5. Quantum circuits

(a) Quantum circuit model (KLM 4.1, NC 1.3.4)

(b) Quantum gates (NC 4.2-4.3, KLM 4.2)

(c) Continuous universal set of quantum gates (reading) (NC 4.5.1-4.5.2, KLM 4.3)

(d) Quantum gate approximations (NC Box 4.1, KLM 4.3)

(e) Finite universal set of q. gates (NC 4.5.3, KLM 4.3)

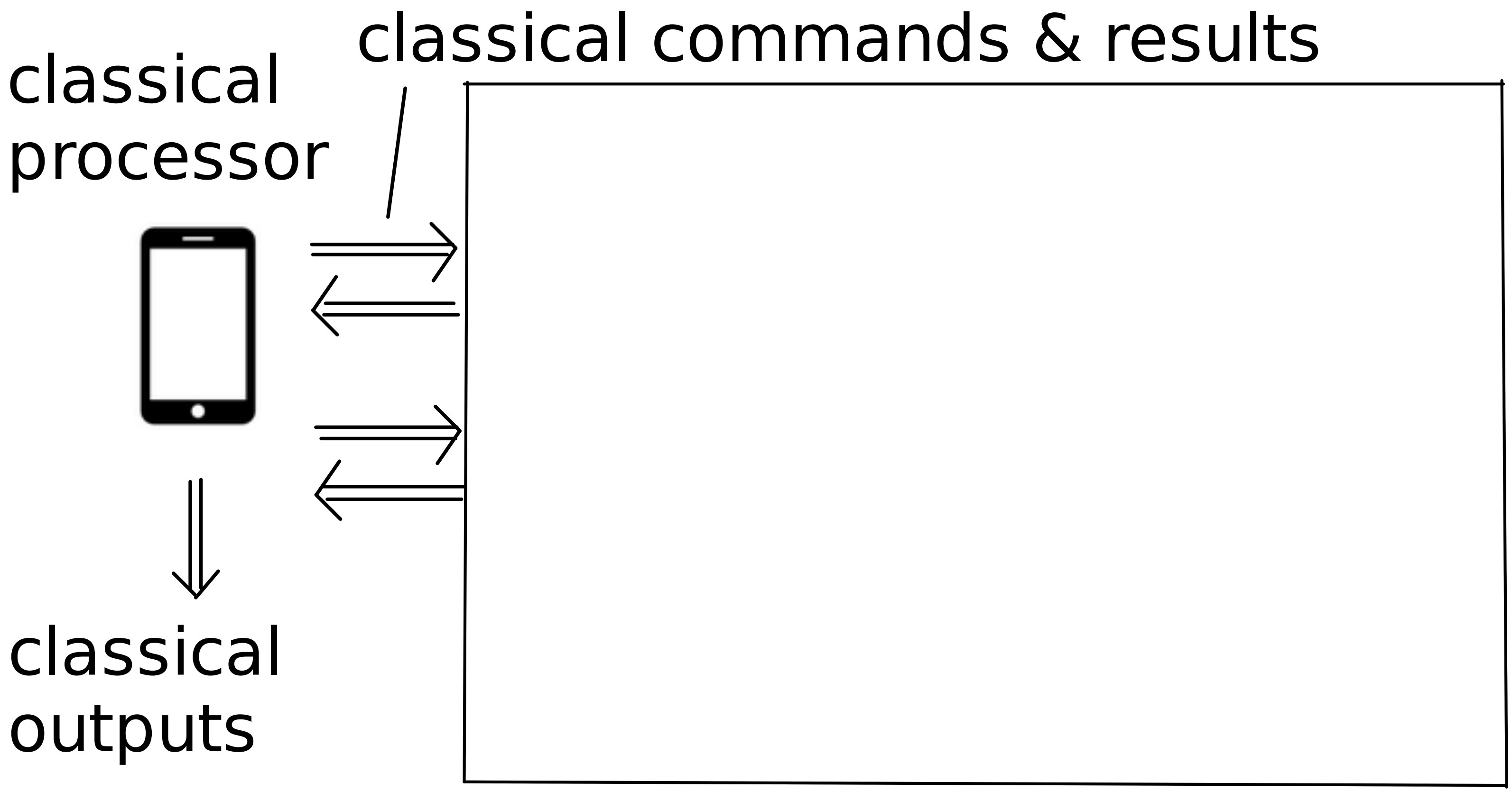
(f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

(g) Quantum circuits for measurements (KLM 4.5*)

(h) Hardness of approximating most unitaries (reading) (NC 4.5.6)

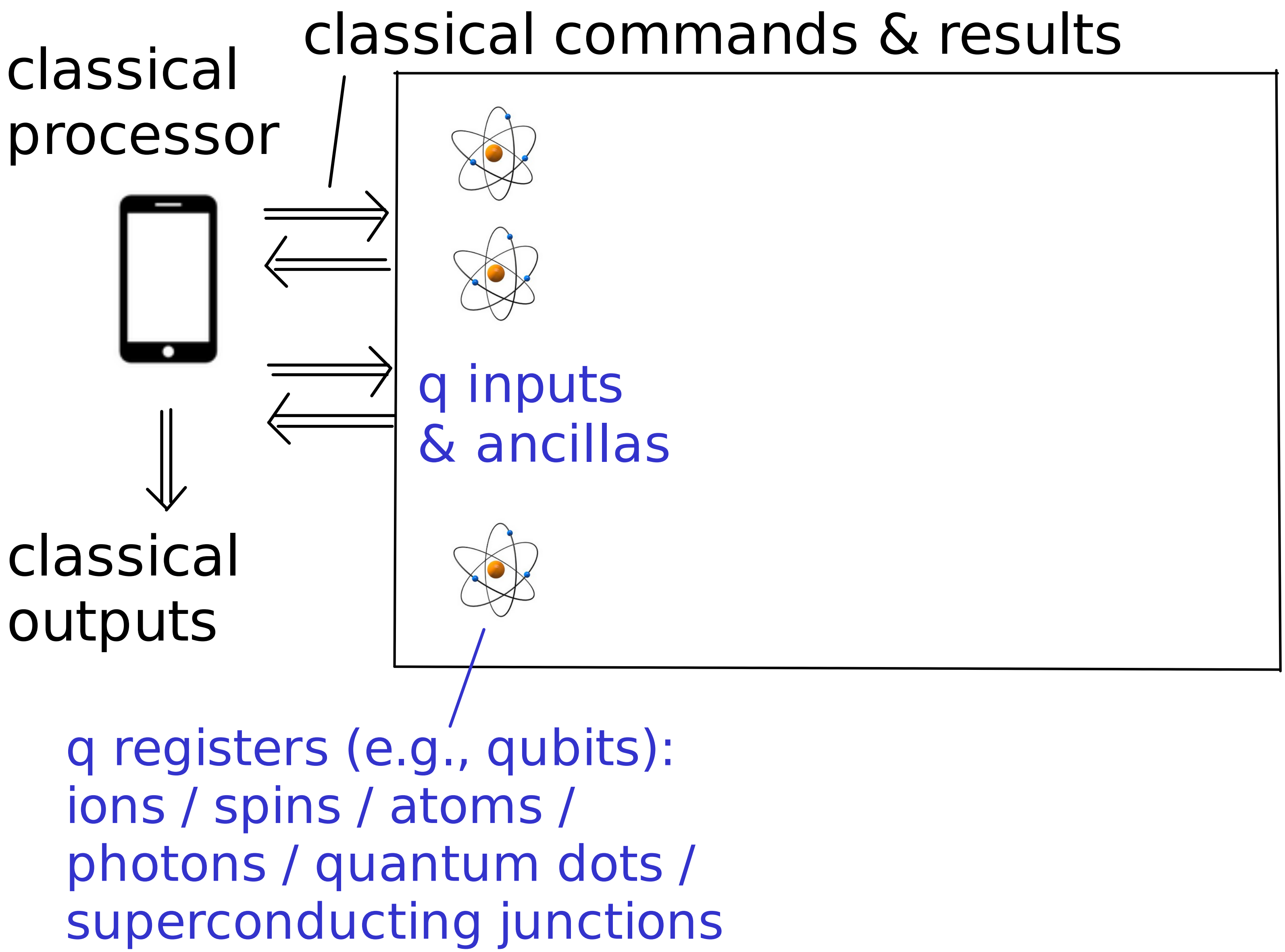
(a) Quantum circuit model (KLM 4.1, NC 1.3.4)

A computation in the quantum setting:



(a) Quantum circuit model (KLM 4.1, NC 1.3.4)

A computation in the quantum setting:

