① Recap: Density Matrices

- A density matrix in dimension $d \in \{2,3,\dots\}$ is a $d \times d$ matrix $\rho \in L(\mathbb{C}^d)$ satisfying the following properties:

(1) Hermitian: $\rho^\dagger = \rho$ $\quad$ $\dagger \equiv$ conjugate transpose.

(2) Unit Trace: $\mathrm{Tr}[\rho] = 1$ $\quad$ (Recall: Tr ≡ trace ≡ sum of diagonal elements of a matrix)

(3): Positive Semi-definite: $\rho \geq 0$

⊛ This means that $\langle v|\rho|v\rangle \geq 0 \ \forall\ |v\rangle \in \mathbb{C}^d$.

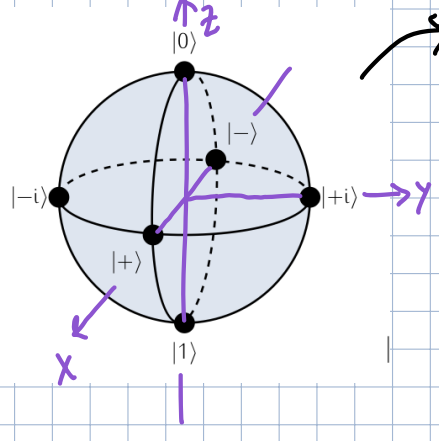
Equivalently: all the eigenvalues of ρ are non-negative.

↳ $M|v\rangle = \lambda|v\rangle$

⊛ **Axiom of Quantum Mechanics:** The state of any quantum system is mathematically described by a density matrix. (arbitrary dimension).

State vector: $|\psi\rangle \to \||\psi\rangle\| = 1 \to \rho = |\psi\rangle\langle\psi|$

- For $d=2$ (qubits), density matrices are synonymous with points on and inside the unit sphere.



(Bloch sphere).

→ Point $\vec{r} \in \mathbb{R}^3$ (real 3D space)

$\vec{r} = (r_x, r_y, r_z)$, $\rho = \frac{1}{2}(\mathbb{1} + r_x X + r_y Y + r_z Z)$.

$\mathrm{Tr}[\rho X] = \mathrm{Tr}\left[\frac{1}{2}(\mathbb{1} + r_x X + r_y Y + r_z Z)X\right]$

$= \frac{1}{2}\left(\mathrm{Tr}[X] + r_x \mathrm{Tr}[\mathbb{1}] + r_y \mathrm{Tr}[Y] + r_z \mathrm{Tr}[ZX]\right)$

$= r_x$. (Tr[X] = 0, Tr[𝟙] = 2, Tr[Y] = 0, Tr[ZX] = 0)

$r_x^2 + r_y^2 + r_z^2 \leq 1$, $r_x = \mathrm{Tr}[\rho X]$, $r_y = \mathrm{Tr}[\rho Y]$, $r_z = \mathrm{Tr}[\rho Z]$.

- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (Pauli matrices).

- If $r_x^2 + r_y^2 + r_z^2 = 1$, then ρ is a pure state: it can be written as $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathbb{C}^2$ is a state vector; $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

✱ Origin, $\vec{r} = (0,0,0) \to \rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \to$ the maximally-mixed state $\quad |\alpha|^2 + |\beta|^2 = 1$

(A completely random state). $\quad = \frac{\mathbb{1}}{2}$

✱ Points on the X-axis: $\vec{r} = (\pm 1, 0, 0) \to \rho = \frac{1}{2}(\mathbb{1} \pm X) = |\pm\rangle\langle\pm|$, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

These are eigenvectors of X! $X|\pm\rangle = \pm|\pm\rangle$. $\to$ $X|+\rangle = |+\rangle$

(Eigenvalues of X are ± 1.) $\quad X|-\rangle = -|-\rangle$

✱ Points on the Y-axis: $\vec{r} = (0, \pm 1, 0) \to \rho = \frac{1}{2}(\mathbb{1} \pm Y) = |\pm i\rangle\langle\pm i|$, $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$.

These are eigenvectors of Y! $Y|\pm i\rangle = \pm|\pm i\rangle$., $Y|+i\rangle = |+i\rangle$

(Eigenvalues of Y are ± 1.) $\quad Y|-i\rangle = -|-i\rangle$

✱ Points on the Z-axis: $\vec{r} = (0, 0, \pm 1) \to \rho = \frac{1}{2}(\mathbb{1} \pm Z)$ $\begin{cases} (+) \to |0\rangle\langle 0| \\ (-) \to |1\rangle\langle 1|. \end{cases}$

These are eigenvectors of Z! $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$. (Eigenvalues of Z are ± 1.)

