}} \left(|w\rangle + \sum_{j \neq w} |j\rangle \right)$$

$$= \frac{1}{\sqrt{N}} |w\rangle + \frac{1}{\sqrt{N}} \sum_{j \neq w} |j\rangle$$

$$= \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} \cdot \underbrace{\frac{1}{\sqrt{N-1}} \sum_{j \neq w} |j\rangle}_{=|r\rangle = \text{normalized superposition of "rejects" (non-wnners)}}$$

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|r\rangle \quad [|w\rangle \text{ and } |r\rangle \text{ from an orthonormal basis: } \frac{1}{N} + \frac{N-1}{N} = 1.]$$
$$= \sin\theta\,|w\rangle + \cos\theta\,|r\rangle\,.$$

A general representation:



$$|s\rangle = \sin\theta\,|w\rangle + \cos\theta\,|r\rangle$$

- Apply U_f:

  $$U_f\,|s\rangle = -\sin\theta\,|w\rangle + \cos\theta\,|r\rangle$$

  Reflects $|s\rangle$ about the x-axis.

- Apply R_s that reflects about $|s\rangle$
- Net effect of R_sU_f is to notate 2θ counter-clockwise.
- **Goal**: Let the final result to be close to $|w\rangle$

Determine optimal number t of applications of R_sU_f:

$$\theta + t(2\theta) = \frac{\pi}{2}$$
$$t = \frac{\pi}{4\theta} - \frac{1}{2}, \qquad \text{where } \sin\theta = \frac{1}{\sqrt{N}}$$
$$\implies \theta = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right) \approx \frac{1}{\sqrt{N}},\ N \to \infty.$$
$$t \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2}, \qquad \text{and round to nearest integers.}$$

If there are p different winner states: $|w_1\rangle, |w_2\rangle, \ldots, |w_p\rangle$, Then,

$$|s\rangle = \frac{1}{\sqrt{N}}(|w_1\rangle + |w_2\rangle + \cdots + |w_p\rangle) + \underbrace{\sum_{N-p} |j\rangle}_{\text{rejects}}$$

- Normalized combined winner state:

$$\frac{1}{\sqrt{p}}(|w_1\rangle + |w_2\rangle + \cdots + |w_p\rangle) = |\text{winners}\rangle$$

- Normalized combined reject state:

$$\frac{1}{\sqrt{N-p}} \sum_{\text{rejects}} |j\rangle = |r\rangle .$$

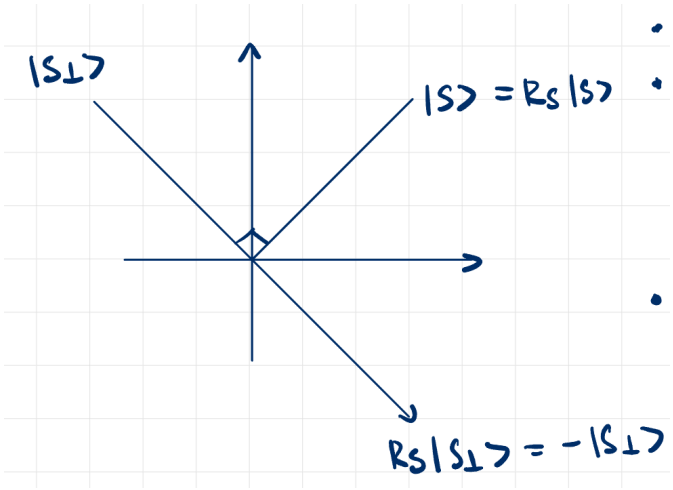
So, $|s\rangle = \sqrt{\frac{p}{N}}\,|\text{winners}\rangle + \sqrt{\frac{N-p}{N}}\,|r\rangle$.

$$\sin\theta = \sqrt{\frac{p}{N}} \implies \theta = \sin^{-1}\sqrt{\frac{p}{N}} \approx \sqrt{\frac{p}{N}}.$$

Then,

$$\text{optimal } t = \frac{\pi}{4}\sqrt{\frac{N}{p}} - \frac{1}{2}.$$

What is R_s?



- R_s is a reflection about $|s\rangle$.
- Observation:

$$RsS\,|s\rangle = |s\rangle$$
$$R_s\,|S_\perp\rangle = -\,|s_\perp\rangle$$

- **Claim** $R_s = 2\,|s\rangle\,\langle s| - I$.

  Proof 1.

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

Moreover,

$$R_s |s_\perp\rangle = 2 |s\rangle \langle s|s_\perp\rangle - I |s_\perp\rangle = - |s_\perp\rangle$$

Q.E.D. ■

Example 8.1.1

$N = 8$, single winner $|w\rangle = |3\rangle$.

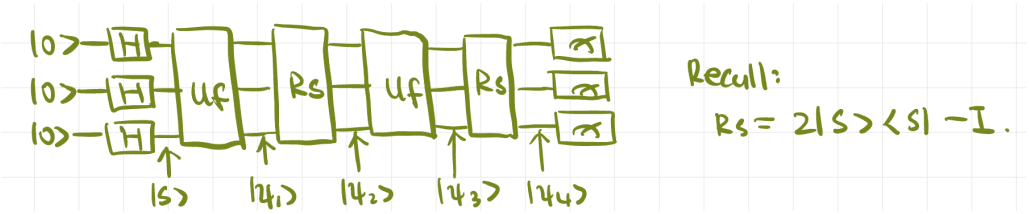
$$|s\rangle = \frac{1}{\sqrt{8}} \sum_{j=0}^{7} |j\rangle = \frac{1}{\sqrt{8}} |3\rangle + \frac{1}{\sqrt{8}} \sum_{j\neq 3} |j\rangle$$
$$|r\rangle = \frac{1}{\sqrt{7}} \sum_{j\neq 3} |j\rangle$$

So,

$$|s\rangle = \frac{1}{\sqrt{8}} |3\rangle + \sqrt{\frac{7}{8}} |r\rangle \implies |r\rangle = \sqrt{\frac{8}{7}} |s\rangle - \frac{1}{\sqrt{7}} |3\rangle \quad \text{and} \quad \langle 3|s\rangle = \frac{1}{\sqrt{8}}.$$

Number of iterations of $(R_s U_f)$ is

$$t = \frac{\pi}{4}\sqrt{8} - \frac{1}{2} \approx 2.$$



$$|\psi_1\rangle = U_f |s\rangle = -\frac{1}{\sqrt{8}} |3\rangle + \sqrt{\frac{7}{8}} |r\rangle = |s\rangle - \frac{2}{\sqrt{8}} |3\rangle$$
$$\begin{aligned}
|\psi_2\rangle = R_s |\psi_1\rangle &= 2 |s\rangle \langle s|s\rangle - I |s\rangle - \frac{2}{\sqrt{8}} \cdot 2 |s\rangle \langle s|3\rangle + I \frac{2}{\sqrt{8}} |3\rangle \\
&= 2 |s\rangle - |s\rangle - \frac{4}{\sqrt{8}} \cdot \frac{1}{\sqrt{8}} + \frac{2}{\sqrt{8}} |3\rangle \\
&= |s\rangle - \frac{1}{2} |s\rangle + \frac{2}{\sqrt{8}} |3\rangle \\
&= \frac{1}{2} |s\rangle + \frac{2}{\sqrt{8}} |3\rangle \\
&= \frac{1}{2} \left(\frac{1}{\sqrt{8}} |3\rangle + \sqrt{\frac{7}{8}} |r\rangle \right) + \frac{2}{\sqrt{8}} |3\rangle \\
&= \left(\frac{1}{2\sqrt{8}} + \frac{2}{\sqrt{8}} \right) |3\rangle + \frac{1}{2} \sqrt{\frac{7}{8}} |r\rangle \\
&= \frac{5}{2\sqrt{8}} |3\rangle + \frac{1}{2} \sqrt{\frac{7}{8}} |r\rangle
\end{aligned}$$