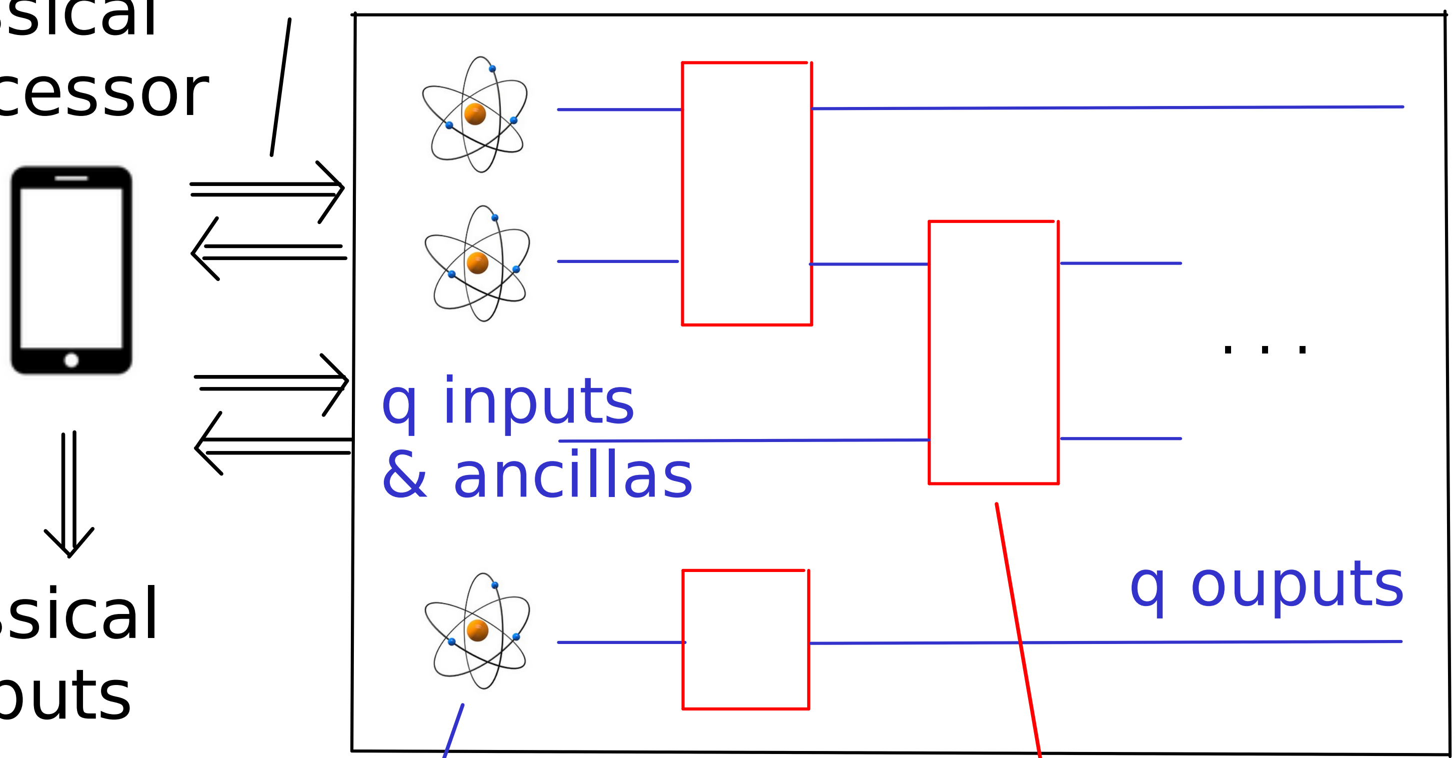


(a) Quantum circuit model (KLM 4.1, NC 1.3.4)

A computation in the quantum setting:

classical commands & results

classical
processor



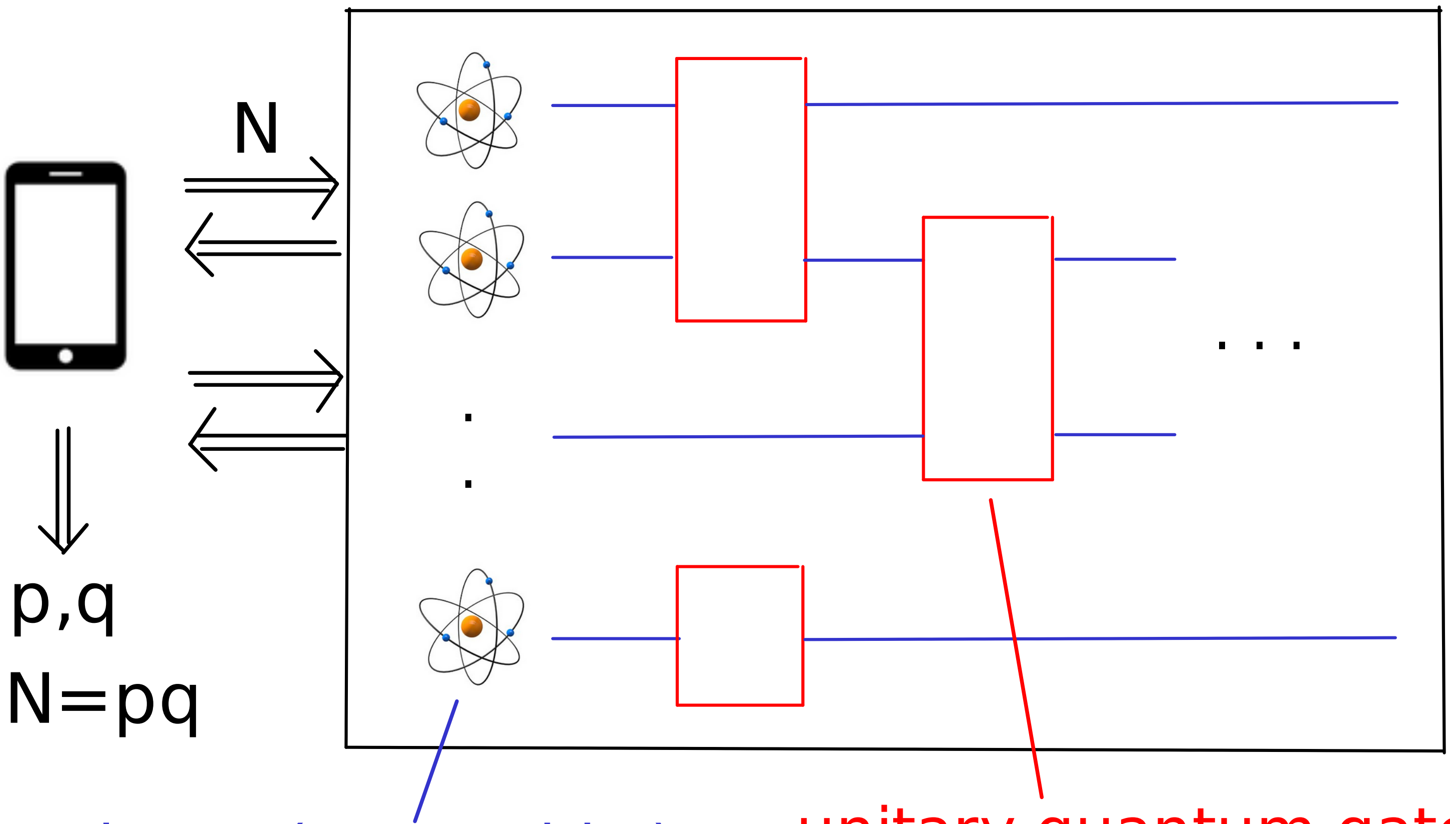
classical
outputs

q registers (e.g., qubits):
ions / spins / atoms /
photons / quantum dots /
superconducting junctions

unitary quantum gates &
measurements: laser pulses /
currents / electric or magnetic
field applied to a few qubits at
a time

(a) Quantum circuit model (KLM 4.1, NC 1.3.4)

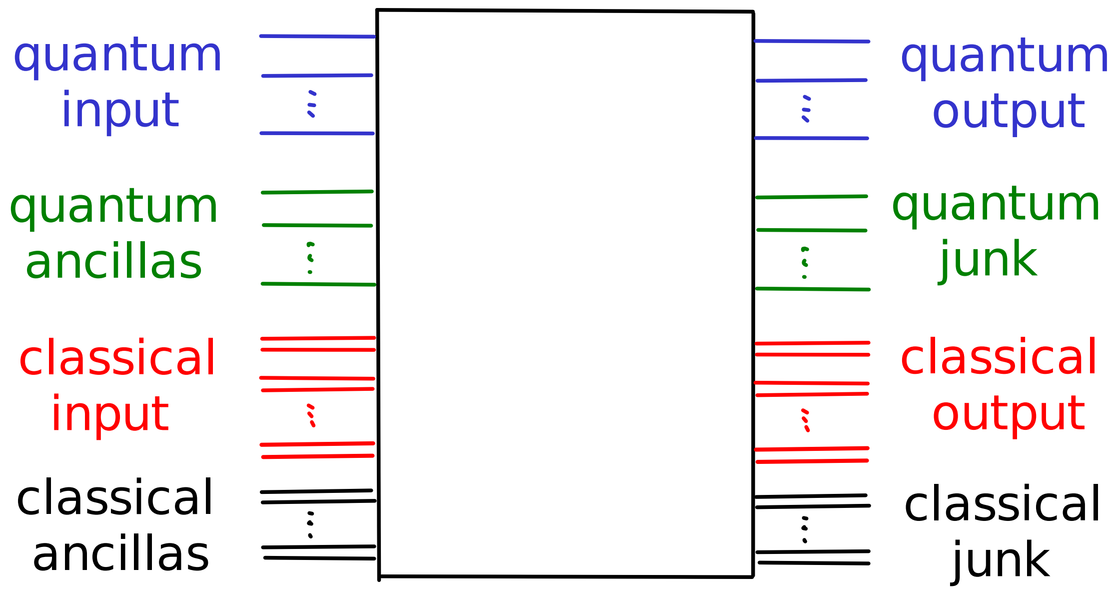
e.g., factoring with a quantum computer:



q registers (e.g., qubits):
ions / spins / atoms /
photons / quantum dots /
superconducting junctions

