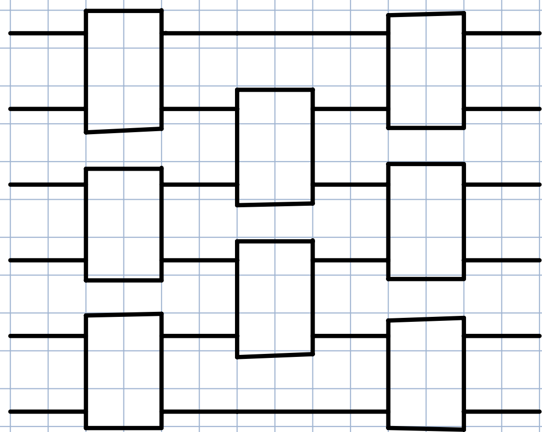
① Universal Gate Sets

- We want to use a set of elementary gates to execute arbitrary unitaries on n qubits.



Relevant when we want the set to be finite.

- Two versions: • Exact • Approximate. $\rightarrow$ we can allow for some error / deviatio in the implementation.

Requires (uncountably) infinite # of gates in the set.

(a) Exact case: CNOT + all single-qubit gates are universal! (✱ This set is not finite.)

Lemma 4.1. Every unitary 2×2 matrix can be expressed as

$$\begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix}\begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix}\begin{pmatrix} \cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & \cos\theta/2 \end{pmatrix} \times \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix},$$

where δ, α, θ, and β are real valued. Moreover, any special unitary 2×2 matrix (i.e., with unity determinant) can be expressed as

$$\begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix}\begin{pmatrix} \cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & \cos\theta/2 \end{pmatrix}\begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix}.$$

✱ Recall the rotation gates!

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

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

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

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

Observe: $R_y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & 0 \\ 0 & \cos(\frac{\theta}{2}) \end{pmatrix} - i\begin{pmatrix} 0 & -i\sin(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2}) & 0 \end{pmatrix} = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$

$$R_z(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & 0 \\ 0 & \cos(\frac{\theta}{2}) \end{pmatrix} - i \begin{pmatrix} \sin(\frac{\theta}{2}) & 0 \\ 0 & -\sin(\frac{\theta}{2}) \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\frac{\theta}{2}) - i\sin(\frac{\theta}{2}) & 0 \\ 0 & \cos(\frac{\theta}{2}) + i\sin(\frac{\theta}{2}) \end{pmatrix}$$

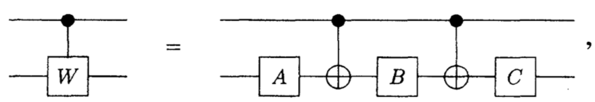
$e^{i\varphi} = \cos(\varphi) + i\sin(\varphi)$

$$= \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

(*) So every single-qubit gate can be decomposed into rotation gates:

$U = R_z(\alpha) R_y(\theta) R_z(\beta)$, for appropriate angles α, β, θ.

Lemma 5.1. For a unitary 2×2 matrix W, a $\wedge_1(W)$ gate can be simulated by a network of the form



where A, B, and $C \in SU(2)$ if and only if $W \in SU(2)$.

(b) Approximate case: Arises when the # of gates in the set is finite

(B/c the set of unitaries is uncountably infinite, while the set of sequences of gates from a finite set will be countably infinite.)

(*) **Theorem:** Clifford gates + one single-qubit non-Clifford gate is universal!

↳ T gate! $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

- Recall Pauli operators on n qubits: $\mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n}$ ↪ $P = I \otimes X \otimes Y \otimes X \otimes Z$

  ↳ 4^n

  → Let $\mathcal{P}_n^* = \mathcal{P}_n \setminus \{I^{\otimes n}\}$ → exclude the identity gate.

- Define the n-qubit Clifford group as

mod out global phase

$$\mathcal{C}_n := \{ U : P \in \pm i\mathcal{P}_n^* \Rightarrow UPU^\dagger \in \pm i\mathcal{P}_n^* \} / U(1)$$

→ Transforms Paulis to Paulis (up to sign)

$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \to HXH = Z,\ HZH = X$

⊛ **Theorem:** $\mathcal{C}_n = \langle H_i, S_i, CNOT_{i,j} : i,j \in \{1,2,\dots,n\} \rangle / U(1)$

⊛ H, S, CNOT are generators of the Clifford group!