$$
\begin{aligned}
|\psi_3\rangle = U_f\,|\psi_2\rangle &= -\frac{5}{2\sqrt{8}}\,|3\rangle + \frac{1}{2}\sqrt{\frac{7}{8}}\,|r\rangle \\
&= -\frac{5}{2\sqrt{8}}\,|3\rangle + \frac{1}{2}\sqrt{\frac{7}{8}}\left(\sqrt{\frac{8}{7}}\,|s\rangle - \frac{1}{\sqrt{7}}\,|3\rangle\right) \\
&= -\frac{5}{2\sqrt{8}}\,|3\rangle + \frac{1}{2}\,|s\rangle - \frac{1}{2\sqrt{8}}\,|3\rangle \\
&= \frac{1}{2}\,|s\rangle - \frac{3}{\sqrt{8}}\,|3\rangle\,. \\
|\psi_4\rangle = R_s\,|\psi_3\rangle &= \frac{1}{2}\,|s\rangle - 2\frac{3}{\sqrt{8}}\,|s\rangle\,\langle s|3\rangle + \frac{3}{\sqrt{8}}\,|3\rangle \\
&= \frac{1}{2}\,|s\rangle - 2\frac{3}{\sqrt{8}}\cdot\frac{1}{\sqrt{8}}\,|s\rangle + \frac{3}{\sqrt{8}}\,|3\rangle \\
&= \frac{1}{2}\,|s\rangle - \frac{3}{4}\,|s\rangle + \frac{3}{\sqrt{8}}\,|3\rangle \\
&= -\frac{1}{4}\,|s\rangle + \frac{3}{\sqrt{8}}\,|3\rangle \\
&= -\frac{1}{4}\left(\frac{1}{\sqrt{8}}\,|3\rangle + \sqrt{\frac{7}{8}}\,|r\rangle\right) + \frac{3}{\sqrt{8}}\,|3\rangle \\
&= -\frac{1}{4\sqrt{8}}\,|3\rangle + \frac{3}{\sqrt{8}}\,|3\rangle - \frac{1}{4}\sqrt{\frac{7}{8}}\,|r\rangle \\
&= \frac{11}{4\sqrt{8}}\,|3\rangle - \frac{1}{4}\sqrt{\frac{7}{8}}\,|r\rangle \\
\text{probability of } |3\rangle &= \left(\frac{11}{4\sqrt{8}}\right)^2 = \frac{121}{128}.
\end{aligned}
$$

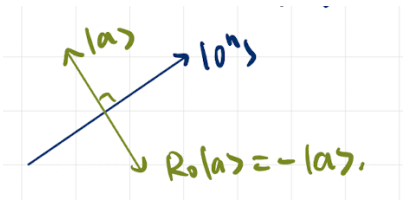
8.2 How to construct R_s out of Elementary Gates?

$$
R_s = 2\,|s\rangle\,\langle s| - I, \quad \text{where } |s\rangle = H^{\otimes n}\,|0\rangle^{\otimes n} = H^{\otimes n}\,|0^n\rangle \implies \langle s| = \langle 0^n|\,H^{\otimes n}.
$$

$$
\begin{aligned}
R_s = 2\,|s\rangle\,\langle s| - I &= 2H^{\otimes n}\,|0^n\rangle\,\langle 0^n|\,H^{\otimes n} - I \\
&= H^{\otimes n}\,\underbrace{\left(2\,|0^n\rangle\,\langle 0^n| - I\right)}_{R_0}\,H^{\otimes n}
\end{aligned}
$$

What does R_0 do?

- To $|0^n\rangle$, $R_0\,|0^n\rangle = 2\,|0^n\rangle\,\langle 0^n|0^n\rangle - |0^n\rangle = |0^n\rangle \implies$ no effects.
- To $|a\rangle \neq |0^n\rangle$: $R_0 = |a\rangle = -\,|a\rangle$.

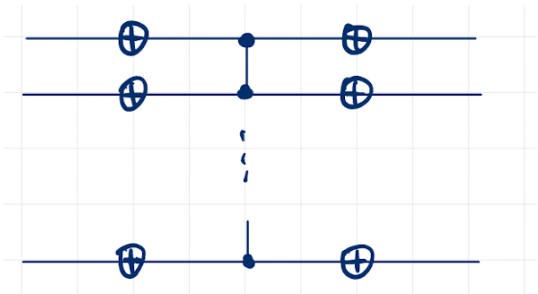


So, R_0 is a reflection about $|0^n\rangle$.

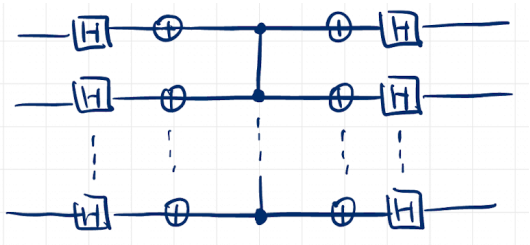
To make R_0, recall $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -1$. Controlled Z multiplies only $|11\rangle$ by -1.

R_0 multiplies every computational basis state except the all-zero state by -1. Let's construct first an operator that multiplies only the all-zero state by -1:

Then, $-R_0$ is given by:



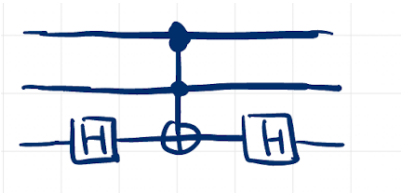
This multiplies $|0^n\rangle$ by -1. Then, R_s is



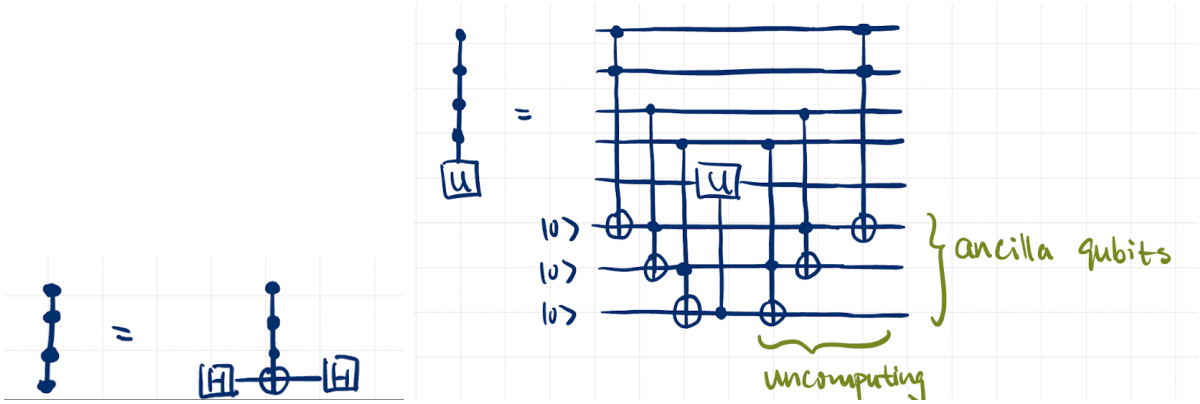
How to make controlled Z and Doubly controlled Z?

- Controlled Z: drop control (the $\cdot$) on $\boxed{Z}$

- Doubly controlled Z:



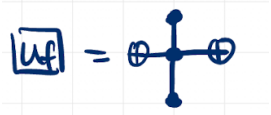
- More controlled Z gates:



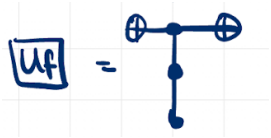
How to construct U_f, using knowledge of w (to test whether Grover's Algorithm works)

- U_f multiplies $|w\rangle$ by -1. So, if $|2\rangle = |111\rangle$,

- If $|w\rangle = |101\rangle$,



- If $|w\rangle = |110\rangle$,

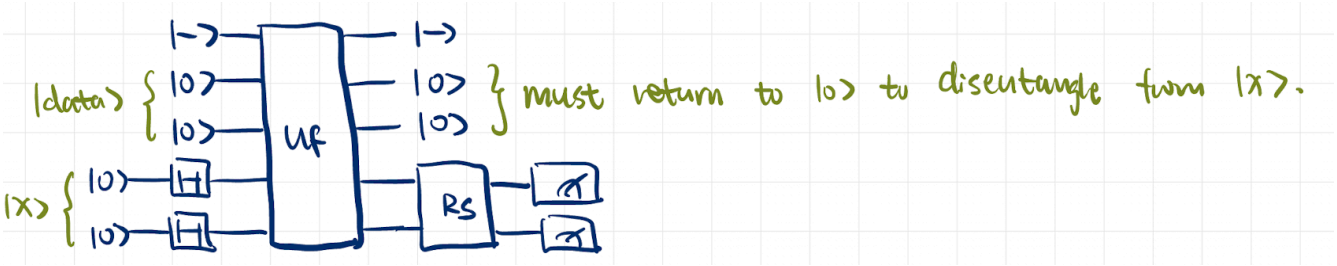


- If there are 2 winners, $|w_1\rangle = |101\rangle$ and $|w_2\rangle = |110\rangle$, then

