Portland State University

05/22/2020

S'20 CS410/510
Intro to quantum computing

Fang Song

Week 8

- Mixed states, density matrices
- General quantum operations
- POVM

Credit: based on slides by Richard Cleve

Exercise

1. Let I be identity on n qubits. Show that $I = \sum_{x \in \{0,1\}^n} |x\rangle\langle x|$.

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

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

x^{th}

$|x\rangle\langle x| = \begin{pmatrix} \ddots & & 0 \\ & 1 & \\ 0 & & \ddots \end{pmatrix} \sim x^{th}$

2. Let $|A\rangle, |B\rangle$ be as defined below. Show that $I = a|A\rangle\langle A| + b|B\rangle\langle B|$

- $A \subseteq \{0,1\}^n, B = \{0,1\}^n \backslash A$
- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, |B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$

$a = |A|$

$a|A\rangle\langle A| = \left(\frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle\right)\left(\frac{1}{\sqrt{a}} \sum_{x'} \langle x'|\right)$

$= \frac{1}{a} \sum_{\substack{x \in A \\ x' \in A}} |x\rangle\langle x'|$

$+$ $\qquad +$

$b|B\rangle\langle B| = \frac{1}{b} \sum_{\substack{x \in B \\ x' \in B'}} |x\rangle\langle x|$

Exercise

3. Let Z_f be as below. Show that $Z_f = I - 2|A\rangle\langle A|$. What is $Z_f|A\rangle$? $|B\rangle$

- $Z_f : |x\rangle \mapsto \begin{cases} -|x\rangle, & x \in A \\ |x\rangle, & x \notin A \end{cases}$

$$Z_f|A\rangle = (I - 2|A\rangle\langle A|)|A\rangle$$

$$|B\rangle = |A\rangle - 2|A\rangle\underbrace{\langle A|A\rangle}_{=1} \qquad \langle A|B\rangle = 0$$

$$= -|A\rangle$$

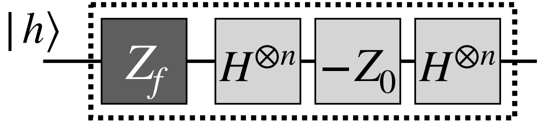
4. Let Z_0 be as below. Show that $Z_0 = I - 2|0^n\rangle\langle 0^n|$.

- $Z_0 : |x\rangle \mapsto \begin{cases} -|x\rangle, & x = 0^n \\ |x\rangle, & x \neq 0^n \end{cases}$

5. What is $H^{\otimes n} Z_0 H^{\otimes n}$?

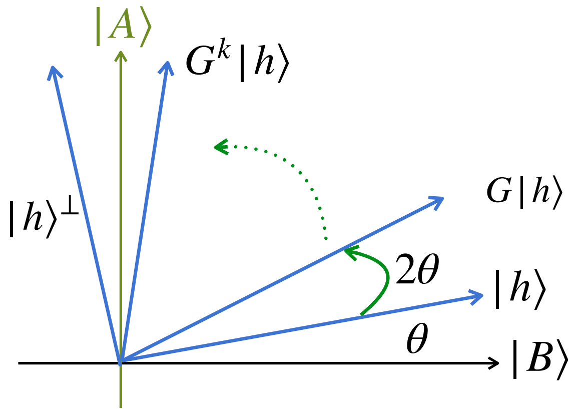
Review: Grover's algorithm

Grover Iteration G



- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$, $|B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle$
- $|h\rangle^{\perp}$: orthogonal to $|h\rangle$ on span$\{|A\rangle, |B\rangle\}$

- $Z_f = I - 2|A\rangle\langle A|$: reflection about $|B\rangle$
- $-HZ_0H = 2|h\rangle\langle h| - I$: reflection about $|h\rangle$
- $G = (-HZ_0H)Z_f$: rotation by 2θ