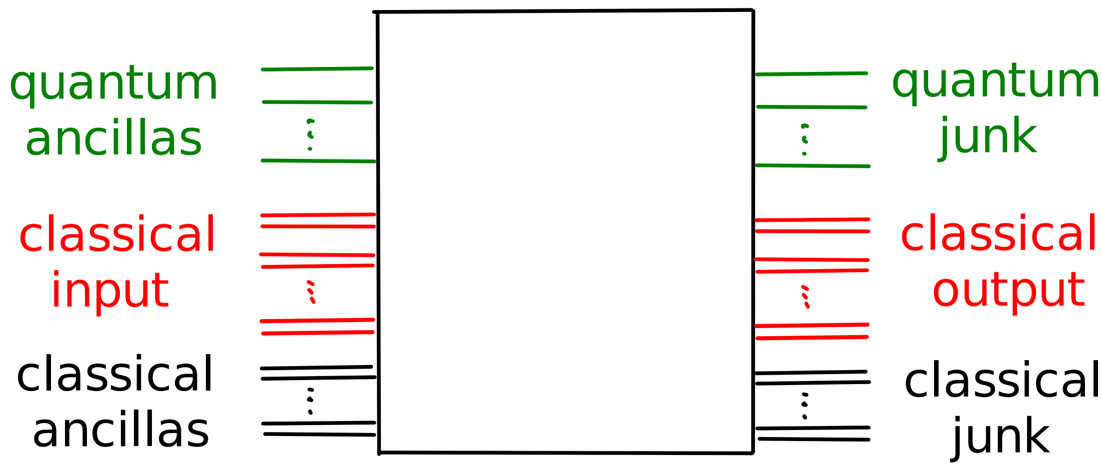
unitary quantum gates &
measurements: laser pulses /
currents / electric or magnetic
field applied to a few qubits at
a time

A computation in the quantum setting:



- obeys QM :
- classical registers can control the unitary evolution
- classical computation allowed in the box

For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):



For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

(1) Encode classical data in computational basis states, perform classical computation reversibly as a unitary, return ancillas to the initial state without junk.

For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

(1) Encode classical data in computational basis states, perform classical computation reversibly as a unitary, return ancillas to the initial state without junk.

e.g., we can perform the NOT gate on 1 bit by encoding the bit as $|0\rangle$ or $|1\rangle$ and apply the unitary

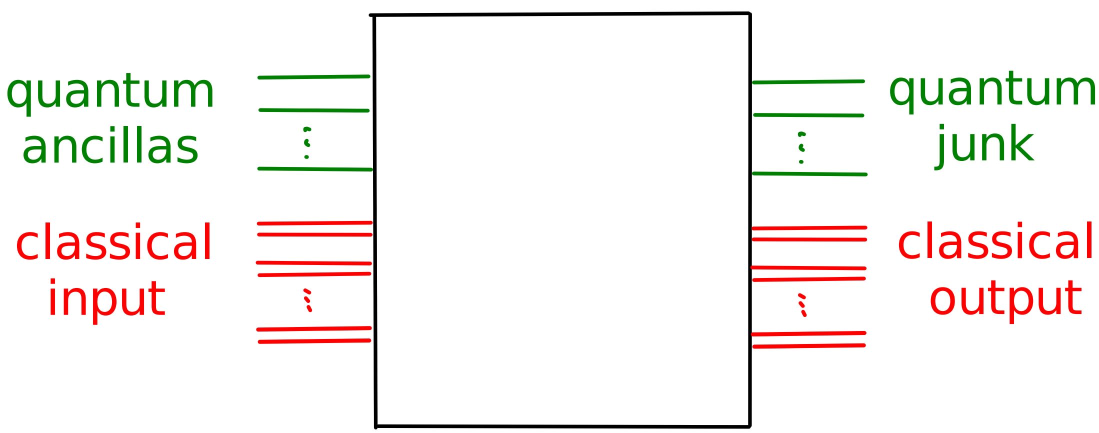
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

This follows from topic 2 (classical computation is reversible, the Toffoli gate is unitary and universal for classical computation).

For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

(1) Encode classical data in computational basis states,
perform classical computation reversibly as a unitary,
return ancillas to the initial state without junk.



For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

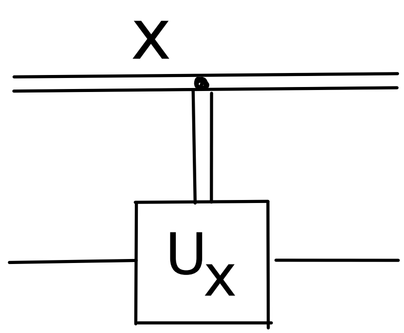
(2) Unitary operations controlled by classical data can be implemented as a "controlled-unitary" operation and vice versa.

For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

(2) Unitary operations controlled by classical data can be implemented as a "controlled-unitary" operation and vice versa.

If classical register C is in state x,
then apply U_x to the quantum register Q



For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

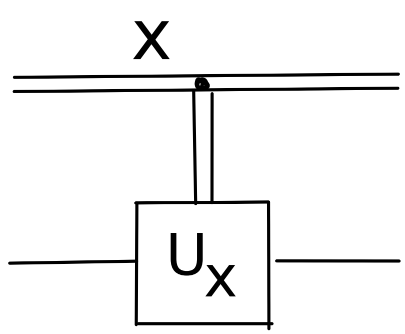
Simplifying ideas:

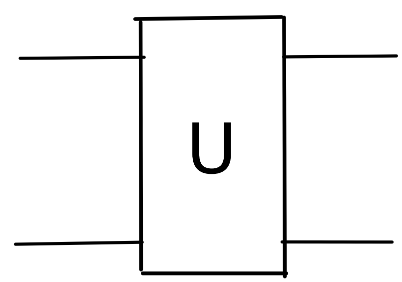
(2) Unitary operations controlled by classical data can be implemented as a "controlled-unitary" operation and vice versa.

If classical register C is in state x, then apply U_x to the quantum register Q

$$U = \sum_x |x\rangle\langle x|_C \otimes (U_x)_Q$$

unitary if the Ux's are





For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

(2) Unitary operations controlled by classical data can be implemented as a "controlled-unitary" operation and vice versa.

e.g., in superdense coding, Alice receives one of 0,x,y,z and she applies σ_0, σ_x, σ_y, σ_z accordingly.
This is a unitary controlled by classical data.

For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

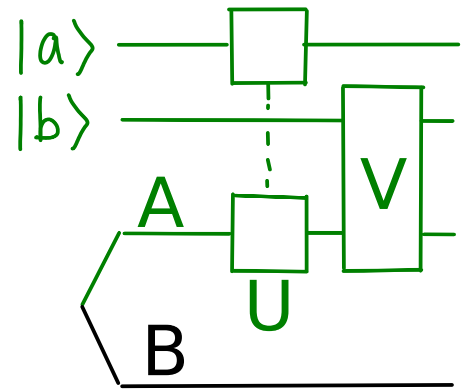
(2) Unitary operations controlled by classical data can be implemented as a "controlled-unitary" operation and vice versa.

e.g., in superdense coding, Alice receives one of 0,x,y,z and she applies $\sigma_0, \sigma_x, \sigma_y, \sigma_z$ accordingly.
This is a unitary controlled by classical data.

Instead, encode 0,x,y,z as

$|ab\rangle = |00\rangle, |01\rangle, |11\rangle, |10\rangle$

and apply 2 controlled unitaries:



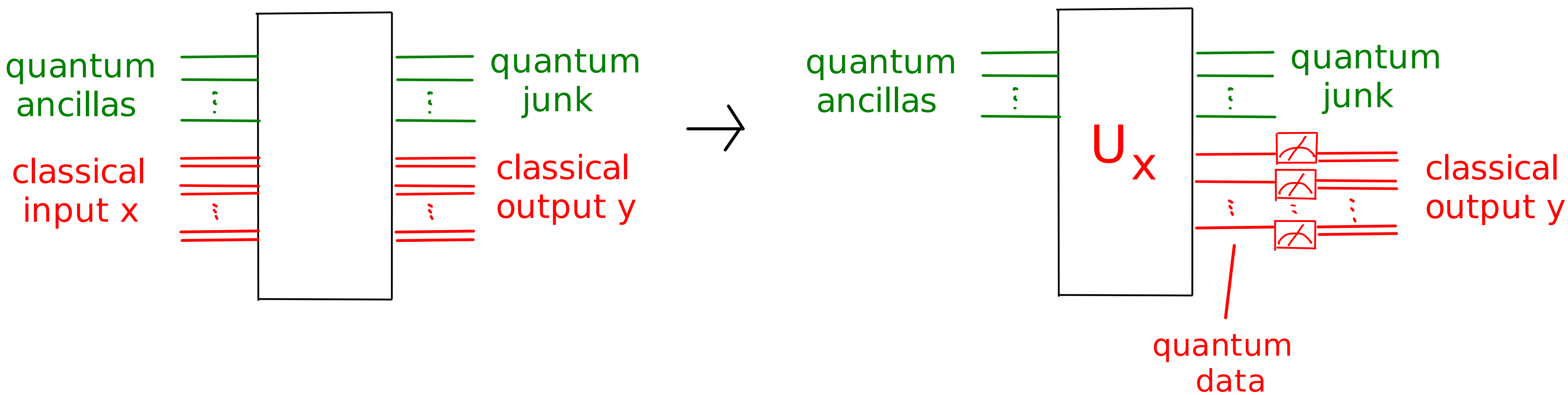
$$U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_z$$

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x$$

For quantum computation of classical problems
(no quantum inputs or outputs in topics 5-7):

Simplifying ideas:

(3) Classical input is encoded in the choice of the unitary.