8.3 Quantum Database

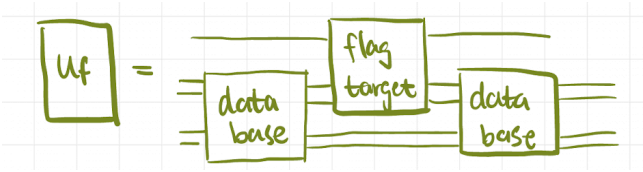
Goal: Construct U_f without assuming the solution

- We will use $|x\rangle|0\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle$, where $f(x) = \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{o/w.} \end{cases}$
- If $|x\rangle$ has 2 qubits:

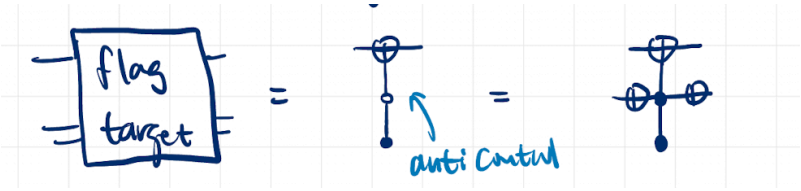


Example 8.3.1 Phonebook

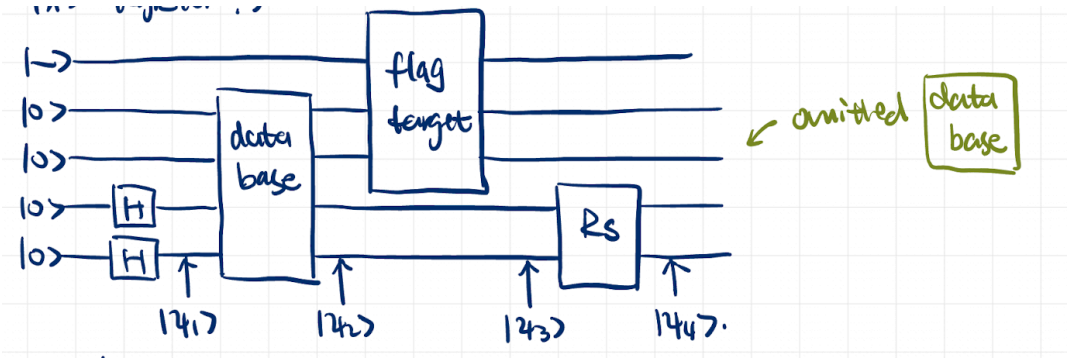
$\|x\rangle = \|\text{name}\rangle$	$\|\text{data}\rangle = \|\text{phoneNumber}\rangle$
$\|00\rangle$	$\|11\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|00\rangle$
$\|11\rangle$	$\|01\rangle$



- What $|x\rangle = |w\rangle$ that gives $|\text{data}\rangle = |10\rangle$?



- What happens if we forget to uncompute (returning the ancilla qubits, the data register, to $|00\rangle$, to disentangle them from the $|x\rangle$ register)?



1. $|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|00\rangle\,|-\rangle$
2. $|\psi_2\rangle = \frac{1}{2}(|00\rangle\,|11\rangle + |01\rangle\,|10\rangle + |10\rangle\,|00\rangle + |11\rangle\,|01\rangle)\,|-\rangle$

   Effect of database: change the $|y\rangle$ register according to the $|x\rangle$ register and the database table.
3. $|\psi_3\rangle = \frac{1}{2}(|00\rangle\,|11\rangle - |01\rangle\,|10\rangle + |10\rangle\,|00\rangle + |11\rangle\,|01\rangle)\,|-\rangle$

   Effect of flag target: change the sign of the winning state.
4. $R_S = 2\,|s\rangle\,\langle s| - I$. $\langle s|x\rangle = \frac{1}{2}$. So,

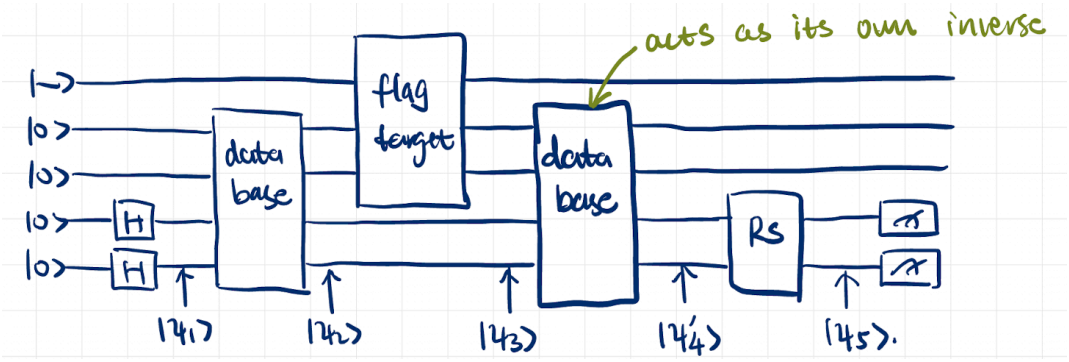
$$R_s\,|x\rangle = (2\,|s\rangle\,\langle s| - I)\,|x\rangle = 2\,|s\rangle\,\langle s|x\rangle - |x\rangle = |s\rangle - |x\rangle$$
$$|\psi_4\rangle = \frac{1}{2}[(|s\rangle - |00\rangle)\,|11\rangle - (|s\rangle - |01\rangle)\,|10\rangle + (|s\rangle - |10\rangle)\,|00\rangle + (|s\rangle - |11\rangle)\,|01\rangle]\,|-\rangle$$

5. Imaging measuring $|\text{data}\rangle$ register, suppose we get $|11\rangle$. Then, $|x\rangle$ register is

$$|s\rangle - |00\rangle = -\frac{1}{2}\,|00\rangle + \frac{1}{2}\,|01\rangle + \frac{1}{2}\,|10\rangle + \frac{1}{2}\,|11\rangle\,.$$

   So, we have 25% of all $|x\rangle$ values. Grover's algorithm fails if we don't uncompute.

- The correct circuit:



1. $|\psi_3\rangle = \frac{1}{2}(|00\rangle\,|11\rangle - |01\rangle\,|10\rangle + |10\rangle\,|00\rangle + |11\rangle\,|01\rangle)\,|-\rangle$
2. $|\psi_4'\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)\,|00\rangle\,|0\rangle$

Effect of database: turn everything back to $|00\rangle$.

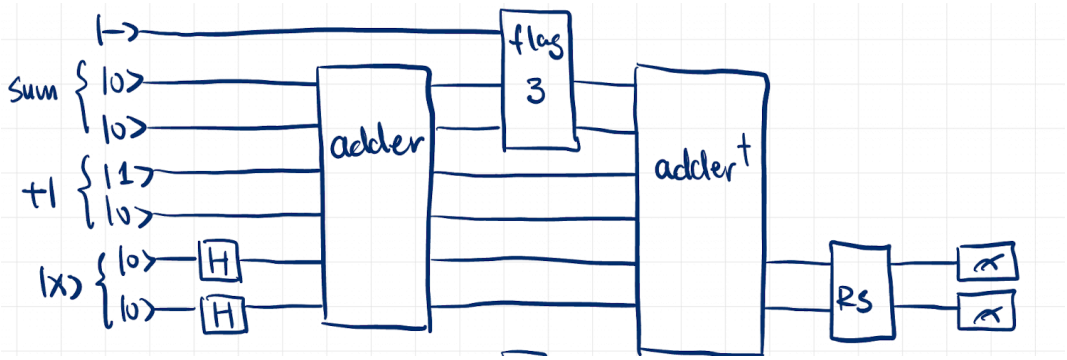
3. $R_s|x\rangle = |s\rangle - |x\rangle$:

$$\begin{aligned}|\psi_5\rangle &= \frac{1}{2}[|s\rangle - |00\rangle - (|s\rangle - |01\rangle) + (|s\rangle - |10\rangle) + (|s\rangle - |11\rangle)]\,|00\rangle\,|-\rangle \\ &= \frac{1}{2}(2\,|s\rangle - |00\rangle + |01\rangle - |10\rangle - |11\rangle)\,|00\rangle\,|-\rangle \\ &\quad [2\,|s\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle] \\ &= \frac{1}{2}(2\,|01\rangle)\,|00\rangle\,|-\rangle = |01\rangle\,|00\rangle\,|-\rangle\,.\end{aligned}$$

The probability of measuring $|01\rangle = 100\%$. So, the Grover's algorithm succeeds!

