

Quantum gates (section 4.1 in main ref.)

Terminology

A gate is a unitary transform (unitary matrix) on $\mathbb{C}^N$ representing a quantum mechanical system

Ex. gates on single qubit space $\mathbb{C}^2$

Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$

for $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, ...

NOT gate $\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $\text{NOT}|0\rangle = |1\rangle$, $\text{NOT}|1\rangle = |0\rangle$

"square root of NOT" $\sqrt{\text{NOT}} = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$ $\sqrt{\text{NOT}}^2 = \text{NOT}$

$$\sqrt{\text{NOT}}^2 = \frac{1}{4} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 2i-2i & 2+2 \\ 2+2 & 2i-2i \end{bmatrix}$$

Measurement of quantum mechanical system

Setting : $\mathbb{C}^N$ for some QM system

$|V_i\rangle$ ($0 \leq i < N$) some orthonormal basis of $\mathbb{C}^N$
state

corresponding to some "type" of information on the system

- value of i : possible value of that info. type

Ex. spin "up" or "down" for electron

- state of the system with value i : $|V_i\rangle \in \mathbb{C}^N$

(generalized) Born rule

suppose the system is in some generic state represented

by $|\psi\rangle \in \mathbb{C}^N$, when you do a measurement, you get

the ^{unit vector} value i with probability $p_i = |\underbrace{\langle V_i | \psi \rangle}_{\text{amplitude}}|^2$

Rem. $\|\psi\| = 1 \Leftrightarrow \sum_{0 \leq i < N} p_i = 1$

$$(|v_i\rangle)_{0 \leq i < N}$$

orthonormal basis of $\mathbb{C}^N$

$$\forall |\psi\rangle = \sum_{0 \leq i < N} \alpha_i |v_i\rangle$$

$$\alpha_i = \langle v_i | \psi \rangle$$

from $\rightarrow$

$$\langle v_i | v_j \rangle = \begin{cases} 0 & (i \neq j) \\ 1 & (i = j) \end{cases}$$

$$\|\psi\|^2 = \langle \psi | \psi \rangle = \sum_{0 \leq i, j < N} \alpha_i^* \alpha_j \langle v_i | v_j \rangle$$

$$= \sum_{0 \leq i < N} \alpha_i^* \alpha_i = \sum_i |\alpha_i|^2$$

Contrast between gates and measurements

Unitary transformations (gates) U are

- **invertible / reversible** : $U^{-1} = U^\dagger$ ($U^\dagger U = I_N$)
transf: $|\psi\rangle \mapsto |\varphi\rangle = U|\psi\rangle$ can be reversed: $|\varphi\rangle \mapsto U^\dagger|\varphi\rangle$
 $U^\dagger U |\psi\rangle = I_N |\psi\rangle = |\psi\rangle$
- **deterministic** : modelled by a map $\mathbb{C}^N \rightarrow \mathbb{C}^N$
"one output for one input" $|\psi\rangle \mapsto U|\psi\rangle$
- **continuous in time** : modelled by $U^t = \exp(i t H)$
for some $H^\dagger = H$ (self adjoint / Hermitian)
 $\exp(X) = I_N + X + \frac{1}{2} X^2 + \dots + \frac{1}{k!} X^k + \dots$
but in practice we fix some value of t and talk about
just one $U = U^t$

Rem. $\exp(i s H) \exp(i t H) = \exp(i (s+t) H)$

so $U^{\frac{t}{2}}$ is a square root of U^t

$|V_j\rangle$ ($0 \leq j < N$) orthonormal basis diagonalizing H

with $H |V_j\rangle = x_j |V_j\rangle \leadsto U^t |V_j\rangle = e^{i t x_j} |V_j\rangle$

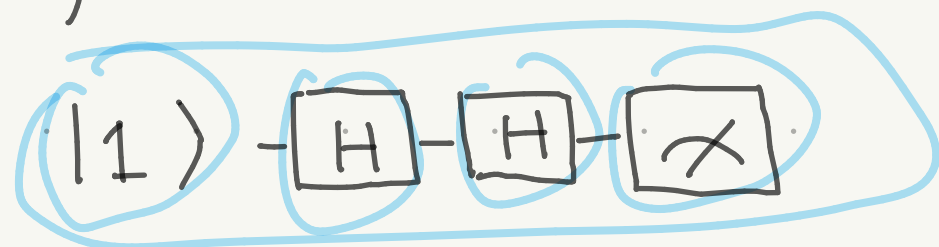
Measurements are :

- **irreversible** : we cannot model measurement by an invertible transform / after measurement of one information, the system is in a new state and info. of other type about the previous state is lost
- **probabilistic** : we can only predict probability of outcomes
- **discontinuous in time** : change of state happens instantaneously

Quantum circuit notation (section 4.2 in main ref.)