⊛ (Take all possible products of H, S, CNOT, and ignore global phase.)

⊛ **Corollary:** $\{H, S, CNOT, T\}$ is universal → $\{H, CNOT, T\}$ is universal. $(S = T^2)$.

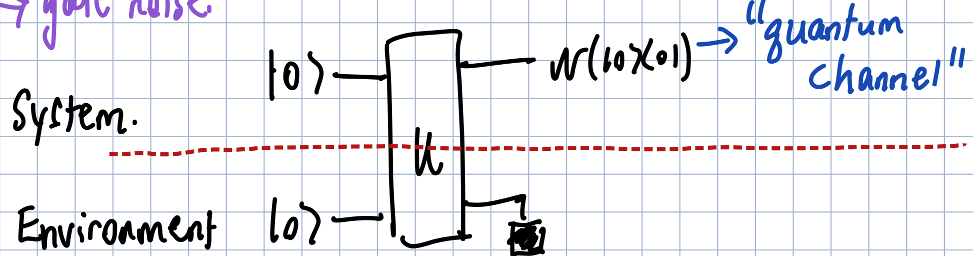
② Noise and Errors in Quantum Computing

⊛ In quantum computing we care about precise control of qubits — but they they inevitably interact with their environment! This evolution is unitary.

(ideal case). $|0\rangle - \boxed{G} - G|0\rangle$

Unitary gate.

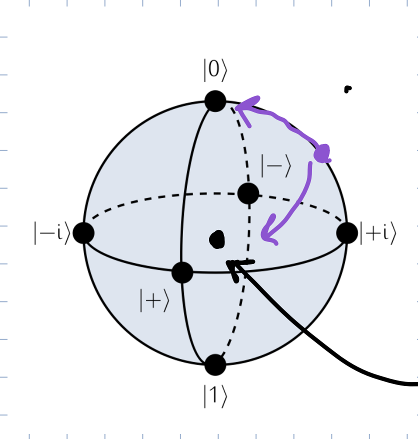
(reality) → gate noise.



(reality) → decoherence

↓

Qubit state drifts over time.



Origin: maximally-mixed state $\frac{\mathbb{1}}{2}$.

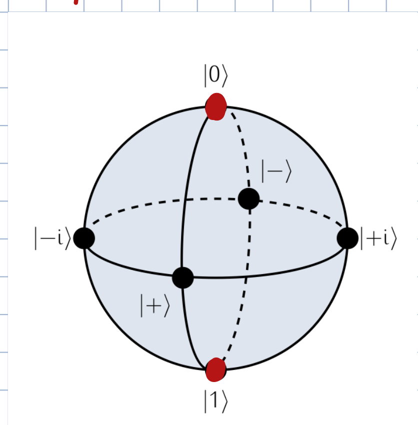
(a) Any unwanted gate applied to the qubit can be thought of as noise.

Example: Bit flip → Pauli-X gate, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ → opposite ends of the Bloch sphere!

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$

→ measurement probabilities get flipped!



Example: Rotations → $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$

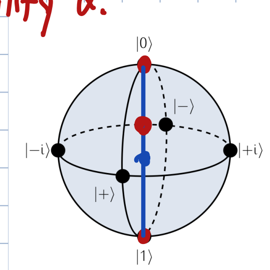
✱ Recall teleportation! The state before Bob's correction is precisely a noisy version of the true state Alice wants to send.

(b) Different gates can also be applied randomly to the state

- Example: Apply X with probability α, do nothing with probability $1-\alpha$.