8.4 Application of Grover's Algorithm

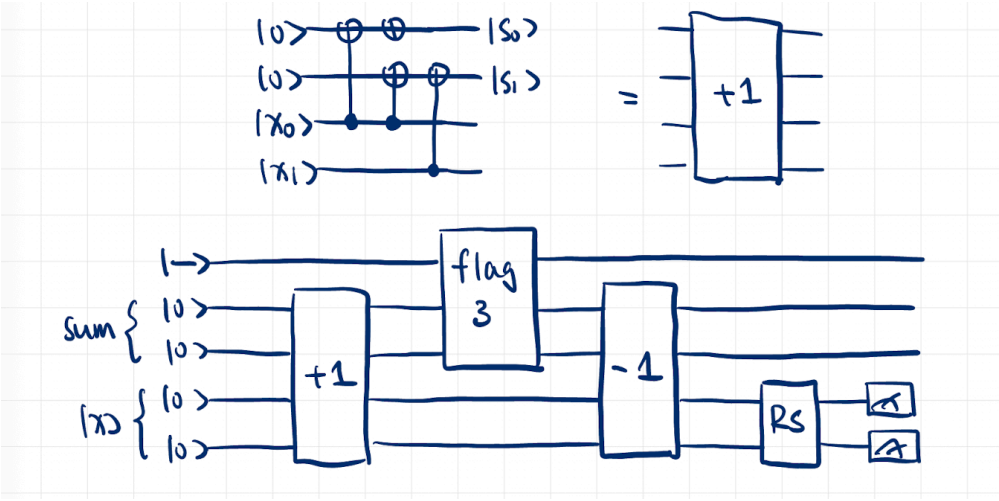
Solve $x + 1 = 3$. Assume candidate $x = 1, 2, 3$.



Or, we could handwrite +1:

$$\begin{array}{rccc} \text{carry} \rightarrow & x_0 & & \\ & x_1 & x_0 & \\ + & & & 1 \\ \hline & s_1 & s_2 & \end{array}$$

We have $s_0 = \overline{x}_0$ and $s_1 = x_0 \oplus x_1$, where $\oplus$ is the exclusively or operator. Making it quantum:



9 Quantum Fourier Transformation

9.1 Discrete Fourier Transform (DFT)

Goal: allows us to determine the period of elements in a vector.

Example 9.1.1

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\\0\\0\end{pmatrix} \quad \text{has a period of } 3$$

$$\frac{1}{\sqrt{3}}\begin{pmatrix}1\\0\\1\\0\\1\\0\end{pmatrix} \quad \text{has a period of } 2$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\\1\\0\\0\\0\end{pmatrix} \quad \text{has a period of } 4$$

The discrete Fourier transform (DFT) of $\begin{pmatrix}a_0\\a_1\\\vdots\\a_{N-1}\end{pmatrix}$ is $\begin{pmatrix}\varphi_0\\\varphi_1\\\vdots\\\varphi_{N-1}\end{pmatrix}$, where

$$\varphi_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} a_j \omega^{jk}, \quad \text{and} \quad \omega = e^{2\pi \mathrm{i}/N}.$$

So,

$$\begin{aligned}\varphi_0 &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} a_j\omega^0 = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} a_j \\ &= \frac{1}{\sqrt{N}}(a_0 + a_1 + \cdots + a_{N-1}) \\ \varphi_1 &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} a_j\omega^j = \frac{1}{\sqrt{N}}\big(a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{N-1}\omega^{N-1}\big).\end{aligned}$$

In matrix form,

$$\begin{pmatrix}\varphi_0\\ \varphi_1\\ \varphi_2\\ \vdots\\ \varphi_{N-1}\end{pmatrix} = \underbrace{\frac{1}{\sqrt{N}}\begin{pmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1}\\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2N-2}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \omega^{N-1} & \omega^{2N-2} & \cdots & \omega^{(N-1)^2}\end{pmatrix}}_{\text{DFT}} \begin{pmatrix}a_0\\ a_1\\ a_2\\ \vdots\\ a_{N-1}\end{pmatrix}.$$

Example 9.1.2

$N = 6$, so,

$$\omega = e^{2\pi \mathrm{i}/6} = \frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2},$$

and

$$\text{DFT} = \begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1\\ 1 & \omega & \omega^2 & \omega^4 & \omega^4 & \omega^5\\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10}\\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15}\\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20}\\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25}\end{pmatrix}$$

- $\text{DFT}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\\0\\0\end{pmatrix} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\0\\1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{3}}\begin{pmatrix}\varphi_0\\ \varphi_1\\ \varphi_2\\ \varphi_3\\ \varphi_4\\ \varphi_5\end{pmatrix}$.

  The indices (subscript of φ) of the non-zero elements are $0, 2, 4$, and they are multiples of 2.

$$2 = \frac{N}{r} = \frac{6}{r}, \quad \text{where } r = \text{period}.$$

- $\text{DFT} \cdot \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \varphi_0 \\ \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \\ \varphi_5 \end{pmatrix}$.

  Nonzero elements' indices: $0, 3$. Multiples of 3:

$$3 = \frac{N}{r} = \frac{6}{r} \implies r = 2.$$

Rule to find the period Find the number that indices of nonzero elements are multiple of, set equal to $\frac{N}{r}$, solve for r.

9.2 Quantum Fourier Transform (QFT)

Quantum Fourier transform is just the DFT written in quantum form. Let's write DFT in kets:

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots = a_0 |0\rangle + a_1 |1\rangle + \cdots + a_{N-1} |N-1\rangle$$

$$= \sum_{j=0}^{N-1} a_j |j\rangle = |\psi\rangle$$

$$\text{QFT} |\psi\rangle = |\psi\rangle = \begin{pmatrix} \varphi_0 \\ \vdots \\ \varphi_{N-1} \end{pmatrix} = \sum_{k=0}^{N-1} \varphi_k |k\rangle = \sum_{k=0}^{N-1} \underbrace{\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi \mathrm{i} jk/N}}_{\text{amplitude of } |k\rangle} |k\rangle$$

- Special case: QFT of basis state:

$$|j'\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad a_j = \begin{cases} 0, & j \neq j' \\ 1, & j = j'. \end{cases}$$

So,

$$\varphi_k = \frac{1}{\sqrt{N}} e^{2\pi \mathrm{i} j' k/N}$$
$$\mathrm{QFT}\left|j'\right\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi \mathrm{i} j' k/N} \left|k\right\rangle \quad \text{for computational basis state } \left|j'\right\rangle$$

Renaming $j \leftarrow j'$.

- QFT with periodic amplitudes: let $a_{j+r} = a_j$.