Quantum algorithms so far

	Problem	Deterministic	Randomized	Quantum	
	Deutsch	2	2	1	oracle model
Partial function	Deutsch-Josza	$2^n/2$	$O(n)$	1	
	Simon	$2^n/2$	$\sqrt{2^n}$	$O(n^2)$	
	Order-finding Factoring N (Kitaev/Shor)	$2^{O((\log N)^{1/3}(\log\log N)^{2/3})}$		$(\log N)^3$	
Total function	Unstructured search (Grover)	$\Omega(2^n)$		$\Theta(\sqrt{2^n})$	oracle model

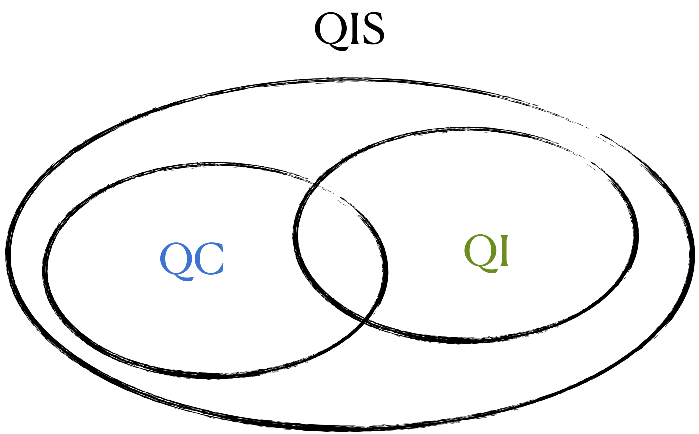
Quantum information theory

An coarse taxonomy

Quantum information science (QIS)

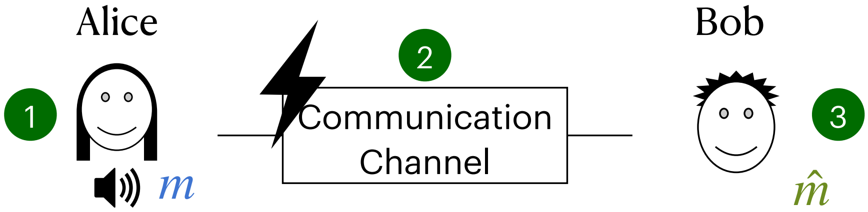
- Quantum computing (QC): making information useful
  - Algorithms, software, ...

- Quantum information (QI): making information available
  - Elementary tasks: create, store, transmit, ...



Basic communication scenario

Goal: convey information from Alice to Bob



1. Alice: information source
2. Communication channel (resource): can you get everything I say in class?
3. Bob: because of noise, get disturbed $\hat{m}$

Central questions

0. What is information, mathematically?

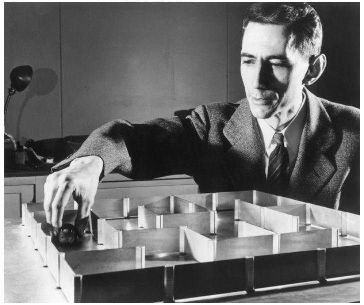
- Defining bit as unit of information

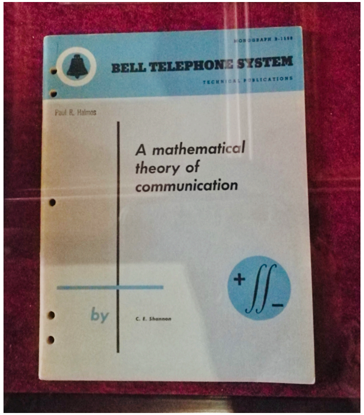
1. Assuming noiseless channel, how many bits needed to transmit m?

- Shannon noiseless/source coding theorem: entropy

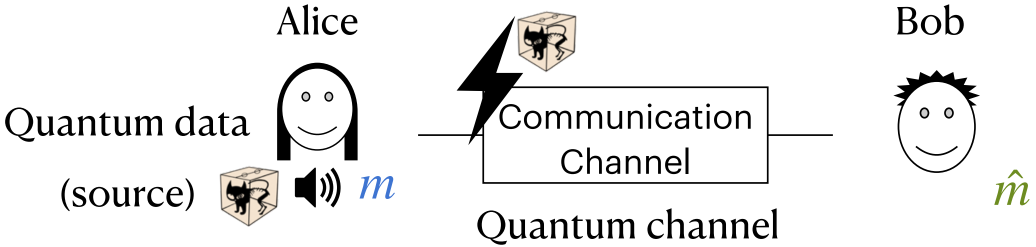
2. Assuming noisy channel, how many bits can be transmitted reliably?