Canonical quantum computation of classical problems:

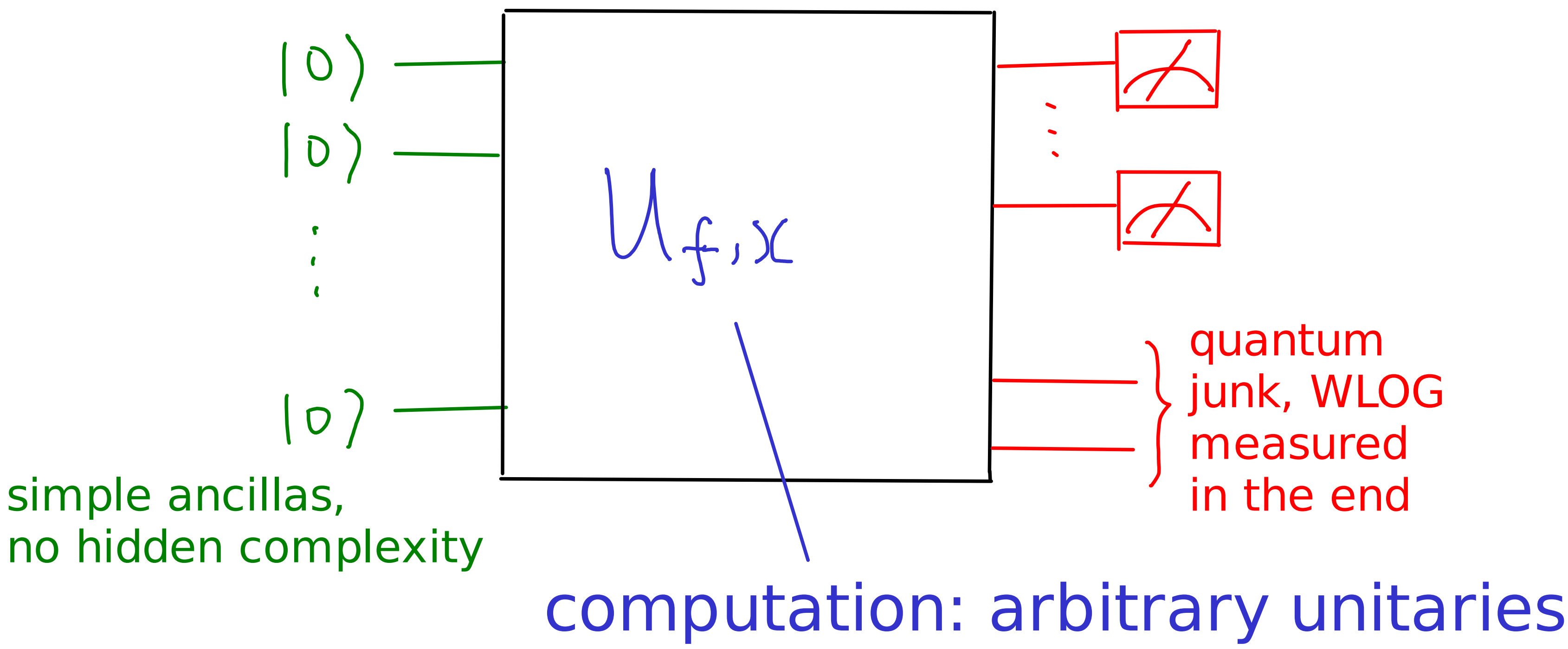
- Only has quantum registers.
- Computation is unitary until final measurements.

Canonical quantum computation of classical problems:

- Only has quantum registers.
- Computation is unitary until final measurements.
- Classical input is encoded in the choice of the unitary.

  All registers can start as $|0\rangle$.
- Outputs (classical) are measurement outcomes.

Conventions as in classical circuits.



With goals and ideas similar to topic 1:

Quantum circuit (acyclic graph):
- time going from left to right
- quantum wires (registers) carry quantum data
- gates are vertices in the graph

With goals and ideas similar to topic 1:

Quantum circuit (acyclic graph):
- time going from left to right
- quantum wires (registers) carry quantum data
- gates are vertices in the graph

Each quantum gate acts unitarily on the Hilbert space associated with the input registers. Since a quantum gate preserves dimension, for each gate

incoming edges = # outgoing edges.

(Assuming each register has the same dimension.)

With goals and ideas similar to topic 1:

Quantum circuit (acyclic graph):
- time going from left to right
- quantum wires (registers) carry quantum data
- gates are vertices in the graph

Each quantum gate acts unitarily on the Hilbert space associated with the input registers. Since a quantum gate preserves dimension, for each gate

incoming edges = # outgoing edges.

Are there "universal sets of quantum gates" that implement any arbitrary "computation" (i.e., unitary transformation)?

5. Quantum circuits

(a) Quantum circuit model (KLM 4.1, NC 1.3.4) ✓

(b) Quantum gates (NC 4.2-4.3, KLM 4.2)

(c) Continuous universal set of quantum gates (reading)
(NC 4.5.1-4.5.2, KLM 4.3)

(d) Quantum gate approximations (NC Box 4.1, KLM 4.3)

(e) Finite universal set of q. gates (NC 4.5.3, KLM 4.3)

(f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

(g) Quantum circuits for measurements (KLM 4.5*)

(h) Hardness of approximating most unitaries (reading)
(NC 4.5.6)

(c) Continuous universal set of quantum gates (reading) (NC 4.5.1-4.5.2, KLM 4.3)

Universal set of quantum gates

Definition: a set G of quantum gates is universal, if for any unitary U, there is a circuit using only gates from G performing U.

(c) Continuous universal set of quantum gates (reading) (NC 4.5.1-4.5.2, KLM 4.3)

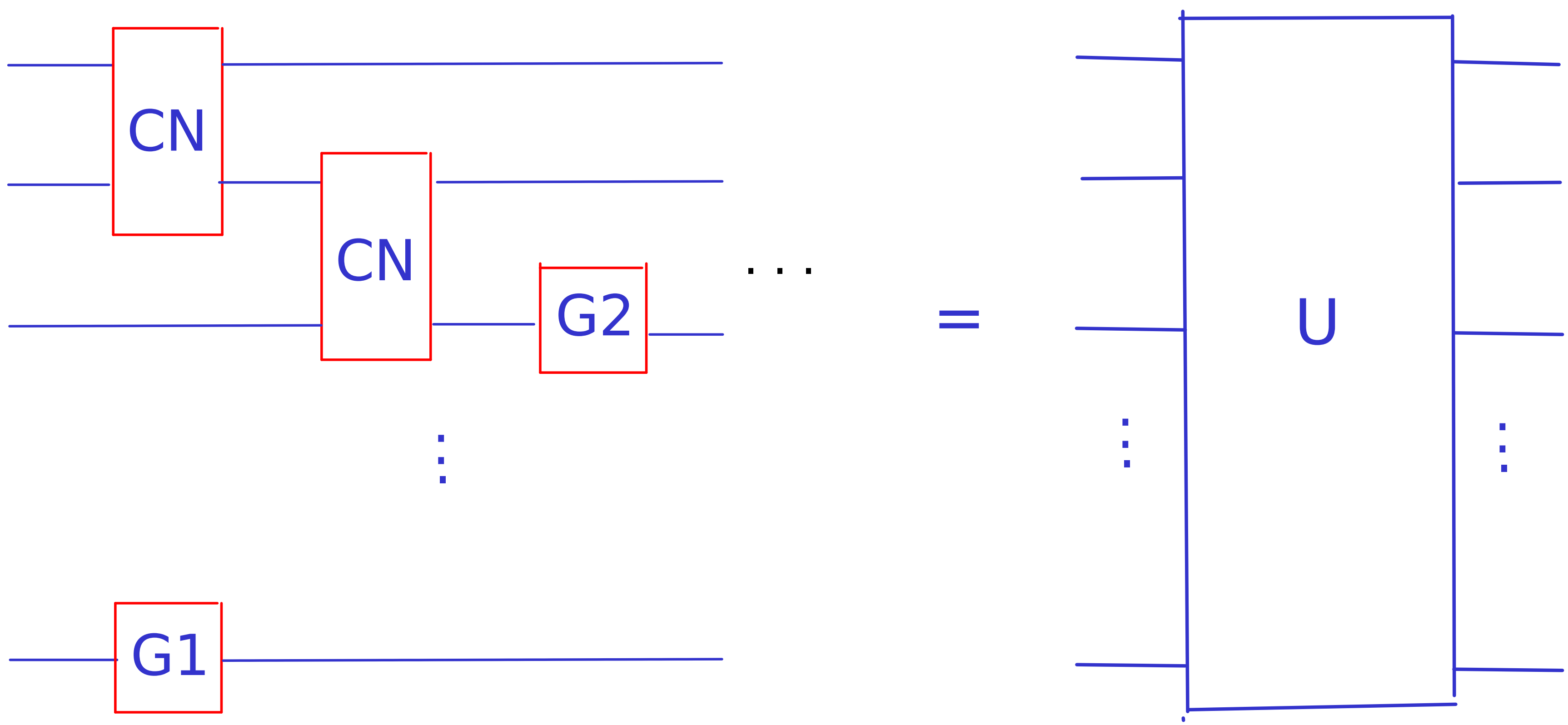
Universal set of quantum gates

Definition: a set G of quantum gates is universal, if for any unitary U, there is a circuit using only gates from G performing U.