  For simplicity, assume $\dfrac{N}{r} = \text{integer} = m$.

$$\mathrm{QFT}\left|\psi\right\rangle = \sum_{k=0}^{N-1} \underbrace{\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi \mathrm{i} j l/N}}_{\text{amplitude of } |k\rangle} \left|k\right\rangle$$

$$\begin{aligned}
\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi \mathrm{i} jk/N} &= \frac{1}{\sqrt{N}} \left(\sum_{j=0}^{r-1} a_j e^{2\pi \mathrm{i} jk/N} + \sum_{j=r}^{2r-1} a_j e^{2\pi \mathrm{i} jk/N} + \cdots + \sum_{j=N-r}^{N-1} a_j e^{2\pi \mathrm{i} jk/N} \right) \\
&= \frac{1}{\sqrt{N}} \sum_{j=0}^{r-1} a_j e^{2\pi \mathrm{i} jk/N} + \underbrace{a_{j+r}}_{=a_j} e^{2\pi \mathrm{i}(j+r)k/N} + \cdots + \underbrace{a_{j+N-r}}_{=a_j} e^{2\pi \mathrm{i}(j+N-r)k/N} \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{r-1} a_j e^{2\pi \mathrm{i} jk/N} \left(1 + e^{2\pi \mathrm{i} rk/N} + \cdots + e^{2\pi \mathrm{i}(N-r)k/N}\right) \\
&= \frac{1}{\sqrt{N}} \sum_{j=0}^{r-1} a_j e^{2\pi \mathrm{i} jk/N} \left(1 + e^{2\pi \mathrm{i} rk/N} + \cdots + e^{2\pi \mathrm{i}(\underbrace{(N/r)}_{=m} - 1) rk/N} \right) \\
&= \frac{1}{\sqrt{N}} \sum_{j=0}^{r-1} a_j e^{2\pi \mathrm{i} jk/N} \underbrace{\left(1 + e^{2\pi \mathrm{i} rk/N} + \cdots + e^{2\pi \mathrm{i}(m-1) rk/N}\right)}_{(\star)}.
\end{aligned}$$

We want to show when $(\star)$ will be 0. This is a geometric series, and recall

$$1 + \omega + \omega^2 + \cdots + \omega^{m-1} = \frac{\omega^m - 1}{\omega - 1} \quad \text{if } \omega \neq 1.$$

With $\omega = e^{2\pi \mathrm{i} rk/N}$, $\omega^m = e^{2\pi \mathrm{i} \underbrace{rN}_{=N} k/N} = e^{2\pi \mathrm{i} k}$.

Amplitude of $|k\rangle$ is

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{r-1} a_j e^{2\pi \mathrm{i} jk/N} \left(\frac{e^{2\pi \mathrm{i} k} - 1}{e^{2\pi \mathrm{i} rk/N} - 1} \right).$$

The numerator $= 0$ for all k. So, amplitude of $|k\rangle$ is 0 unless the denominator is 0. Therefore, $e^{2\pi \mathrm{i} rk/N = 1}$.

From math, we have $(e^a)^b = e^{ab}$ only if a is real or b is integer. So, $\dfrac{rk}{N}$ is an integer.

how to design QFT circuit? Recall that

$$\mathrm{QFT}\,|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi \mathrm{i} jk/N}\,|k\rangle$$

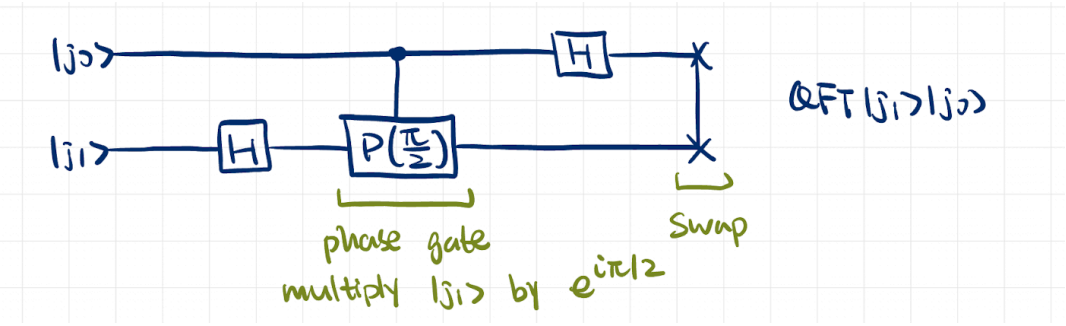
- Single qubit, $N = 2$, basis states

$$\mathrm{QFT}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$\mathrm{QFT}\,|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi \mathrm{i}/2}\,|1\rangle\right) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

  So, $\mathrm{QFT} = H$.

- For 2 qubits, $N = 4$.

$$\mathrm{QFT}\,|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$
$$\mathrm{QFT}\,|1\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle + \mathrm{i}\,|1\rangle).$$



10 Quantum Phase Estimation (QPE)

Recall quantum Fourier transformation:

$$\mathrm{QFT}\,|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi \mathrm{i} jk/N}\,|k\rangle\,.$$

- With 2 qubits, $N=4$,

$$\begin{aligned}
\mathrm{QFT}\,|0\rangle = |00\rangle &= \frac{1}{2}(|0\rangle+|1\rangle+|2\rangle+|3\rangle) = \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\\
\mathrm{QFT}\,|1\rangle = |01\rangle &= \frac{1}{2}\sum_{k=0}^{3} e^{2\pi \mathrm{i}k/4} = \frac{1}{2}(|0\rangle+\mathrm{i}\,|1\rangle-|2\rangle-\mathrm{i}\,|3\rangle)\\
&= \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle+\mathrm{i}\,|1\rangle)\\
\mathrm{QFT}\,|2\rangle = |10\rangle &= \frac{1}{2}\sum_{k=0}^{3} e^{\pi \mathrm{i}k}\,|k\rangle = \frac{1}{2}(|0\rangle-|1\rangle+|2\rangle-|3\rangle)\\
&= \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)\\
\mathrm{QFT}\,|3\rangle = |11\rangle &= \frac{1}{2}\sum_{k=0}^{3} e^{\frac{3\pi}{2}\mathrm{i}k}\,|k\rangle = \frac{1}{2}(|0\rangle-\mathrm{i}\,|1\rangle-|2\rangle+\mathrm{i}\,|3\rangle)\\
&= \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-\mathrm{i}\,|1\rangle)\\
\mathrm{QFT}\,|j\rangle = |j_1 j_0\rangle &= \frac{1}{2}\left(|0\rangle+e^{\pi \mathrm{i} j_0}\,|1\rangle\right)\left(|0\rangle+e^{\pi \mathrm{i}\left(j_1+\frac{j_0}{2}\right)}\,|1\rangle\right)
\end{aligned}$$

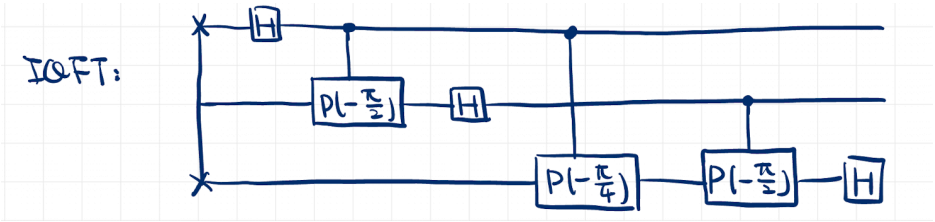
- Extrapolate to 3-qubit case:

$$\mathrm{QFT}\,|j_2 j_1 j_0\rangle = \frac{1}{2\sqrt{2}}\left(|0\rangle+e^{\pi \mathrm{i} j_0}\,|1\rangle\right)\left(|0\rangle+e^{\pi \mathrm{i}\left(j_1+\frac{j_0}{2}\right)}\,|1\rangle\right)\left(|0\rangle+e^{\pi \mathrm{i}\left(j_2+\frac{j_1}{2}+\frac{j_0}{4}\right)}\,|1\rangle\right).$$

- Inverse QFT: Reverse order of gates and replace with inverses.

$$H^{-1}=H,\quad P(\theta)=\begin{pmatrix}1 & 0\\ 0 & e^{\mathrm{i}\theta}\end{pmatrix} \implies [P(\theta)]^{-1}=[P[(\theta)]^{\dagger}=P(-\theta).$$

For 3 qubits,



Lemma 10.1 : Eigenvalues of unitary matrices have norm-square of 1.

Proof 1. Let $U|v\rangle = \lambda|v\rangle$. So,

$$\langle v| U^\dagger = \lambda^* \langle v|.$$

Inner product of the two equalities:

$$\langle v| \underbrace{U^\dagger U}_{=I} |v\rangle = \lambda^* \lambda \langle v|v\rangle$$
$$\langle v|v\rangle = |\lambda|^2 \langle v|v\rangle$$
$$|\lambda|^2 = 1.$$

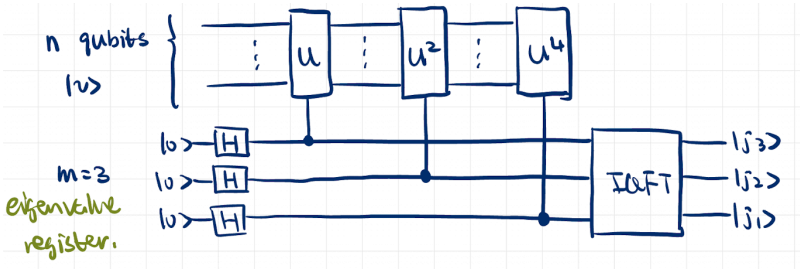
Q.E.D. ■

Corollary 10.2 : So, λ can be written as $e^{i\theta}$.