"circuit diagram" for various operations on qubits

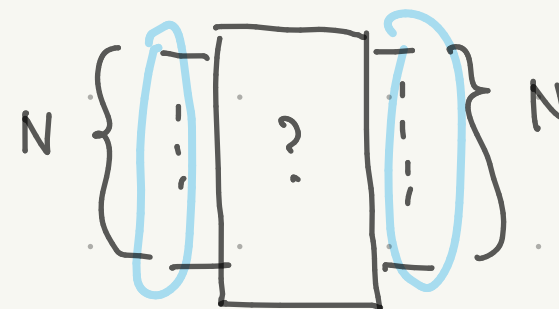
Ex. prepare the $|1\rangle$ qubit, then apply the Hadamard gate twice, then measure the system (for some info.):

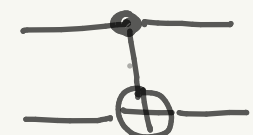


i.e.  gate acting on single qubit (2×2 unitary mat.)

 some measurement

we can have gates acting on multiple qubits
($2^N \times 2^N$ unitary matrix)



Ex.  CNOT gate

Single qubit gates

$$\boxed{\text{NOT}} = \boxed{\text{X}} : \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{NOT / Pauli-X gate}$$

$$\boxed{\text{Y}} : \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \text{Pauli-Y gate}$$

$$\boxed{\text{Z}} : \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{Pauli-Z gate}$$

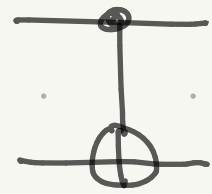
$$\boxed{\text{H}} : \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{Hadamard gate}$$

$$\boxed{\text{R}_\theta} : \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \quad \text{rotation gate}$$

$$\boxed{\text{R}_\phi} : \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \quad \text{phase shift gate}$$

$$\boxed{\text{R}_{\phi = \frac{\pi}{4}}} = \boxed{\text{T}} : \text{T gate} \quad \begin{bmatrix} 1 & \\ & \frac{1+i}{2} \end{bmatrix}$$
$$\boxed{\text{R}_{\phi = \frac{\pi}{2}}} = \boxed{\text{S}} : \text{S gate} \quad \begin{bmatrix} 1 & \\ & i \end{bmatrix}$$

Two-qubit gates

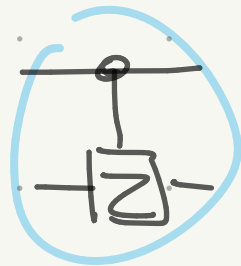


$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}$$

$|0\rangle \otimes |0\rangle$

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |11\rangle \\ |11\rangle &\mapsto |10\rangle \end{aligned}$$

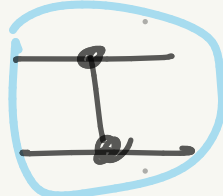
CNOT gate

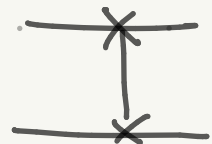


$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}$$

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |10\rangle \\ |11\rangle &\mapsto -|11\rangle \end{aligned}$$

controlled-Z gate

(sometimes  because it's invariant under $|ij\rangle \leftrightarrow |ji\rangle$)

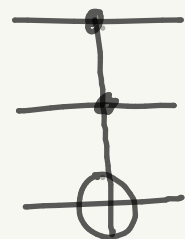


$$\begin{bmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{bmatrix}$$

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |10\rangle \\ |10\rangle &\mapsto |01\rangle \\ |11\rangle &\mapsto |11\rangle \end{aligned}$$

swap gate

Three-qubit gates

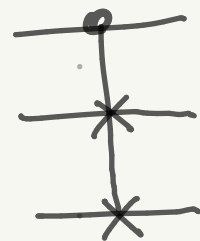


$$|0 * j\rangle \mapsto |0 * j\rangle$$

$$|* 0 j\rangle \mapsto |* 0 j\rangle$$

$$|1 1 0\rangle \mapsto |1 1 1\rangle$$

$$|1 1 1\rangle \mapsto |1 1 0\rangle$$



$$|0 * * \rangle \mapsto |0 * * \rangle$$

$$|1 j k\rangle \mapsto |1 k j\rangle$$

Toffoli gate

controlled - controlled - NOT

Fredkin gate

controlled - swap

Turing's paradox / quantum Zeno effect (section 4.3)

suppose we have some deviation from our initial state due to some error, etc.