Theorem (NC 4.5.1-4.5.2) :
Let S = set of all single-qubit gates.
The set G ={CNOT} U S is universal.

Proof: not difficult but long, left as reading ex.

It means for all n, for all unitary U acting on n qubits, there is a circuit with CNOT's and single qubit gates that implements U:



(b) Quantum gates

Quantum gates

Single-qubit gates

Entangling gates

Simpler to implement
and understand

Necessary, harder
to implement,
preferably 2-body

The Bloch sphere: a useful way to visualize a qubit

The most general qubit:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle \quad \text{where} \quad |a_0|^2 + |a_1|^2 = 1$$

$$= e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

The Bloch sphere: a useful way to visualize a qubit

The most general qubit:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle \quad \text{where} \quad |a_0|^2 + |a_1|^2 = 1$$

$$= e^{i\eta} \left(\cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle \right)$$

since $\exists\, \theta$ s.t. $|a_0|^2 = \cos^2\theta$, $|a_1|^2 = \sin^2\theta$

and η, ϕ give the arguments of a0, a1.

real and non-negative

The Bloch sphere: a useful way to visualize a qubit

The most general qubit:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle \quad \text{where} \quad |a_0|^2 + |a_1|^2 = 1$$

$$= e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

since $\exists\,\theta$ s.t. $|a_0|^2 = \cos^2\theta$, $|a_1|^2 = \sin^2\theta$

and η, ϕ give the arguments of a0, a1.

In test Q2, you showed:

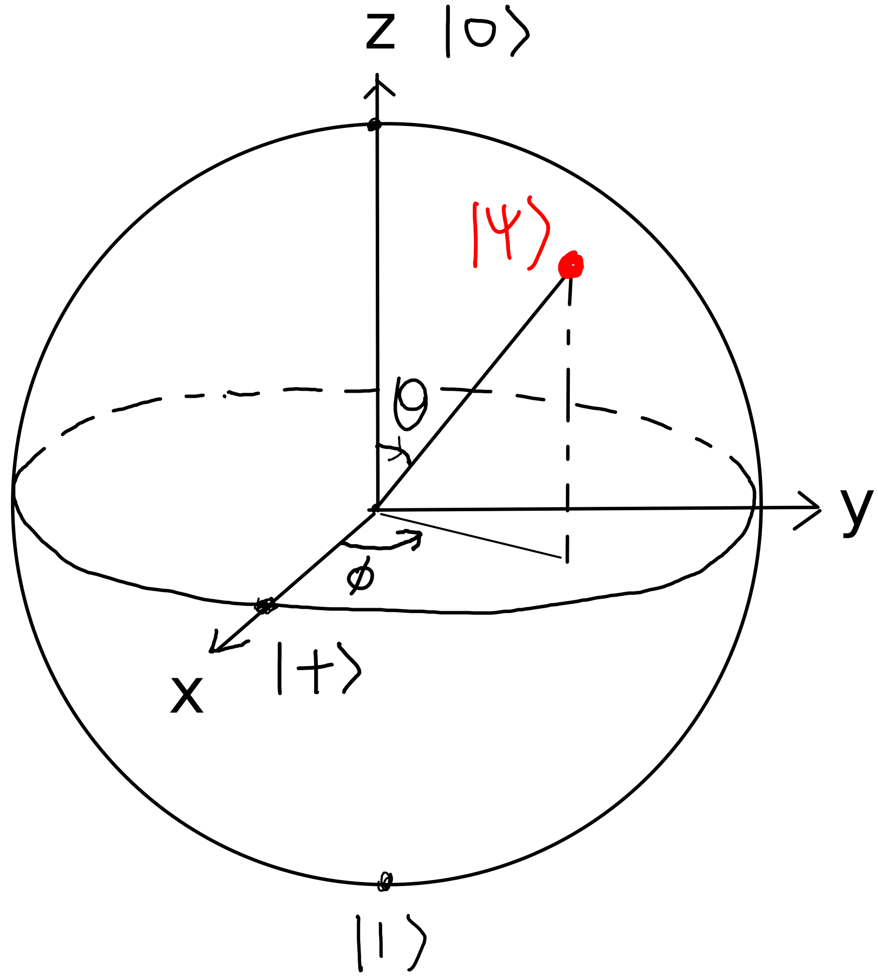
$$|\psi\rangle\langle\psi| = \frac{1}{2}\left(I + \cos\phi\sin\theta\, X + \sin\phi\sin\theta\, Y + \cos\theta\, Z\right)$$

forms a 3-dim, real, unit vector
called the Bloch vector

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

$$|\psi\rangle\langle\psi| = \frac{1}{2}\left(I + \cos\phi\sin\theta\, X + \sin\phi\sin\theta\, Y + \cos\theta\, Z\right)$$

Plotting the 3 coordinates:



Single-qubit gates:

These are 2x2 complex unitaries acting on 1 qubit.

e.g., I, X, Y, Z, Hadamard

1st characterization of single-qubit gates

Theorem:

The most general single-qubit unitary has the form

$$e^{i(\varphi I + \alpha X + \beta Y + \gamma Z)}$$

for some $\varphi, \alpha, \beta, \gamma \in \mathbb{R}$.

1st characterization of single-qubit gates

Theorem:

The most general single-qubit unitary has the form

$$e^{i(\varphi I + \alpha X + \beta Y + \gamma Z)}$$

for some $\varphi, \alpha, \beta, \gamma \in \mathbb{R}$.

Proof idea: U unitary iff $U = e^{iH}$

for some hermitian matrix H

Any 2x2 hermitian matrix is a linear combination of I, X, Y, Z with real coefficients (cf test Q2).

2nd characterization of single-qubit gates

Theorem:

The most general single-qubit unitary has the form

$$R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$$

where $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector.

2nd characterization of single-qubit gates

Theorem:

The most general single-qubit unitary has the form

$$R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$$

where $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector.

Proof: From the 1st char, the unitary has the form

$$e^{i(\phi I + \alpha X + \beta Y + \gamma Z)}.$$

We can choose

$$\varphi = \phi, \quad n_x = \frac{-\alpha}{\sqrt{\alpha^2+\beta^2+\gamma^2}}, \quad n_y = \frac{-\beta}{\sqrt{\alpha^2+\beta^2+\gamma^2}}, \quad n_z = \frac{-\gamma}{\sqrt{\alpha^2+\beta^2+\gamma^2}},$$

$$\xi = 2\sqrt{\alpha^2+\beta^2+\gamma^2}.$$

2nd characterization of single-qubit gates

What does $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

do to the Bloch vector?

2nd characterization of single-qubit gates

What does $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

do to the Bloch vector?

If the initial state is $|\psi\rangle$, and a unitary U is applied,

the resulting state is $U|\psi\rangle$.

2nd characterization of single-qubit gates

What does $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$ do to the Bloch vector?

If the initial state is $|\psi\rangle$, and a unitary U is applied, the resulting state is $U|\psi\rangle$.

So, if $|\psi\rangle\langle\psi| = \frac{1}{2}(I + aX + bY + cZ)$

and $U|\psi\rangle\langle\psi|U^\dagger = \frac{1}{2}(I + a'X + b'Y + c'Z)$

then the Bloch vector changes from (a,b,c) to (a',b',c').

2nd characterization of single-qubit gates

What does $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

do to the Bloch vector?

If the initial state is $|\psi\rangle$, and a unitary U is applied,

the resulting state is $U|\psi\rangle$.

So, if $|\psi\rangle\langle\psi| = \frac{1}{2}(I + aX + bY + cZ)$

and $U|\psi\rangle\langle\psi|U^{\dagger} = \frac{1}{2}(I + a'X + b'Y + c'Z)$

then the Bloch vector changes from (a,b,c) to (a',b',c').

Note: $|\psi\rangle \in \mathbb{C}^2$, $U \in \mathbb{U}(2)$

but we are looking at a transformation on $\mathbb{R}^3$.

e.g., consider U = $e^{-i\frac{\xi}{2}Z}$ $(\hat{n} = (0, 0, 1))$.

By power series expansion, U = $\begin{bmatrix} e^{-i\frac{\xi}{2}} & 0 \\ 0 & e^{i\frac{\xi}{2}} \end{bmatrix}$.

e.g., consider U = $e^{-i\frac{\xi}{2}Z}$ $\quad (\hat{n} = (0, 0, 1))$.

By power series expansion, U = $\begin{bmatrix} e^{-i\frac{\xi}{2}} & 0 \\ 0 & e^{i\frac{\xi}{2}} \end{bmatrix}$.