- For higher dimensions, we don't have such a nice representation.
- We can still check if a state is pure using the purity:

For density matrix ρ in dimension d, $\mathrm{Tr}[\rho^2] \equiv$ purity

The state ρ is pure if and only if $\mathrm{Tr}[\rho^2] = 1$.

✱ Every pure state is represented by a density matrix of the form $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathbb{C}^d$ is a state vector ($\||\psi\rangle\| = 1$).

If a state is not pure, then we call it a mixed state.

✱ Important fact: Every mixed state can be written as a convex combination of pure states:

$$\rho = \sum_{k=1}^{M} p_k |\psi_k\rangle\langle\psi_k|, \quad p_k \in [0,1], \quad \sum_{k=1}^{M} p_k = 1.$$

p_k: probabilities.

Check: $\mathrm{Tr}[\rho] = \sum_{k=1}^{m} p_k \underbrace{\mathrm{Tr}[|\gamma_k\rangle\langle\gamma_k|]}_{=1} = \sum_{k=1}^{m} p_k = 1$ ✓

$\left((M_1 + M_2)^\dagger = M_1^\dagger + M_2^\dagger\right)$

Check: $\rho^\dagger = \sum_{k=1}^{m} p_k \underbrace{\left(|\gamma_k\rangle\langle\gamma_k|\right)^\dagger}_{=|\gamma_k\rangle\langle\gamma_k|} = \sum_{k=1}^{m} p_k |\gamma_k\rangle\langle\gamma_k| = \rho$ ✓

$\left(|v_1\rangle\langle v_2|\right)^\dagger = |v_2\rangle\langle v_1|$

Check: $\rho \geq 0$ ⟶ Yes, b/c we sum over PSD elements.

$M_1, M_2 \geq 0$

$\langle v|(M_1 + M_2)|v\rangle = \underbrace{\langle v|M_1|v\rangle}_{\geq 0} + \underbrace{\langle v|M_2|v\rangle}_{\geq 0} \geq 0$

② Quantum Circuits and gates.

- Recap: classical computation: manipulation of bits via logic gates (AND, OR, NOT, XOR)

For input $x \in \{0,1\}^n$, calculate $f(x)$ for some f.
(How to realize f with a circuit? How many gates / depth is necessary and/or sufficient?)

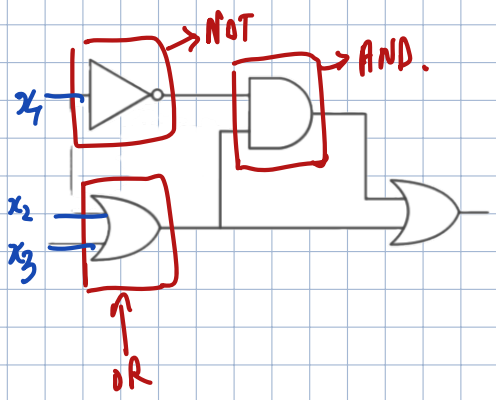
✱ We rarely think about computation in these terms anymore!

✱ We program in some high-level language (C++, python, julia) and then the code gets compiled into the machine-level language.

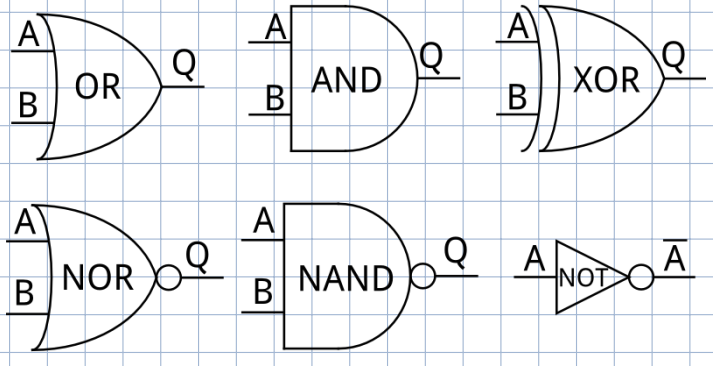
✱ Quantum computing is still thought about at the gate level.

(Although "quantum programming languages" are being developed — qiskit is a simple example.)

- **Classical logic circuits:**



- For every logic gate, we have a truth table (how 0 + 1 are transformed by the gate.)