10.1 The Problem

Given U ($2^n \times 2^n$) and $|v\rangle$ (with n qubits), we want to find $\lambda = e^{i\theta}$.

To estimate θ to m bits, we need m additional qubits. Choose $m = 3$.



- After H's, $\frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|v\rangle$.
- Since $U|v\rangle = e^{i\theta}|v\rangle$, controlled U multiplies by $e^{i\theta}$ if control if 1.
  1. After controlled U: $\frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\left(|0\rangle + e^{i\theta}|1\rangle\right)|v\rangle$
  2. After controlled U^2: $\frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)\left(|0\rangle + e^{2i\theta}|1\rangle\right)\left(|0\rangle + e^{i\theta}|1\rangle\right)|v\rangle$
  3. After controlled U^4: $\frac{1}{2\sqrt{2}}\left(|0\rangle + e^{4i\theta}|1\rangle\right)\left(|0\rangle + e^{2i\theta}|1\rangle\right)\left(|0\rangle + e^{i\theta}|1\rangle\right)|v\rangle$.
- For $\lambda = e^{i\theta}$,

λ	θ	$j = \frac{\theta}{2\pi}$
1	0	0
-1	π	$\frac{1}{2}$

We will represent $\widehat{j} = (0.j_1 j_2 j_3)_2 = \frac{j_1}{2} + \frac{j_2}{4} + \frac{j_3}{8}$. Substitude, we have

$$\theta = 2\pi j = 2\pi\left(\frac{j_1}{2} + \frac{j_2}{4} + \frac{j_3}{8}\right).$$

- Hence,

$$e^{\mathrm{i}\theta} = e^{2\pi\mathrm{i}(j_1/2+j_2/4+j_3/8)} = e^{\pi\mathrm{i}(j_1+j_2/2+j_3/4)}$$
$$e^{2\mathrm{i}\theta} = e^{2\mathrm{i}\theta} = e^{\pi\mathrm{i}(2j_1+j_2+j_3/2)} = \underbrace{e^{2\pi\mathrm{i}j_1}}_{=1} e^{\pi\mathrm{i}(j_2+j_3/2)} = e^{\pi\mathrm{i}(j_2+j_3/2)}$$
$$e^{4\mathrm{i}\theta} = e^{4\mathrm{i}\theta} = e^{\pi\mathrm{i}(4j_1+2j_2+j_3)} = \underbrace{e^{4\pi\mathrm{i}j_1}}_{=1}\underbrace{e^{2\pi\mathrm{i}j_2}}_{=1} e^{\pi\mathrm{i}j_3} = e^{\pi\mathrm{i}j_3}.$$

  So, the qubit is

$$\underbrace{\frac{1}{2\sqrt{2}}\left(|0\rangle + e^{\pi\mathrm{i}j_3}|1\rangle\right)\left(|0\rangle + e^{\pi\mathrm{i}(j_2+j_3/2)|1\rangle}\right)\left(|0\rangle + e^{\pi\mathrm{i}(j_1+j_2/2+j_3/4)}|1\rangle\right)}_{=\mathrm{QFT}|j_1j_2j_3\rangle|v\rangle}|v\rangle$$

- The final state is

$$|j_1\rangle|j_2\rangle|j_3\rangle|v\rangle,$$

  where $j = \frac{j_1}{2} + \frac{j_2}{4} + \frac{j_3}{8} \implies \theta = 2\pi j \implies \lambda = e^{\mathrm{i}\theta}$.

What if U has two eigenvectors? If input to quantum phase estimation (QPE) circuit is

$$|00\cdots0\rangle\,(\underbrace{\alpha|v_1\rangle + \beta|v_2\rangle}_{\text{eigenvector register}}),$$

then the output before measurement if

$$\alpha|j_1j_2\cdots j_m\rangle|v_n\rangle + \beta|j_1'j_2'\cdots j_n'\rangle|v_2\rangle,$$

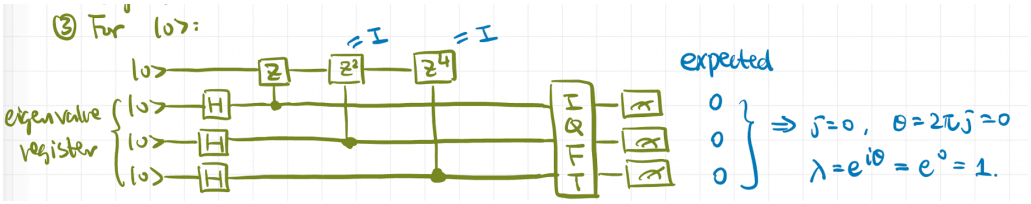
where the probability of getting the two eigenvectors are $|\alpha|^2$ and $|\beta|^2$, respectively, $|j_1j_2\cdots j_m\rangle$ is the eigenvalue for $|v_1\rangle$, and $|j_1'j_2'\cdots j_n'\rangle$ is the eigenvalue for $|v_2\rangle$.

Example 10.1.1 Find Eigenvalues of Z

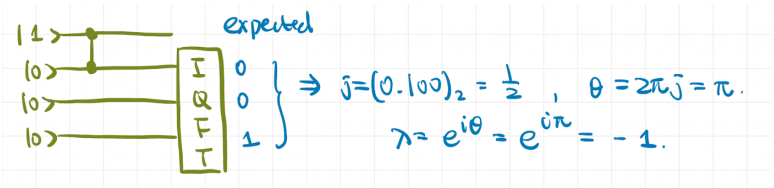
- Z acts on 1 qubit, so $|v\rangle$ is q qubit:

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

- Eigenvectors are $|0\rangle$ and $|1\rangle$.
- For $|0\rangle$:



- For $|1\rangle$:



11 Order Finding and Shor's Algorithm

11.1 Order Finding Problems

Definition 11.1.1 (Modulo Arithmetic).

$$a \mod b = \text{remainder when } a \text{ is divided by } b.$$

Example 11.1.2

$15 \mod 12 = 3$. Sometimes, we also write $15 \equiv 3 \mod 12$ or $15 \equiv 27 \mod 12$ to indicate that the both sides have the same remainder.

Modular Exponentiation and Order

$$\begin{aligned} 2^0 &\mod 7 = 1 \\ 2^1 &\mod 7 = 2 \\ 2^2 &\mod 7 = 4 \\ 2^3 &\mod 7 = 1 \\ 2^4 &\mod 7 = 2 \\ 2^5 &\mod 7 = 4 \\ 2^6 &\mod 7 = 1 \end{aligned}$$

Pattern repeats with period $r = 3$. This is called the *order* of $2 \mod 7$. It is also the smallest positive r such that

$$2^r \mod 7 = 1.$$

Order Finding Circuit: Uses modular multiplication operator

$$U|y\rangle = |ay \mod N\rangle .$$

We want to find the order r of $a \mod N$.

Lemma 11.3 : Eigenvalues of U are

$$|v_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left| a^k \mod N \right\rangle$$

for $s = 0, 1, \ldots, r-1$ with eigenvalues $e^{2\pi i s/r}$.

[*Recall in QPE:* $e^{2\pi i j}$.]

Proof 1.

$$\begin{aligned} U|v_s\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{2\pi isk/r}\left|a^{k+1} \mod N\right\rangle \\ &= \frac{1}{\sqrt{r}}\left(\sum_{k=0}^{r-2} e^{-2\pi isk/r}\left|a^{k+1} \mod N\right\rangle + e^{-2\pi is(r-1)/r}\left|a^{k} \mod N\right\rangle\right). \end{aligned}$$

Simplify the final term:

- $e^{-2\pi is(r-1)/r} = e^{-2\pi isr/k}e^{2\pi is/r} = e^{2\pi is/r}$.
- $\left|a^k \mod N\right\rangle = \left|a^0 \mod N\right\rangle = |1\rangle$.