If $|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$

then $U|\psi\rangle = e^{i\eta}\left(e^{-i\frac{\xi}{2}}\cos\frac{\theta}{2}|0\rangle + e^{i\frac{\xi}{2}}e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$

$$= e^{i\eta}\, e^{-i\frac{\xi}{2}}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\xi}e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

e.g., consider U = $e^{-i\frac{\xi}{2}Z}$ $\quad (\hat{n} = (0,0,1))$.

By power series expansion, U = $\begin{bmatrix} e^{-i\frac{\xi}{2}} & 0 \\ 0 & e^{i\frac{\xi}{2}} \end{bmatrix}$.

If $|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$

then $U|\psi\rangle = e^{i\eta}\left(e^{-i\frac{\xi}{2}}\cos\frac{\theta}{2}|0\rangle + e^{i\frac{\xi}{2}}e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$

$= e^{i\eta}e^{-i\frac{\xi}{2}}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\xi}e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$

So, when $|\psi\rangle \longrightarrow U|\psi\rangle$, $\phi \longrightarrow \xi + \phi$

θ unchanged

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + \cos\phi\sin\theta\, X + \sin\phi\sin\theta\, Y + \cos\theta\, Z)$$

$$U|\psi\rangle = e^{i\eta}\, e^{-i\frac{\xi}{2}}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\xi}\, e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

$$U|\psi\rangle\langle\psi|U^{\dagger} = \frac{1}{2}(I + \cos(\phi+\xi)\sin\theta\, X + \sin(\phi+\xi)\sin\theta\, Y + \cos\theta\, Z)$$

$$|\psi\rangle \longrightarrow U|\psi\rangle$$

$$\phi \longrightarrow \xi + \phi$$

θ unchanged

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

$$|\psi\rangle\langle\psi| = \frac{1}{2}\left(I + \cos\phi\sin\theta\, X + \sin\phi\sin\theta\, Y + \cos\theta\, Z\right)$$

$$U|\psi\rangle = e^{i\eta}\, e^{-i\frac{\xi}{2}}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\xi} e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

$$U|\psi\rangle\langle\psi|U^\dagger = \frac{1}{2}\left(I + \cos(\phi+\xi)\sin\theta\, X + \sin(\phi+\xi)\sin\theta\, Y + \cos\theta\, Z\right)$$

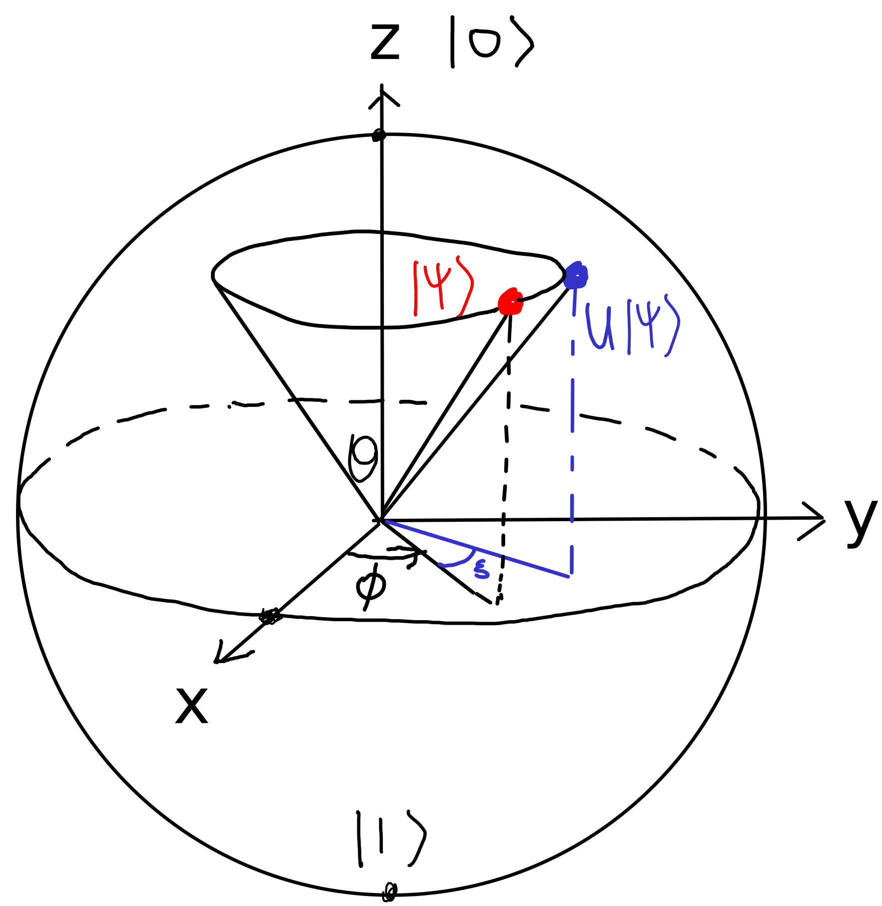
$|\psi\rangle \longrightarrow U|\psi\rangle$

$\phi \longrightarrow \xi + \phi$

θ unchanged

$e^{-i\frac{\xi}{2}Z}$ is a rotation about the z-axis of angle ξ !

End of e.g.



use right-hand-rule

So, $e^{-i\frac{\xi}{2}Z}$ is a rotation about the z-axis of angle ξ.

What is $e^{i\varphi}\, e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$?

2nd characterization of single-qubit gates

Claim: $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

rotates the Bloch vector by an angle ξ

about the axis $\hat{n} = (n_x, n_y, n_z)$.

2nd characterization of single-qubit gates

Claim: $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

rotates the Bloch vector by an angle ξ

about the axis $\hat{n} = (n_x, n_y, n_z)$.

Proof: let $M = n_x X + n_y Y + n_z Z$.

$$M^2 = (n_x X + n_y Y + n_z Z)(n_x X + n_y Y + n_z Z)$$

2nd characterization of single-qubit gates

Claim: $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

rotates the Bloch vector by an angle ξ

about the axis $\hat{n} = (n_x, n_y, n_z)$.

Proof: let $M = n_x X + n_y Y + n_z Z$.

$$M^2 = (n_x X + n_y Y + n_z Z)(n_x X + n_y Y + n_z Z)$$

$$= n_x^2 X^2 + n_y^2 Y^2 + n_z^2 Z^2 + n_x n_y (XY + YX) + n_x n_z (XZ + ZX) + n_y n_z (YZ + ZY)$$

all equal to I

all equal to 0, since any two of the Pauli matrices anticommute

2nd characterization of single-qubit gates

Claim: $R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$

rotates the Bloch vector by an angle ξ

about the axis $\hat{n} = (n_x, n_y, n_z)$.

Proof: let M = $n_x X + n_y Y + n_z Z$.

$$M^2 = (n_x X + n_y Y + n_z Z)(n_x X + n_y Y + n_z Z)$$

$$= n_x^2 X^2 + n_y^2 Y^2 + n_z^2 Z^2 + n_x n_y (XY + YX)$$
$$+ n_x n_z (XZ + ZX)$$
$$+ n_y n_z (YZ + ZY)$$

all equal to I

all equal to 0, since any two of the Pauli matrices anticommute

$$= I$$

since $\hat{n}$ is a unit vector

So, what are the eigenvalues of M?

$M = n_x X + n_y Y + n_z Z$ hermitian so real eigenvalues.

tr (M) = 0, $M^2 = I$.

So, what are the eigenvalues of M?

$M = n_x X + n_y Y + n_z Z$ hermitian so real eigenvalues.

$\mathrm{tr}(M) = 0$, $M^2 = I$.

So, the eigenvalues are +1, -1.

So, what are the eigenvalues of M?

$M = n_x X + n_y Y + n_z Z$ hermitian so real eigenvalues.

$\mathrm{tr}(M) = 0$, $M^2 = I$.

So, the eigenvalues are +1, -1.

By spectral decomposition: $M = V Z V^\dagger$ for some unitary V!

So, what are the eigenvalues of M?

M = $n_x X + n_y Y + n_z Z$ hermitian so real eigenvalues.

tr (M) = 0, $M^2 = I$.

So, the eigenvalues are +1, -1.

By spectral decomposition: $M = V Z V^{\dagger}$ for some unitary V!

$$R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$$

$$= e^{i\varphi} e^{-i\frac{\xi}{2} V Z V^{\dagger}}$$

$$= e^{i\varphi} V e^{-i\frac{\xi}{2} Z} V^{\dagger}$$ by test Q1

So, what are the eigenvalues of M?

$M = n_x X + n_y Y + n_z Z$ hermitian so real eigenvalues.

$\mathrm{tr}(M) = 0$, $M^2 = I$.

So, the eigenvalues are +1, -1.

By spectral decomposition: $M = V Z V^\dagger$ for some unitary V!

$$R_{\hat{n}}(\xi) := e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$$

$$= e^{i\varphi} e^{-i\frac{\xi}{2} V Z V^\dagger}$$

$$= e^{i\varphi} V e^{-i\frac{\xi}{2} Z} V^\dagger$$ by test Q1

When we apply V or $V^\dagger$ to the qubit, how does the Bloch vector transform?

When we apply V or $V^\dagger$ to the qubit, how does the Bloch vector transform?

$\therefore$ $M = V Z V^\dagger$

$\frac{1}{2}(I + M) = V \frac{1}{2}(I + Z) V^\dagger$ (add I to both sides then divide by 2)

When we apply V or $V^\dagger$ to the qubit, how does the Bloch vector transform?