- Shannon noisy-channel coding theorem: channel capacity
- Tool: error correcting code





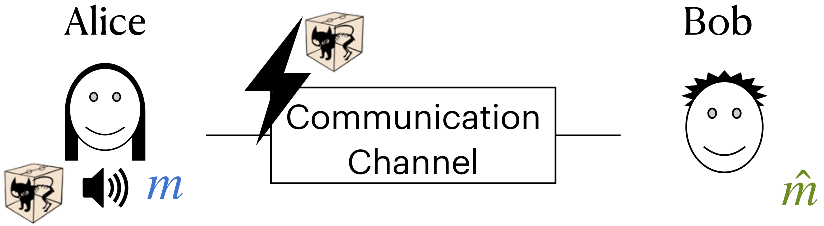
The new quantum player



Channel / Source	C	Q
Classical	1. Shannon 2. theory	1. Holevo's bound: # info. in qstates? 2. Capacity to transmit C data
Quantum	*teleportation	1. Schumacher's Thm: compress Q data 2. Quantum capacity

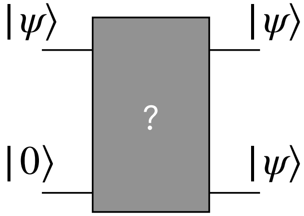
1. Noiseless channel
2. Noisy channel

The new quantum player

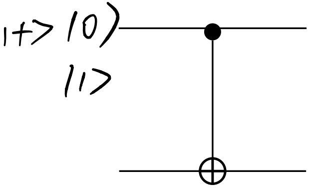


- **New resource: entanglement**
  - Teleportation, super dense coding
  - Violation of Bell's inequality: validating quantum mechanics
- **New challenges (easy for classical information)**
  - copying a quantum state?
  - distinguishing states?

Copy a quantum state?



- **How about CNOT?**

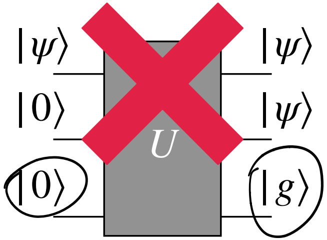


- $|0\rangle|0\rangle \mapsto |0\rangle|0\rangle$
- $|1\rangle|0\rangle \mapsto |1\rangle|1\rangle$
- $|+\rangle|0\rangle \mapsto |0\rangle|0\rangle + |1\rangle|1\rangle \neq |+\rangle|+\rangle$

$(|0\rangle+|1\rangle)|0\rangle = |00\rangle + |10\rangle \xrightarrow{\text{CNOT}} |00\rangle + |11\rangle$

No-cloning theorem

Theorem. There is no valid quantum operation that maps an arbitrary (unknown) state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$.



- **Proof.** (Linearity) Consider two states $|\psi\rangle$ and $|\psi'\rangle$
  - $|\psi\rangle|0\rangle|0\rangle \overset{\mathcal{U}}{\mapsto} |\psi\rangle|\psi\rangle|g\rangle$
  - $|\psi'\rangle|0\rangle|0\rangle \overset{\mathcal{U}}{\mapsto} |\psi'\rangle|\psi'\rangle|g'\rangle$

U preserves inner product

LHS $\overbrace{\langle 0|\langle 0|\underbrace{\langle\psi|\psi'\rangle}\,|0\rangle|0\rangle}^{1}$ $\qquad \langle g|\langle\psi|\underbrace{\langle\psi|\psi'\rangle}|\psi'\rangle|g'\rangle$ RHS

$\boxed{\langle\psi|\psi'\rangle}$ $=$ $\boxed{\langle\psi|\psi'\rangle\langle\psi|\psi'\rangle\langle g|g'\rangle}$