If the qubit state is given by a density operator ρ, then after the noise it is

$$\underbrace{(1-\alpha)\rho}_{\text{Do nothing with probability } 1-\alpha} + \underbrace{\alpha X\rho X}_{\text{Apply the } X \text{ gate with probability } \alpha.} \longrightarrow \text{"Bit-flip channel"}$$



$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \mapsto (1-\alpha)\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \alpha \underbrace{X\overbrace{|0\rangle\langle 0|}^{\rho}X}_{=|1\rangle\langle 1|} = \begin{pmatrix} 1-\alpha & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix}$$

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

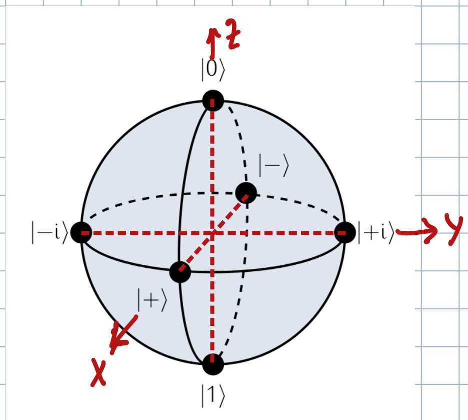
$$= (1-\alpha)|0\rangle\langle 0| + \alpha |1\rangle\langle 1|.$$

* If we measured the initial (noiseless) state, then we would get the outcome "0" with probability $1 \to$ after noise, the state becomes mixed: with probability $1-\alpha$ we get "0" and with probability α we get "1".

* So α quantifies the amount of noise! $\to \alpha = 0 \Rightarrow$ no noise
  $\alpha = \frac{1}{2} \Rightarrow \boxed{\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|}$

* For a general density matrix: recall the form $\rho = \frac{1}{2}(\mathbb{1} + r_x X + r_y Y + r_z Z)$

Coordinates in the Bloch sphere.



How do those coordinates transform after the noise?

$(r_x, r_y, r_z) \mapsto (r_x', r_y', r_z')$?

$$(1-\alpha)\rho + \alpha X\rho X = (1-\alpha)\underbrace{\tfrac{1}{2}(\mathbb{1}+r_xX+r_yY+r_zZ)}_{\rho} + \alpha \underbrace{X\overbrace{\tfrac{1}{2}(\mathbb{1}+r_xX+r_yY+r_zZ)}^{\rho}X}$$

$\underbrace{XY=-YX}$

$XZ=-ZX$

$$=\tfrac{1}{2}\Big(\underbrace{X\mathbb{1}X}_{\substack{=X^2\\=\mathbb{1}}} + r_x\underbrace{XXX}_{\substack{=X^2\cdot X\\=X}} + r_y\underbrace{XYX}_{\substack{=-X^2Y\\=-Y}} + r_z\underbrace{XZX}_{\substack{=-X^2Z\\=-Z}}\Big)$$

$$=(1-\alpha)\tfrac{1}{2}(\mathbb{1}+r_xX+r_yY+r_zZ)+\alpha\tfrac{1}{2}(\mathbb{1}+r_xX-r_yY-r_zZ)$$

$$\begin{aligned}=\tfrac{1}{2}\Big((1-\alpha+\alpha)\mathbb{1} &+ \big((1-\alpha)r_x+\alpha r_x\big)X\\ &+\big((1-\alpha)r_y-\alpha r_y\big)Y\\ &+\big((1-\alpha)r_z-\alpha r_z\big)Z\Big)\end{aligned}$$

$$=\tfrac{1}{2}\big(\mathbb{1}+\underbrace{r_x}_{r_x'=r_x}X+\underbrace{(1-2\alpha)r_y}_{r_y'}Y+\underbrace{(1-2\alpha)r_z}_{r_z'}Z\big).$$

Check: If $\rho=|0\rangle\langle 0|$, then $r_x=0,\ r_y=0,\ r_z=1 \xrightarrow{\alpha=1} r_x'=0,\ r_y'=0,\ r_z'=-1$ ✓

- Example: Phase-flip / dephasing channel

$$\rho\mapsto \underbrace{(1-\alpha)\rho}_{\substack{\text{Do nothing}\\ \text{with probability } 1-\alpha}} + \underbrace{\alpha Z\rho Z}_{\text{Apply Pauli-}Z\text{ with probability }\alpha}.$$

⊛ Now how do the coordinates transform?

$$\rho=\tfrac{1}{2}(\mathbb{1}+r_xX+r_yY+r_zZ)\longmapsto \rho'=\tfrac{1}{2}(\mathbb{1}+r_x'X+r_y'Y+r_z'Z)$$

$$r_x'=(1-2\alpha)r_x,\quad r_y'=(1-2\alpha)r_y,\quad r_z'=r_z.$$

(*) For this channel, it is useful to see the transformation in the standard basis.