$\because$ $M = V Z V^\dagger$

$$\frac{1}{2}(I+M) = V \frac{1}{2}(I+Z) V^\dagger$$

$$\parallel$$

$$\frac{1}{2}(I + n_x X + n_y Y + n_z Z)$$

$\therefore$ V takes the Bloch vector $(0,0,1)$ to (n_x, n_y, n_z).

When we apply V or $V^\dagger$ to the qubit, how does the Bloch vector transform?

$\because$ $M = V Z V^\dagger$

$$\frac{1}{2}(I + M) = V \frac{1}{2}(I + Z) V^\dagger$$

$$\parallel$$

$$\frac{1}{2}(I + n_x X + n_y Y + n_z Z)$$

$\therefore$ V takes the Bloch vector (0,0,1) to (n_x, n_y, n_z).

Furthermore, conjugating the above equation by $V^\dagger$

$V^\dagger M V = Z$, so, $V^\dagger$ takes (n_x, n_y, n_z) to (0,0,1).

Altogether:

$$R_{\hat{n}}(\xi) = e^{i\varphi}\, V e^{-i\frac{\xi}{2}Z}\, V^{+}$$

1. V^{+} takes (n_x, n_y, n_z) to (0,0,1).

2. $e^{-i\frac{\xi}{2}Z}$ rotates about the z-axis (0,0,1) of angle ξ.

3. V takes (0,0,1) back to (n_x, n_y, n_z).

$\therefore R_{\hat{n}}(\xi)$ rotates about the axis (n_x, n_y, n_z) of angle ξ.

For the Pauli matrices:

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

they are all π rotations on the Bloch sphere, but they are also generators of rotations, namely:

$$R_x(\alpha) := e^{-i\frac{\alpha}{2}X}$$

$$R_y(\alpha) := e^{-i\frac{\alpha}{2}Y}$$

$$R_z(\alpha) := e^{-i\frac{\alpha}{2}Z}$$

These are rotations about the x, y, z-axes of angle α.

Remark:

$$U = R_{\hat{n}}(\xi) = e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$$

Consider the mapping

from 2x2 matrices to 2x2 matrices:

$$f(M) = U M U^{\dagger} .$$

What are the invariances of f ?

set of M such that f(M) = M

Remark:

$$U = R_{\hat{n}}(\xi) = e^{i\varphi} e^{-i\frac{\xi}{2}(n_x X + n_y Y + n_z Z)}$$

Consider the mapping
from 2x2 matrices to 2x2 matrices:

$$f(M) = U M U^{\dagger}.$$

What are the invariances of f ?

f(I) = I, f(M) = M,
so, for all scalars a, b, f(aI + bM) = aI + bM

Fact: if $U \neq I$, then, no more invariances.
Proof: exercise. Hint: consider a spanning set
for 2x2 matrices that include I and M.

Question:

Suppose a 2x2 unitary U does the following:

$$U X U^\dagger = Y$$

$$U Y U^\dagger = Z$$

$$U Z U^\dagger = X$$

Which of the following can be U?

(a) $(X+Y+Z)/\sqrt{3}$

(b) $e^{-i\frac{\pi}{2}(X+Y+Z)/\sqrt{3}}$

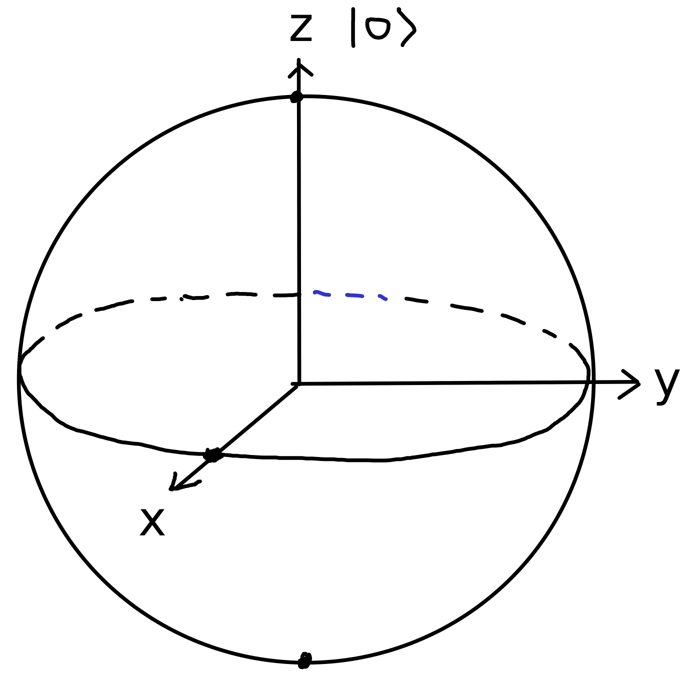
(c) $e^{-i\frac{\pi}{3}(X+Y+Z)/\sqrt{3}}$

(d) $e^{i\frac{\pi}{3}(X+Y+Z)/\sqrt{3}}$

$$U X U^\dagger = Y$$

$$U Y U^\dagger = Z$$

$$U Z U^\dagger = X$$

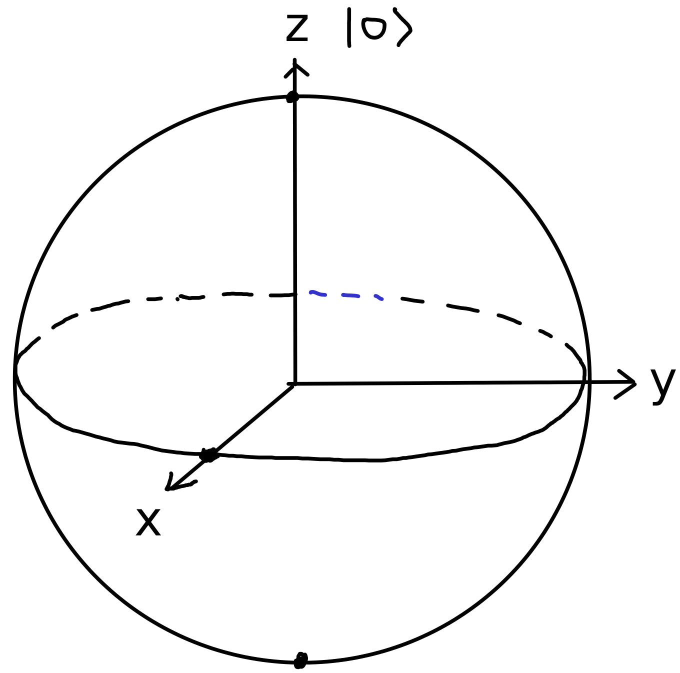


So, the axis of rotation on the Bloch sphere is

$$(X+Y+Z)/\sqrt{3}$$

since this matrix is an invariant under the conjugation by U.

$$U X U^\dagger = Y$$
$$U Y U^\dagger = Z$$
$$U Z U^\dagger = X$$



So, the axis of rotation on the Bloch sphere is

$$(X+Y+Z)/\sqrt{3}$$

since this matrix is an invariant under the conjugation by U.

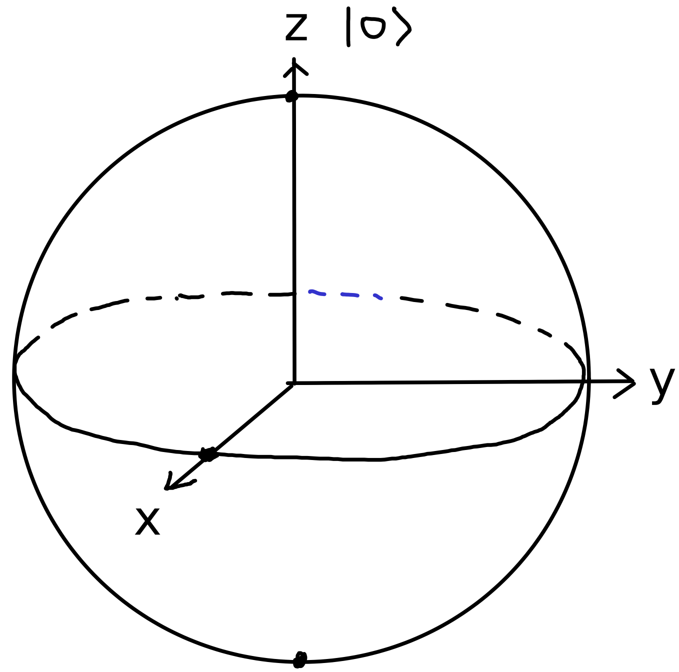
The angle of rotation is $\pm\, \xi = 2\pi/3$???

since $U^3 = I$.

$$U X U^\dagger = Y$$

$$U Y U^\dagger = Z$$

$$U Z U^\dagger = X$$



So, the axis of rotation on the Bloch sphere is

$$(X+Y+Z)/\sqrt{3}$$

since this matrix is an invariant under the conjugation by U.

The angle of rotation is $+\xi = 2\pi/3$.

Answer = $e^{-i\frac{\xi}{2}(X+Y+Z)/\sqrt{3}} = e^{-i\frac{\pi}{3}(X+Y+Z)/\sqrt{3}}$

(c)

3rd characterization of single-qubit gates

Theorem: (NC Thm 4.1)

The most general single-qubit unitary has the form

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

(From Euler angles, but there is also a quick direct proof using linear algebra.)