$\underbrace{\langle\psi|\psi'\rangle}\underbrace{(1-\langle\psi|\psi'\rangle\langle g|g'\rangle)}_{\neq 0} = 0$

$1 = \langle\psi|\psi'\rangle\overbrace{\langle g|g'\rangle}^{1}$

Two possibilities:
$\langle\psi|\psi'\rangle = 0$ or 1

Density matrix formalism

Another continent language

State vector formalism

- State: $|\psi\rangle \in \mathbb{C}^d$
- Unitary operation $U : |\psi\rangle \mapsto U|\psi\rangle$
- Measuring in computational basis
  - $\sum_x \alpha_x |x\rangle$: "$x$" w.p. $|\alpha_x|^2$, p.s. $|x\rangle$

Density matrix formalism

- State: $\rho = |\psi\rangle\langle\psi|$ (density matrix)
  - Ex. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $|\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}$
- Unitary $U : \rho \mapsto U\rho U^\dagger$

$|\psi\rangle \xrightarrow{U} U|\psi\rangle$, $\quad (U\underbrace{|\psi\rangle)(\langle\psi|}_{\rho}U^\dagger) = U\rho U^\dagger$

- Measuring in computational basis
  - $\rho = \sum_{x,x'} \alpha_x \alpha_{x'}^* |x\rangle\langle x'|$: "$x$" w.p. $\langle x|\rho|x\rangle$, p.s. $|x\rangle\langle x|$

Exercise

1. Analyze the circuit below under both formalisms.

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ —[X]—

$\downarrow X$

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

$\downarrow \mathcal{M}$

0 w.p. $|\beta|^2$ $|0\rangle$

1 w.p. $|\alpha|^2$ $|1\rangle$

$\rho = |\alpha|^2 |0\rangle\langle 0| + \alpha\beta^* |0\rangle\langle 1| + \alpha^*\beta |1\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$

$\downarrow X$

$X\rho X^\dagger = |\alpha|^2 X(\underbrace{|0\rangle\langle 0|)X^\dagger} + \cdots$

$\rho' = |\alpha|^2 |1\rangle\langle 1| + \cdots + \cdots$

$\mathcal{M}\downarrow$

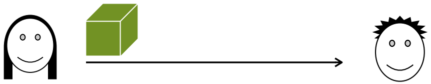
"1" w.p. $\langle 1|\rho'|1\rangle = |\alpha|^2$ $|x\rangle\langle x|$

2. Consider two qubits in state $|+\rangle|-\rangle$. Write down its density matrix.

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

$$\rho = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix} = \begin{pmatrix} & & & \\ & & & \end{pmatrix}_{4\times 4}$$

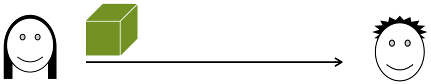
Pure states vs. mixed states



- Alice flips a coin, prepare $|0\rangle$ or $|1\rangle$ accordingly.
- Bob receives the register (Alice's coin unknown). How to describe his state?
  - $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ no compact representation as state vectors
  - Density matrix representation: $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$
- This is called a mixed state. In contrast, $|\psi\rangle$ is called a pure state.

Exercise

1. Alice flips a coin and prepares a qubit as follows. She then sends the qubit (but not the coin) to Bob. How to describe Bob's state?



$\{ (\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle) \}$

HEADS: $| + \rangle$

TAILS: $| - \rangle$

2. Write down the density matrix explicitly and compare with the previous slide.

$\rho = \frac{1}{2} |+\rangle\langle+| + \frac{1}{2} |-\rangle\langle-|$ $\qquad \rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1|$

$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{2\times 2}$ $\qquad \rho^2 = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\qquad = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{2\times 2}$

General mixed states

- Mixed state = a probability distribution (mixture) over pure states
  - $\{(p_i, |\psi_i\rangle) : i = 1,\ldots,k\}$: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
- Properties of density matrices
  - $tr(\rho) = 1$
  - ρ is pure iff. $tr(\rho^2) = 1$ (Think of examples in previous slides)

$tr[(|0\rangle\langle 0|)^2] = tr[|0\rangle\langle 0|] = 1$; $\rho = |\psi\rangle\langle\psi|$; $\rho^2 = (|\psi\rangle\langle\psi|)(|\psi\rangle\langle\psi|)$ $\underbrace{\langle\psi|\psi\rangle}_{=1}$ $= \rho$

  - ρ is positive semi-definite, i.e., $\langle\psi|\rho|\psi\rangle \geq 0$.