original state $|0\rangle$, but after time t_ε we are in

$$\text{the state } |\psi_\varepsilon\rangle = \cos \varepsilon |0\rangle + \sin \varepsilon |1\rangle = R_\varepsilon |0\rangle$$

performing measurement (for $|0\rangle, |1\rangle$) at time t_ε ,

find state $|0\rangle$ with prob. $|\langle 0 | \psi_\varepsilon \rangle|^2 = \cos^2 \varepsilon \sim 1 - \varepsilon^2$

state $|1\rangle$ with prob. $|\langle 1 | \psi_\varepsilon \rangle|^2 = \sin^2 \varepsilon \sim \varepsilon^2$

- we would have $t_{\frac{\varepsilon}{N}} \sim \frac{1}{N} t_\varepsilon$ if the rotation is const.

- performing measurement with interval $t_{\frac{\varepsilon}{N}}$, N times

we would find state $|1\rangle$ with prob. $\sim N \cdot \left(\frac{\varepsilon}{N}\right)^2 = \frac{\varepsilon^2}{N}$
at most

(cont.) consequence:

frequently observing a QM system slows deviation

experimental confirmation ('89)

"Elitzer - Vaidman bomb"

thought experiment:

consider the "bomb" machine:

accepts input $|\psi\rangle \in \mathbb{C}^2$ (one qubit)

performs measurement for basis $|0\rangle, |1\rangle$

if $|0\rangle$ is observed, output $|0\rangle$

if $|1\rangle$ is observed, explode

there is a suitcase that might contain this machine

if there is no bomb, input qubit is returned

if there is bomb, it works as above

Start with $|v^0\rangle = |0\rangle$, construct $|v^i\rangle$ ($i=1, 2, \dots$) by

- feed $|v^i\rangle$ to the suitcase, get $|w^i\rangle$

- (if it didn't explode) apply rotation $|v^{i+1}\rangle = R_\epsilon |w^i\rangle$

after $N \sim \frac{\pi}{2\varepsilon}$ times repeat

if there is a bomb, we receive back $|0\rangle$ each time
(or explodes)

$$\text{then } |v^i\rangle = R_\varepsilon |0\rangle = \cos \varepsilon |0\rangle + \sin \varepsilon |1\rangle$$

bomb observes $|1\rangle$ with prob. $\sin^2 \varepsilon$
it has exploded up to probability $\sim \frac{\pi}{2\varepsilon} \sin^2 \varepsilon \sim \frac{\pi}{2} \varepsilon$

if we survived, measurement for $|0\rangle, |1\rangle$ gives $|0\rangle$

$\leadsto$ we survive with prob. $1 - \frac{\pi \varepsilon}{2}$, measurement gives $|0\rangle$

if there is no bomb, we receive $|u^i\rangle = |v^i\rangle = R_\varepsilon |u^{i-1}\rangle$

$$|v^N\rangle = R_\varepsilon^N |v^0\rangle \sim \cos \frac{\pi}{2} |0\rangle + \sin \frac{\pi}{2} |1\rangle = |1\rangle$$

measurement for $|0\rangle, |1\rangle$ gives $|1\rangle$ almost certainly

$\leadsto$ we can decide if bomb was in the suitcase or not
with high prob.

Review of quiz2

compos. prod MM' : apply M' to the system,
then apply M

convex combination $tM + (1-t)M'$:

with prob. t apply M , with prob. $1-t$ apply M'

tensor product $M \otimes M'$

apply M to one part of the system

M' to another part

$$p \otimes q \mapsto M p \otimes M' q$$

uncorrelated
prob. distr

compos. prod UU' : apply U' to the system,

then apply U ; $(UU')^\dagger = U'^\dagger U^\dagger = U'^{-1}U^{-1}$
 $= (UU')^{-1}$

convex combination $tU + (1-t)U'$ would be

with prob. t apply U , with prob. $1-t$ apply U'

NOT deterministic! $I_2, -I_2$ unitary $tI_2 + (1-t)(-I_2)$
 $= (2t-1)I_2$

tensor product $U \otimes U'$

apply U to one part of the system

U' to another part

$$(U \otimes U')^\dagger = U^\dagger \otimes U'^\dagger$$

$$(U \otimes U')^{-1} = U^{-1} \otimes U'^{-1}$$

$$|v\rangle \otimes |v'\rangle \mapsto U|v\rangle \otimes U'|v'\rangle$$

state vec.

general property of tensor product

$$(A \otimes B)(A' \otimes B') = AA' \otimes BB'$$

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

$$(A \otimes B)(A^{-1} \otimes B^{-1}) = I_N \otimes I_M \Rightarrow A^{-1} \otimes B^{-1} = (A \otimes B)^{-1}$$