A	NOT A
0	1
1	0

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

A	B	A OR B
0	0	0
0	1	1
1	0	1
1	1	1

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

control bit / target bit

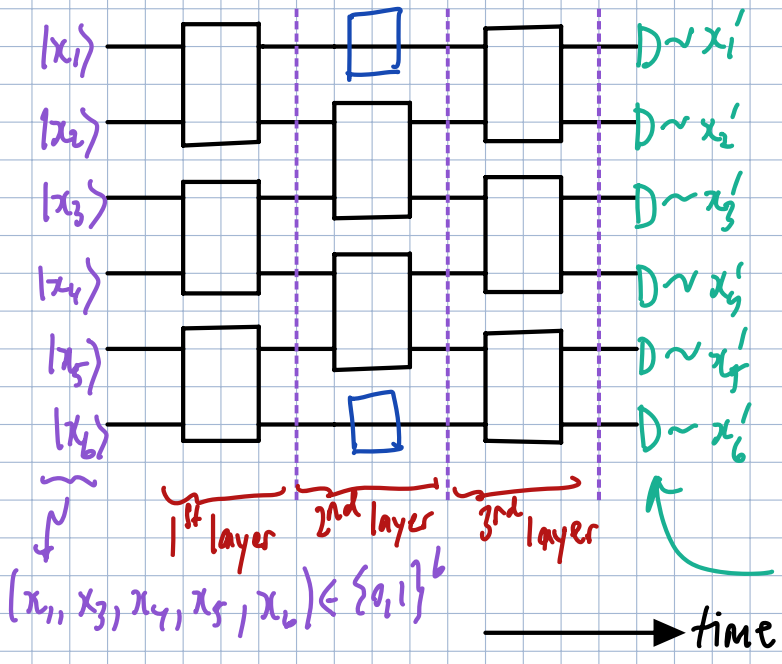
A	B	A CNOT B
0	0	0 0
0	1	0 1
1	0	1 1
1	1	1 0

⊛ Reversible version of XOR gate.

$A, B \mapsto A, A \oplus B.$ ⊕

- For a given circuit, we use these truth tables, combining them to get the truth table of the whole circuit.

• Quantum Circuits and Gates: very similar! But the gates act on the complex vector space $(\mathbb{C}^2)^{\otimes n}$ of n qubits → they are represented by unitary matrices. → matrix $U \in L(\mathbb{C}^d)$ satisfying $U^\dagger U = UU^\dagger = \mathbb{1}$.



✱ Each box represents a gate/unitary matrix.

✱ Multiply the gates to get a unitary matrix for the full circuit.

✱ Why unitary matrix? Comes from quantum physics (Schrödinger equation).

✱ To understand what the circuit does, we just have to know how it acts on basis vectors!

Recall: any state vector of n qubits can be represented as

$$|\psi\rangle = \sum_{\vec{x} \in \{0,1\}^n} c_{\vec{x}} |\vec{x}\rangle, \quad c_{\vec{x}} \in \mathbb{C}, \quad \sum_{\vec{x} \in \{0,1\}^n} |c_{\vec{x}}|^2 = 1.$$

($|\psi\rangle$: input state of the quantum circuit.)

$$\vec{x} \equiv (x_1, x_2, \dots, x_n), \; x_i \in \{0,1\}$$
$$|\vec{x}\rangle \equiv |x_1, x_2, \dots, x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$$

$$\Rightarrow U|\psi\rangle = U\left(\sum_{\vec{x} \in \{0,1\}^n} c_{\vec{x}} |\vec{x}\rangle\right) = \sum_{\vec{x} \in \{0,1\}^n} c_{\vec{x}} \, U|\vec{x}\rangle.$$

(✱ Linearity of matrices: $M(\alpha|v_1\rangle + \beta|v_2\rangle) = \alpha M|v_1\rangle + \beta M|v_2\rangle$).

- From calculating $U|\vec{x}\rangle$ for all $\vec{x}$, we get something like the "truth table" of the quantum circuit.

✱ Elementary quantum gates (building blocks of larger circuits).

- Pauli gates: —[X]— $\rightarrow X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\left(X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle\right)$

—[Y]— $\rightarrow Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\left(Y|0\rangle = i|1\rangle,\ Y|1\rangle = -i|0\rangle\right)$

$X^\dagger = X$,
$X^\dagger X = X^2 = \mathbb{1}$

—[Z]— $\rightarrow Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\left(Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle\right)$

- Hadamard gate: —[H]— $\rightarrow H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H^\dagger = H \rightarrow H^2 = \mathbb{1}$.