$a \in [0,1]$, $c \in \mathbb{C}$.

$$\rho = \begin{pmatrix} a & c \\ \bar{c} & 1-a \end{pmatrix} \mapsto (1-\alpha)\rho + \alpha Z\rho Z = (1-\alpha)\begin{pmatrix} a & c \\ \bar{c} & 1-a \end{pmatrix} + \alpha \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & c \\ \bar{c} & 1-a \end{pmatrix}}_{= \begin{pmatrix} a & c \\ -\bar{c} & -(1-a) \end{pmatrix}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$= (1-\alpha)\begin{pmatrix} a & c \\ \bar{c} & 1-a \end{pmatrix} + \alpha \underbrace{\begin{pmatrix} a & c \\ -\bar{c} & -(1-a) \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{= \begin{pmatrix} a & -c \\ -\bar{c} & 1-a \end{pmatrix}}$$

$\alpha = 0 \Rightarrow$ no noise

$\alpha = \frac{1}{2} \Rightarrow$ max. noise

$$= (1-\alpha)\begin{pmatrix} a & c \\ \bar{c} & 1-a \end{pmatrix} + \alpha \begin{pmatrix} a & -c \\ -\bar{c} & 1-a \end{pmatrix} = \begin{pmatrix} a & \underline{(1-2\alpha)c} \\ \underline{(1-2\alpha)\bar{c}} & 1-a \end{pmatrix}$$

(*) Off-diagonal terms are suppressed!

(*) For $\alpha = \frac{1}{2}$, the off-diagonal terms vanish! $\rightarrow$ superposition is gone!

- <u>Example</u>: Depolarizing channel : $\rho \mapsto (1-\alpha)\rho + \frac{\alpha}{3}X\rho X + \frac{\alpha}{3}Y\rho Y + \frac{\alpha}{3}Z\rho Z$

(With prob. $1-\alpha$, do nothing; with prob. α, apply a Pauli operator uniformly at random.)

(*) For $\alpha = 3/4$: $\frac{1}{4}\rho + \frac{1}{4}X\rho X + \frac{1}{4}Y\rho Y + \frac{1}{4}Z\rho Z = \underbrace{\mathrm{Tr}[\rho]}_{=1}\frac{\mathbb{1}}{2}$ (Assignment!)

(*) Using this, we can write the depolarizing channel in an alternative way:

$$\frac{1}{4}\rho + \frac{1}{4}X\rho X + \frac{1}{4}Y\rho Y + \frac{1}{4}Z\rho Z = \mathrm{Tr}[\rho]\frac{\mathbb{1}}{2} \Rightarrow X\rho X + Y\rho Y + Z\rho Z = 4\mathrm{Tr}[\rho]\frac{\mathbb{1}}{2} - \rho$$

$$\Rightarrow \rho \mapsto (1-\alpha)\rho + \frac{\alpha}{3}\left(4\mathrm{Tr}[\rho]\frac{\mathbb{1}}{2} - \rho\right)$$

$$= (1-\alpha)\rho + \frac{4\alpha}{3}\mathrm{Tr}[\rho]\frac{\mathbb{1}}{2} - \frac{\alpha}{3}\rho$$

$$= \left(1-\alpha-\frac{\alpha}{3}\right)\rho + \frac{4\alpha}{3}\mathrm{Tr}[\rho]\frac{\mathbb{1}}{2}$$

$$= \underbrace{\left(1-\frac{4\alpha}{3}\right)}\underbrace{\rho}_{\substack{\text{"all"}\\ \text{(state perfectly intact)}}} + \frac{4\alpha}{3}\underbrace{\mathrm{Tr}[\rho]\frac{\mathbb{1}}{2}}_{\substack{\text{"nothing"}\\ \text{(all information about state is lost)}}}. \quad (\text{"all or nothing"}).$$

$$\beta = 1-\frac{4\alpha}{3}, \quad \rho \mapsto \beta\cdot\rho + (1-\beta)\frac{\mathbb{1}}{2}$$