So,

$$\begin{aligned} U|v_s\rangle &= \frac{1}{\sqrt{r}}\left(\sum_{k=0}^{r-2} e^{-2\pi isk/r}\left|a^{k+1} \mod N\right\rangle + \underbrace{e^{-2\pi is(-1)/r}\left|a^{-1+1} \mod N\right\rangle}_{k=-1}\right) \\ &= \frac{1}{\sqrt{r}}\sum_{k=-1}^{r-1} e^{-2\pi isk/r}\left|a^{k+1} \mod N\right\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi is(k-1)/r}\left|a^{k} \mod N\right\rangle \\ &= e^{2\pi is/r}\underbrace{\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi isk/r}\left|a^{k} \mod N\right\rangle}_{|v_s\rangle} \\ &= \underbrace{e^{2\pi is/r}}_{\lambda}|v_s\rangle \end{aligned}$$

Q.E.D. ■

Lemma 11.4 : Equally weighted superposition of $|v_s\rangle$,

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

is $|1\rangle = |0\cdots01\rangle$.

Proof 2.

$$\begin{aligned} \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|v_s\rangle &= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi isk/r}\left|a^{k} \mod N\right\rangle \\ &= \frac{1}{r}\sum_{k=0}^{r-1}\left|a^{k} \mod N\right\rangle\sum_{s=0}^{r-1} e^{-2\pi isk/r}. \end{aligned}$$

Look at the latter sum:

- When $k = 0$,
$$\sum_{s=0}^{r-1} e^{-2\pi \mathrm{i} sk/r} = \sum_{s=0}^{r-1} 1 = r.$$
- When $k \neq 0$, consider the geometric sum
$$\sum_{s=0}^{r-1} \omega^s = \frac{\omega^r - 1}{\omega - 1}.$$
Take $\omega = e^{-2\pi \mathrm{i} sk/r}$:
$$\begin{aligned}\sum_{s=0}^{r-1} e^{-2\pi \mathrm{i} sk/r} &= \frac{\left(e^{-2\pi \mathrm{i} sk/r}\right)^r - 1}{e^{-2\pi \mathrm{i} sk/r} - 1} \\ &= \frac{e^{-2\pi \mathrm{i} sk} - 1}{e^{-2\pi \mathrm{i} sk/r} - 1} \\ &= \frac{1 - 1}{e^{-2\pi \mathrm{i} sk/r} - 1} = 0.\end{aligned}$$

So,
$$\begin{aligned}\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |v_s\rangle &= \frac{1}{r}\left(r \left| a^k \mod N \right\rangle + 0\right) \\ &= 1 \cdot \underbrace{\left| a^0 \mod N \right\rangle}_{=1} \\ &= 1.\end{aligned}$$

Q.E.D. ■

To Find Order r :

- Use phase estimation circuit
- Initialize eigenvector register to $|00\cdots01\rangle$ = superposition of eigenvectors of U.
- Recall eigenvalue $e^{\mathrm{i}\theta} = e^{2\pi \mathrm{i} j} = e^{2\pi \mathrm{i} s/r}$.
- Measurement yields $j \approx \frac{s}{r}$, each s equally likely with a probability of $\frac{1}{r}$.
- If $\frac{s}{r}$ is non-determinating ($\frac{1}{3}$, $\frac{5}{6}$, etc. i.e., they have no binary representation), we will use continuing fraction expansion.
  1. For base 2, only when r is a power of 2, we have determinating fractions.
  2. For base 10, we require r to be a combination of power of 2 and power of 5.

Example 11.1.5 Continuing Fraction Expansion

We want to determine the order of $3 \mod 7$, with 5 qubits in the eigenvalue register. We get the following results, each with $\frac{1}{6}$ probability:

$$\begin{aligned}
|00000\rangle &\to \frac{s}{r} = 0 \quad \text{unhelpful} \\
|00101\rangle &\to (0.00101)_2 = \frac{1}{8} + \frac{1}{32} = \frac{5}{32} \approx \frac{s}{r} \\
|01011\rangle &\to (0.01011)_2 = \frac{11}{32} \approx \frac{s}{r} \\
|10000\rangle &\to (0.10000)_2 = \frac{1}{2} = \frac{s}{r} \\
|10101\rangle &\to (0.10101)_2 = \frac{21}{32} \approx \frac{s}{r} \\
|11011\rangle &\to (0.11011)_2 = \frac{27}{32} \approx \frac{s}{r}.
\end{aligned}$$

- For $\frac{s}{r} = \frac{1}{2}$, guess $r = 2$. Test $3^2 \mod 7 = 2 \implies r \neq 2$. We could continuing guessing, but it is more helpful to use continuous fraction expansion.
- For $\frac{s}{r} \approx \frac{5}{32}$:
  1. What we will do is flip and split:
  $$\frac{5}{32} = \frac{1}{\frac{32}{5}} = \frac{1}{6 + \frac{2}{5}} = \frac{1}{6 + \frac{1}{\frac{5}{2}}} = \frac{1}{6 + \frac{1}{2 + \frac{1}{2}}}$$
  2. Find "convergents" (drop proper fractions):
  $$0, \frac{1}{6}, \frac{1}{6 + \frac{1}{2}} = \frac{2}{13}, \frac{5}{32}$$
  3. Find the best guess for r: Since we are looking for the order of $3 \mod 7$, the order cannot be > 7.
  4. The best guess for r is the biggest denominator < 7.
  5. Try $\frac{s}{r} = \frac{1}{6}$. Guess $r = 6$. Test
  $$3^6 \mod 7 = 1 \implies r = 6 \quad \checkmark$$
- For $\frac{s}{r} \approx \frac{11}{32}$,
$$\frac{11}{32} = \frac{1}{\frac{32}{11}} = \frac{1}{2 + \frac{10}{11}} = \frac{1}{2 + \frac{1}{\frac{11}{10}}} = \frac{1}{2 + \frac{1}{1 + \frac{1}{10}}}.$$

Convergents $0, \frac{1}{2}, \frac{1}{2+1} = \frac{1}{3}, \frac{11}{32}$.
guess $\frac{s}{r} = \frac{1}{3}$. Try $s = 1$ and $r = 3$ and test

$$3^3 \mod 7 \neq 1.$$

So, it should be $s = 2$ and $r = 6$.

Problem: If the number has many digits, how would we know if we should multiply the guess by how many times?

Solution: Use a new circuit.

Suppose $\frac{3}{r} = \frac{1}{3} = \frac{2}{6} = \frac{3}{9} = \cdots$. Define $r = 3r'$. Then,

$$3^d \mod 7 = (3^3)^{r'} \mod 7 = 27^{r'} \mod 7.$$

Then, we make a new order finding circuit to find the order of $27 \mod 7$. We will get $r' = 2$. Then, $r = 3r' = 6$. We might need to repeat this process several times.

11.2 Shor's Algorithm

To break RSA encryption, we need to factor $N = pq$.

- Pick any number a, $1 < a < N$, co-prime with N.
- Find order r of a mod N (phase estimation circuit).
  1. If r is odd, pick another a.
  2. If $a^{r/2} \mod N = N - 1$, pick another a.
- Since $a^r \mod N = 1$, we have

$$(a^r - 1) \mod N = 0$$
$$\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) \mod (pq) = 0.$$

1. Is $\left(a^{r/2} - 1\right)$ a multiple of $pq = N$? No because if so, we get

$$\left(a^{r/2} - 1\right) \mod N = 0 \implies a^{r/2} \mod N = 1.$$

Then, $r/2$ would be the order. We reach a contradiction.

2. Is $\left(a^{r/2}+1\right)$ a multiple of $pq = N$? No, because if so, we get

$$\left(a^{r/2}+1\right) \mod N = 0 \implies a^{r/2} = N-1, 2N-1, 3N-1, \ldots$$
$$\implies a^{r/2} \mod N = N-1$$

However, we have excluded such cases.