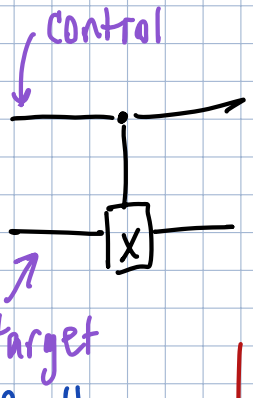
$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

- Phase gate: —[S]— $\rightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rightarrow S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$

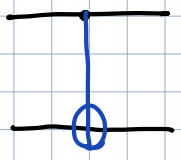
- T-gate: —[T]— $\rightarrow T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$e^{i\pi/4} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)$
$= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$

- CNOT / CX gate :



or



"controlled-X"

$$CNOT = \begin{array}{c|cc|cc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 0 \\ \hline 10 & 0 & 0 & 0 & 1 \\ 11 & 0 & 0 & 1 & 0 \end{array}$$

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

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

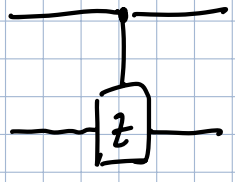
$|1\rangle|0\rangle \mapsto |1\rangle X|0\rangle = |1\rangle|1\rangle$

$|1\rangle|1\rangle \mapsto |1\rangle X|1\rangle = |1\rangle|0\rangle$

Bc of linearity, this determines the action on any state!

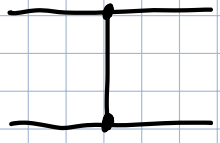
$|\psi\rangle = a|0,0\rangle + b|0,1\rangle + c|1,0\rangle + d|1,1\rangle \mapsto a|0,0\rangle + b|0,1\rangle + c|1,1\rangle + d|1,0\rangle$

- Controlled-Z / CZ gate :



$$CZ = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & & & \\ 01 & & 1 & & \\ 10 & & & 1 & \\ 11 & & & & -1 \end{array}$$

OR



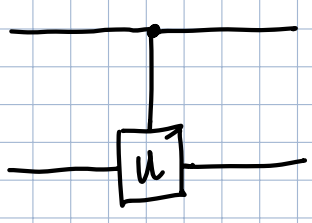
$|0\rangle|0\rangle \mapsto |0\rangle|0\rangle$

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

$|1\rangle|0\rangle \mapsto |1\rangle Z|0\rangle = |1\rangle|0\rangle$

$|1\rangle|1\rangle \mapsto |1\rangle Z|1\rangle = -|1\rangle|1\rangle$

- Controlled Unitary



$$cU = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & U \end{pmatrix}$$

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

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

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

$|1\rangle|1\rangle \mapsto |1\rangle U|1\rangle$

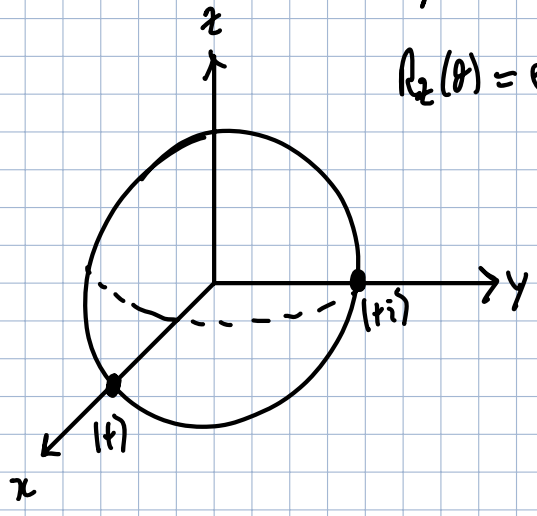
$$\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & U & \\ 0 & 0 & & \end{array}\right)$$

2x2 unitary

- **Rotation Gates:** $R_X(\theta) = e^{-i\frac{\theta}{2}X}$ → rotation around X-axis by angle θ.

$R_Y(\theta) = e^{-i\frac{\theta}{2}Y}$ → rotation around Y-axis by angle θ.

$R_Z(\theta) = e^{-i\frac{\theta}{2}Z}$ → rotation around Z-axis by angle θ.



$e^M := \sum_{k=0}^{\infty} \frac{1}{k!} M^k$ (matrix exponential)

$$\Rightarrow e^{-i\frac{\theta}{2}X} = \sum_{k=0}^{\infty} \frac{1}{k!}\left(-i\frac{\theta}{2}X\right)^k$$

$X^3 = X^2 \cdot X = X$

$X^4 = X^2 \cdot X^2 = \mathbb{1}$

$X^2 = \mathbb{1}$

$\Rightarrow X^k = \mathbb{1}$, k even

$X^k = X$, k odd

$$= \sum_{k=0}^{\infty} \frac{1}{(2k)!}\left(-i\frac{\theta}{2}X\right)^{2k} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!}\left(-i\frac{\theta}{2}X\right)^{2k+1}$$