Operations on mixed states

- **Unitary** $U : \rho \mapsto U\rho U^\dagger$

$\{(p_i, |\psi_i\rangle)\}$ $\quad \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$\xmapsto{U}$

$U|\psi_i\rangle\langle\psi_i|U^\dagger$

$= \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger$

$= U\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)U^\dagger$

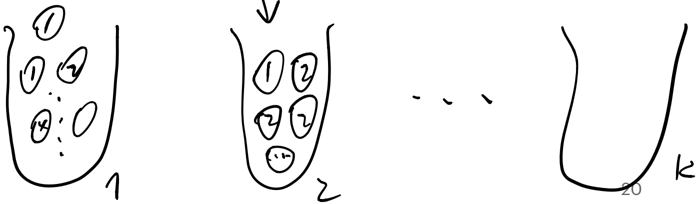
$= U \rho U^\dagger$

- **Measurement: "x" with prob.** $\langle x|\rho|x\rangle$

$\forall i$:

$|\psi_i\rangle\langle\psi_i|$: "x" $\quad \langle x|\,|\psi_i\rangle\langle\psi_i|\,|x\rangle$

ith bin: x. p_x^i $\longrightarrow$ Question:



if pick ith bin w.p. p_i

& pick x from ith bin p_x^i

then $\Pr[x] = \sum_i p_i \Pr[x \mid i]$

$\Pr[\text{meas. } x] = \sum_i p_i \langle x|\,|\psi_i\rangle\langle\psi_i|\,|x\rangle$

$= \langle x|\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)|x\rangle$

General quantum operations

$$\rho \;—\!\!—\boxed{\Phi}—\!\!—\; \rho'$$

Let $A_1, A_2, \ldots, A_m$ be matrices satisfying $\sum_{j=1}^{m} A_j^\dagger A_j = I$.

Then the mapping $\rho \mapsto \sum_{j=1}^{m} A_j \rho A_j^\dagger$ is a general quantum operator.

- N.B. A_i need NOT be square matrices
- Also known as quantum channels
  - admissible operations, completely positive trace preserving maps

Examples of quantum channels

1. **Unitary** $U^\dagger U = I$: $\rho \mapsto U\rho U^\dagger$

2. **Decoherence channel** $A_0 = |0\rangle\langle 0|$, $A_1 = |1\rangle\langle 1|$

- Check validity:

$$A_0^\dagger A_0 + A_1^\dagger A_1 = \mathbb{1}$$

$$(|0\rangle\langle 0|)(|0\rangle\langle 0|) + (|1\rangle\langle 1|)(|1\rangle\langle 1|) = \mathbb{1}$$

- Apply to $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\rho \xrightarrow{\Phi} \sum_i A_i \rho A_i^\dagger$$

$$A_0\left(|\beta|^2 |1\rangle\langle 1|\right) A_0^\dagger \qquad |0\rangle\langle 0| \qquad |0\rangle\langle 0|$$

$$\rho = \begin{pmatrix} |\alpha|^2 & \cancel{\alpha\beta^*} \\ \cancel{\alpha^*\beta} & |\beta|^2 \end{pmatrix} = |\alpha|^2|0\rangle\langle 0| + \alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$$

- Compare to measurement:

$$A_0\rho A_0^\dagger = |\alpha|^2|0\rangle\langle 0|$$

$$+ \qquad \Phi(|\psi\rangle\langle\psi|) = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$$

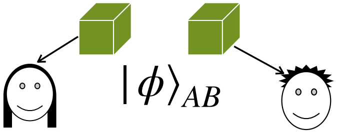
$$A_1\rho A_1^\dagger = |\beta|^2|1\rangle\langle 1|$$

Examples of quantum channels

3. Partial trace $A_0 = I \otimes \langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, A_1 = I \otimes \langle 1| = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

- Check validity:
- Apply to $|0\rangle\langle 0| \otimes |+\rangle\langle +|$
- Apply to $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Exercise



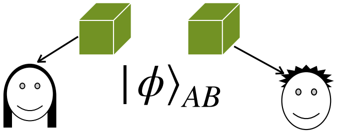
1. let Tr_B denote partial trace of subsystem B. Suppose Alice and Bob shares two qubits in state $|\phi\rangle_{AB}$.