3. Conclusion: $\left(a^{r/2}-1\right)$ and $\left(a^{r/2}+1\right)$ must each be a multiple of a different factor of N. Use the concept of greatest common divisor (gcd):

$$p = \gcd\left(a^{r/2}-1, N\right) \quad \text{and} \quad q = \gcd\left(a^{r/2}+1, N\right).$$

Example 11.2.1 Factor 15

- Pick $a = 2$:
  1. Find the order of $2 \mod 15$.
  2. QPE gives $r = 4$.
  3. Find the factor
$$\gcd(4-1, 15) = 3 \quad \text{and} \quad \gcd(4+1, 15) = 5.$$
- Pick $a = 7$:
  1. Order of $7 \mod 15$ is also 4.
  2. Find the factor:
$$\gcd(7^2-1, 15) = \gcd(48, 15) = 3$$
$$\gcd(7^2+1, 15) = \gcd(50, 15) = 5$$
  3. Euclid's algorithm:
     - Replace the larger one with their difference
     - Repeat until we get the same number on both sides.

48	15	50	15
$48-15=33$	15	$50-15=35$	15
$33-15=18$	15	$35-15=20$	15
$18-15=3$	15	$20-15=5$	15
3	$15-3=12$	5	$15-5=10$
3	$12-3=9$	5	$10-5=5$
3	$9-3=6$	5	5
3	$6-3=3$		
3	3		

Quantum Circuit: Phase estimation circuit to factor 15

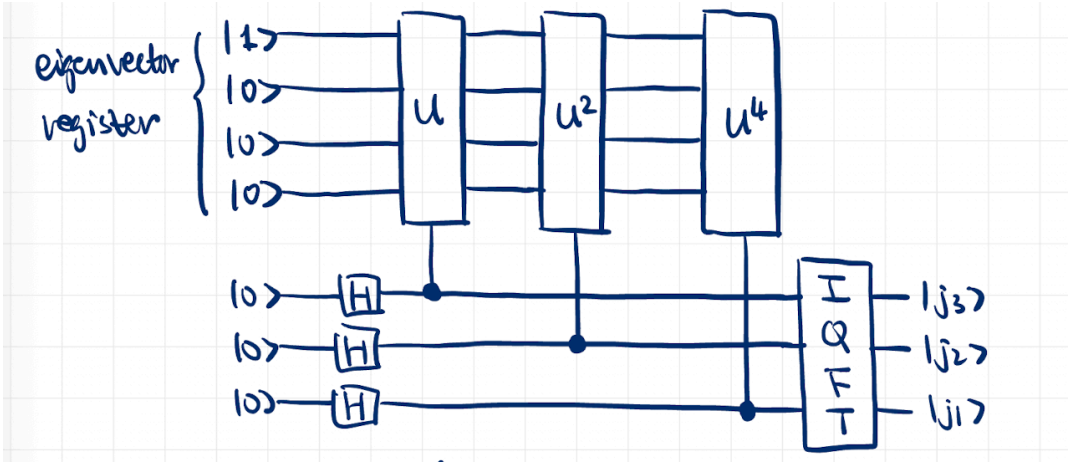
- Modular multiplication operator:

$$U|y\rangle = |ay \mod 15\rangle .$$

  The only a's that work for Shor's algorithm are $2, 4, 7, 8, 11, 13$.

- Eigenvector register initialized to $|0001\rangle$ = equally weighted superposition of eigenvectors of U. We need 4 qubits to count up to 14.

- Let's use 3 qubits for the eigenvalue register:



  Measurement of eigenvalue register gives $j = (0.j_1 j_2 j_3)_2 \approx \frac{s}{r}$, and

$$\mathbf{P}\left(\frac{0}{r}\right) = \mathbf{P}\left(\frac{1}{r}\right) = \cdots = \mathbf{P}\left(\frac{r-1}{r}\right) = \frac{1}{r}.$$

- If $r = 2$,

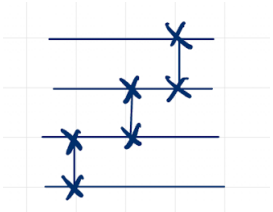
$$\frac{s}{r} = \frac{0}{2} \quad \text{or} \quad \frac{1}{2} \implies j = (0.000)_2 \quad \text{or} \quad (0.100)_2.$$

  If $r = 4$,

$$\frac{s}{r} = \frac{0}{4}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4} \implies j = (0.000)_2, (0.010)_2, (0.100)_2, (0.110)_2$$

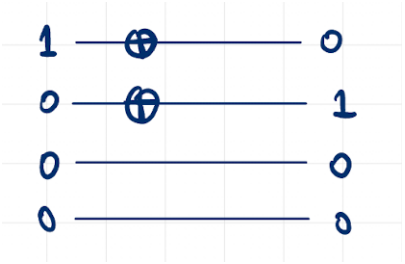
- What is U (Modular multiplication operator)?

  1. From Monz (2018), but inverted to match IBM conventions: Multiply by $2 \mod 15$:

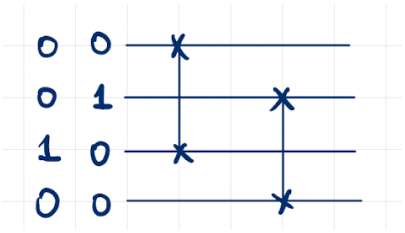


     For example, $|0001\rangle \to |0010\rangle$ and $|0010\rangle \to |0100\rangle$.
     Problem: swap gate is not a small gate. We make the circuit very complicated, and error accumulates. The results can be bad.

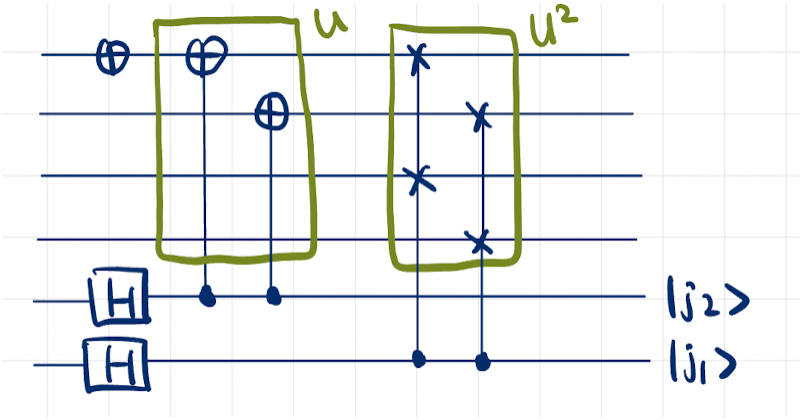
2. Simplified multiply by $2 \mod 15$:
   - Initial state is $|0001\rangle$, so the operator only needs to multiply $|0001\rangle$ by 2.
   - Since $|0001\rangle \xrightarrow{\times 2} |0010\rangle$, we get U is given by



   - Multiply by $2^2 \mod 15 = 4$, which is our U^2.
   (a) After the first controlled U, the eigenvector register is in a superposition of $|0001\rangle$ and $|0010\rangle$.
   (b) Now, we need an operator that achieves both of the following: $|0001\rangle \xrightarrow{\times 4} |0100\rangle$ and $|0010\rangle \xrightarrow{\times 4} |0100\rangle$.



   - Multiply by $2^4 \mod 15 = 16 \mod 15 = 1$. Multiplication by 1 isn't doing anything. We don't need U^4.
   - The simplied circuit is given by



Example 11.2.2 Use Short's Algorithm to Factor 33

- Pick $a = 4$.
- Find the order of $4 \mod 33$. The results are:
  1. 0000000: $\frac{s}{r} = 0$.

2. 0011010: $\frac{s}{r} \approx \frac{13}{64}$. Use continuing fraction expansion:

$$\frac{13}{64} = \frac{1}{\frac{64}{13}} = \frac{1}{4 + \frac{12}{13}} = \frac{1}{4 + \frac{1}{\frac{13}{12}}} = \frac{1}{4 + \frac{1}{1 + \frac{1}{12}}}.$$

   So, convergents are $0, \frac{1}{4}, \frac{4+1}{=}\frac{1}{5}, \frac{13}{64}$.

   Best guess for $\frac{s}{r} = \frac{1}{5}$. Try $4^5 \mod 33 = 1$ ✔.

   However, $r = 5$ is odd, and Short's algorithm cannot be applied. So, we need to pick another a.

3. 0110011

4. 1001101

5. 1100110