$0, 2, 4, 6, \ldots$ $\quad$ $1, 3, 5, 7, \ldots$

$$= \sum_{k=0}^{\infty} \frac{1}{(2k)!}\left(\frac{\theta}{2}\right)^{2k}(-i)^{2k}\mathbb{1} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!}\left(\frac{\theta}{2}\right)^{2k+1}(-i)^{2k+1}X$$

$i \cdot i = i^2 = -1$

$(-i)^1 = -i \quad (k=0)$

$(-i)^3 = \underbrace{-i \cdot -i}_{-1} \cdot -i = i \quad (k=1)$

$(-i)^5 = -i \quad (k=2)$

$\vdots$

$(-i)^{2k+1} = -i(-1)^k$

$(-i)^2 = -i \cdot -i = -1 \quad (k=1)$

$(-i)^4 = ((-i)^2)^2 = 1 \quad (k=2)$

$(-i)^6 = -1 \quad (k=3)$

$\vdots$

$(-i)^{2k} = (-1)^k$

$$= \underbrace{\sum_{k=0}^{\infty} \frac{1}{(2k)!} \left(\frac{\theta}{2}\right)^{2k} (-1)^k}_{\cos\left(\frac{\theta}{2}\right)} \mathbb{1} - i \underbrace{\sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \left(\frac{\theta}{2}\right)^{2k+1} (-1)^k}_{\sin\left(\frac{\theta}{2}\right)} X$$

$$= \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)X$$

✱ Similar argument to show $R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)Y$

$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)Z$

- **Important properties of Unitaries.**

  - **Unitaries preserve norm**: For $U \in L(\mathbb{C}^d)$ unitary, $|v\rangle \in \mathbb{C}^d$ arbitrary,

$$|\tilde{v}\rangle = U|v\rangle \rightarrow \| |\tilde{v}\rangle \|^2 = \langle \tilde{v}|\tilde{v}\rangle = \langle v| \underbrace{U^\dagger U}_{=\mathbb{1}} |v\rangle = \langle v|v\rangle$$

$$\langle \tilde{v}| = (|\tilde{v}\rangle)^\dagger = (U|v\rangle)^\dagger = \langle v|U^\dagger$$

$$\left((M_1 M_2)^\dagger = M_2^\dagger M_1^\dagger \right)$$

  - **Unitaries preserve states**: let ρ be a density operator representing a mixed quantum state. Then the transformed state is given by

$\tilde{\rho} = U\rho U^\dagger \rightarrow$ This is still a density matrix!

Check: (1) $\tilde{\rho}^\dagger = (\underbrace{U\rho U^\dagger}_{\tilde{\rho}})^\dagger = (U^\dagger)^\dagger \rho^\dagger U^\dagger = U\rho U^\dagger$ ✓

($U^\dagger = U$, $\rho^\dagger = \rho$, $U\rho U^\dagger = \tilde{\rho}$)

$$\left((M_1 M_2 M_3)^\dagger = M_3^\dagger M_2^\dagger M_1^\dagger \right)$$

(2) $\mathrm{Tr}[\tilde{\rho}] = \mathrm{Tr}[U\rho U^\dagger] = \mathrm{Tr}[U^\dagger U \rho] = \mathrm{Tr}[\rho] = 1$ ✓

✱ **Cyclicity of trace**: $\mathrm{Tr}[M_1 M_2 M_3] = \mathrm{Tr}[M_2 M_3 M_1] = \mathrm{Tr}[M_3 M_2 M_1]$

(3) For arbitrary $|v\rangle \in \mathbb{C}^d$, $\langle v|\vec{\rho}|v\rangle = \underbrace{\langle v|u}_{\langle \tilde{v}|}\, \rho\, \underbrace{u^\dagger|v\rangle}_{|\tilde{v}\rangle}$

$= \langle \tilde{v}|\rho|\tilde{v}\rangle \geq 0$ b/c $\rho \geq 0$ by assumption.

$\Rightarrow$ So $\vec{\rho} \geq 0$ ✓

- Product of unitaries is a unitary: if u_1, u_2 are unitaries, then $u = u_1 u_2$ is also a unitary.

Check: $u^\dagger u = (u_1 u_2)^\dagger u_1 u_2 = u_2^\dagger \underbrace{u_1^\dagger u_1}_{=\mathbb{1}} u_2 = u_2^\dagger u_2 = \mathbb{1}$ ✓

$uu^\dagger = (u_1 u_2)(u_1 u_2)^\dagger = u_1 \underbrace{u_2 u_2^\dagger}_{=\mathbb{1}} u_1^\dagger = u_1 u_1^\dagger = \mathbb{1}$ ✓.