Check lecture time ... may demote proof to reading.

Theorem: (NC Thm 4.1)

The most general single-qubit unitary has the form

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

relative phase between the 2 columns

Proof: any 2x2 unitary has the form

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

overall phase for both columns

$U|0\rangle$: general qubit state up to overall phase

$U|1\rangle$: qubit state ortho to $U|0\rangle$ up to a phase

Finally, checking:

$$R_z(\beta)\ R_y(\gamma)\ R_z(\delta)$$

phases multi-
plied to rows

phases multi-
plied to cols

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

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

completes the proof.

Corollary:

The most general single-qubit unitary has the form

$$W = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

y in the theorem

Corollary:

The most general single-qubit unitary has the form

$$W = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Proof: $W = R_z(-\frac{\pi}{2})\, U\, R_z(\frac{\pi}{2})$ for some 2×2 unitary U.

becaus you can take

$$R_z(\tfrac{\pi}{2})\, W\, R_z(-\tfrac{\pi}{2}) = U$$

Corollary:

The most general single-qubit unitary has the form

$$W = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Proof: $W = R_z(-\frac{\pi}{2})\, U\, R_z(\frac{\pi}{2})$ for some 2×2 unitary U.

From the theorem $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

for some $\alpha, \beta, \gamma, \delta \in \mathbb{R}$,

so, $W = R_z(-\frac{\pi}{2})\, e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)\, R_z(\frac{\pi}{2})$

Corollary:

The most general single-qubit unitary has the form

$$W = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Proof: $W = R_z(-\frac{\pi}{2})\, U\, R_z(\frac{\pi}{2})$ for some 2×2 unitary U.

From the theorem $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

for some $\alpha, \beta, \gamma, \delta \in \mathbb{R}$,

so, $W = R_z(-\frac{\pi}{2})\, e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) R_z(\frac{\pi}{2})$

$= e^{i\alpha} R_z(-\frac{\pi}{2}) R_z(\beta) R_z(\frac{\pi}{2}) R_z(-\frac{\pi}{2}) R_y(\gamma) R_z(\frac{\pi}{2}) R_z(-\frac{\pi}{2}) R_z(\delta) R_z(\frac{\pi}{2})$

Corollary:

The most general single-qubit unitary has the form

$$W = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Proof: $W = R_z(-\frac{\pi}{2})\, U\, R_z(\frac{\pi}{2})$ for some 2×2 unitary U.

From the theorem $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

for some $\alpha, \beta, \gamma, \delta \in \mathbb{R}$,

so, $W = R_z(-\frac{\pi}{2})\, e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) R_z(\frac{\pi}{2})$

$$= e^{i\alpha} \underbrace{R_z(-\tfrac{\pi}{2}) R_z(\beta) R_z(\tfrac{\pi}{2})}_{R_z(\beta)} \underbrace{R_z(-\tfrac{\pi}{2}) R_y(\gamma) R_z(\tfrac{\pi}{2})}_{R_x(\gamma)} \underbrace{R_z(-\tfrac{\pi}{2}) R_z(\delta) R_z(\tfrac{\pi}{2})}_{R_z(\delta)}$$

(b) Quantum gates

Quantum gates

Single-qubit gates

Entangling gates

Simpler to implement
and understand

Necessary, harder
to implement,
preferably 2-body

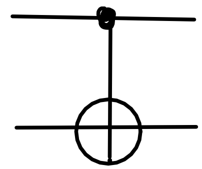
Entangling gates:

Definition: a unitary U that acts on two systems S1, S2 is a tensor product unitary if $U = U1 \otimes U2$ for some unitaries U1 (U2) acting on S1 (S2).

A unitary U is called entangling if it is not a tensor product unitary.

Entangling gates:

Example: CNOT



control (1st qubit)

target (2nd qubit)

Action on a basis:

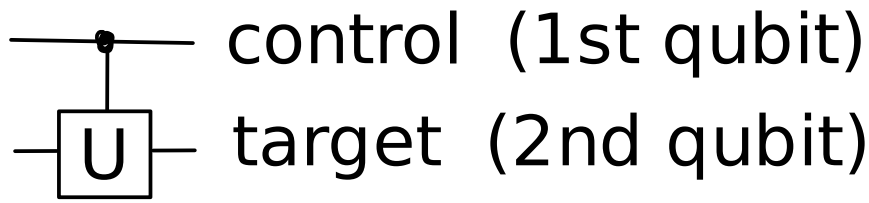
$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$$
$$|1\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$$

Conditioned on control being "1" (filled circle)
apply a NOT to the target.

Matrix representation:
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Entangling gates:

Generalization:
controlled-U



Action on a basis:

$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \longrightarrow |1\rangle\, U|0\rangle$$
$$|1\rangle|1\rangle \longrightarrow |1\rangle\, U|1\rangle$$

Conditioned on control being "1" (filled circle)
apply U to the target.

Matrix representation:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{\boxed{U}}} \\ 0 & 0 & & \end{pmatrix}$$

In Dirac notation: $C\text{-}U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$

Labelling the control register "C" and target register "T"

$\forall\, |\psi\rangle, a, b:$

$$(a|0\rangle + b|1\rangle)_C\, |\psi\rangle_T \longrightarrow a|0\rangle_C |\psi\rangle_T + b|1\rangle_C (U|\psi\rangle_T)$$

Question:

Let $U \neq I$. Is there an input for which the control qubit is changed by the controlled-U gate?

(a) for any such U, there is always an input such that the control qubit changes,

(b) for some U, the control qubit never changes, for some other U, there is an input such that the control qubit changes,

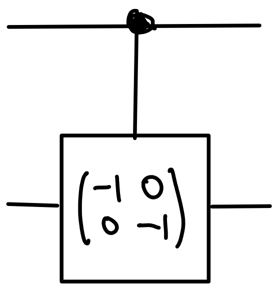
(c) the control qubit is never changed by a controlled-U gate.

Answer in the next 3 pages. Please do not read before we vote ...

(c) is wrong.

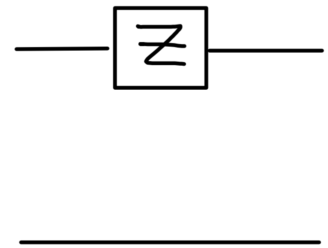
Unlike the classical setting, the control register of a c-U gate can be changed by the gate !

e.g.1 c-(-I) = Z $\otimes$ I



$$|00\rangle \longrightarrow |00\rangle$$
$$|01\rangle \longrightarrow |01\rangle$$
$$|10\rangle \longrightarrow -|10\rangle$$
$$|11\rangle \longrightarrow -|11\rangle$$

which is



NB. Overall phase of U matters when taking c-U.

e.g.2, for CNOT, consider the input

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

Output after a CNOT: $\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)$

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

(a) is correct. If $U \neq I$, there is an input whose controlled qubit is changed by controlled-U:

Proof: let U has eigenvalues λ_0, λ_1 with corresponding eigenvectors $|e_0\rangle, |e_1\rangle$.

Since $U \neq I$, at least one eigenvalue not equal to one.

(a) is correct. If $U \neq I$, there is an input whose controlled qubit is changed by controlled-U:

Proof: let U has eigenvalues λ_0, λ_1 with corresponding eigenvectors $|e_0\rangle, |e_1\rangle$.

Since $U \neq I$, at least one eigenvalue not equal to one.

WLOG: let $\lambda_0 \neq 1$.

Take the input: $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_C \otimes |e_0\rangle_T$

Output of the gate: $\frac{1}{\sqrt{2}}|0\rangle_C \otimes |e_0\rangle_T + \frac{1}{\sqrt{2}}|1\rangle_C \otimes \lambda_0|e_0\rangle_T$

(a) is correct. If $U \neq I$, there is an input whose controlled qubit is changed by controlled-U:

Proof: let U has eigenvalues λ_0, λ_1 with corresponding eigenvectors $|e_0\rangle, |e_1\rangle$.

Since $U \neq I$, at least one eigenvalue not equal to one.

WLOG: let $\lambda_0 \neq 1$.

Take the input: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_C \otimes |e_0\rangle_T$

Output of the gate: $\frac{1}{\sqrt{2}}|0\rangle_C \otimes |e_0\rangle_T + \frac{1}{\sqrt{2}}|1\rangle_C \otimes \lambda_0|e_0\rangle_T$

$$= \frac{1}{\sqrt{2}}(|0\rangle + \lambda_0|1\rangle)_C \otimes |e_0\rangle_T$$

So the control qubit is changed (a "phase kick-back")!

Question:

Is the SWAP gate, defined by: $|i\rangle|j\rangle \longrightarrow |j\rangle|i\rangle$ entangling?

(a) Yes
(b) No

Question:

Is the SWAP gate, defined by: $|i\rangle|j\rangle \longrightarrow |j\rangle|i\rangle$ together with all single qubit gates, a universal gate set for quantum computation ?

(a) Yes
(b) No

Recall for classical circuits:

<u>Definition: universal set of gates</u>

A set of gates G is universal if :

for any positive integers n,m
and
for any function f : $\{0,1\}^n \to \{0,1\}^m$
there is a circuit to compute f using the gates in G.

For quantum circuits: the possible unitaries form a continous set. Do we need a continous set of gates for universality (e.g., CNOT+all 1-qubit gates)?