- Apply Tr_B to $|\phi\rangle_{AB} = \dfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

- Apply Tr_B to $|\phi\rangle_{AB} = \dfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

- Is Alice able to tell the two cases on her side?

Exercise



2. let Tr_B denote partial trace of subsystem B. Suppose Alice and Bob shares two qubits in state $|\phi\rangle_{AB}$.

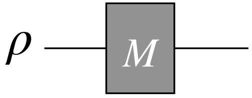
- Apply Tr_B to $|\phi\rangle_{AB} = \frac{3}{5}|00\rangle + \frac{4}{5}|11\rangle$

- Apply Tr_B to $|\phi\rangle_{AB} = \frac{4}{5}|00\rangle - \frac{3}{5}|11\rangle$

- Is Alice able to tell the two cases on her side?

General measurement

- A measurement is described by a collection of matrices $M = \{M_a : a \in \Gamma\}$ with possible outcomes Γ satisfying $\sum_{a\in\Gamma} M_a^\dagger M_a = I$.



outcome	probability	posterior state
a	$Tr(M_a \rho M_a^\dagger)$	$\dfrac{M_a \rho M_a^\dagger}{Tr(M_a \rho M_a^\dagger)}$

- Example. $M_0 = |0\rangle\langle 0| \otimes I, M_1 = |1\rangle\langle 1| \otimes I, \Gamma = \{0,1\}$.
  - Measure $|\psi\rangle = |+\rangle|0\rangle$

outcome	probability	posterior state
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$|\psi\rangle\langle\psi| = |+\rangle\langle+| \otimes |0\rangle\langle 0|$

$M_0 (|+\rangle\langle+| \otimes |0\rangle\langle 0|) M_0^\dagger$

$= (|0\rangle\langle 0| + \rangle\langle + |0\rangle\langle 0|) \otimes |0\rangle\langle 0| = \frac{1}{2} |0\rangle\langle 0| \otimes |0\rangle\langle 0| = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \; 0 \; 0 \end{pmatrix}$

Projective measurement & POVM

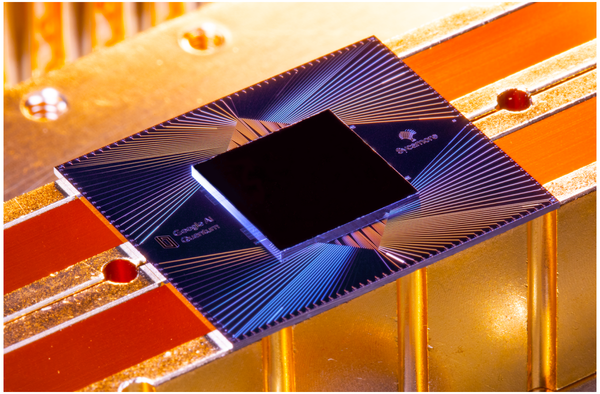
- **Projective (von Neumann) measurement: M_a projections ($M_a^2 = M_a$).**
  - Complete projective measurement $M_a = |\psi_a\rangle\langle\psi_a|$ and $\{|\psi_a\rangle\}$ an orthonormal basis
  - $\equiv$ measurement under basis $\{|\psi_a\rangle\}$
- **Positive-operator-valued measurement (POVM) measurement**
  - $\Pr[a] = Tr(M_a \rho M_a^\dagger) = Tr((\underbrace{M_a^\dagger M_a}_{E_a})\rho)$ $\quad Tr(AB) = Tr(BA)$
  - Suffice to specify POVM elements $\{E_a = M_a^\dagger M_a : a \in \Gamma\}$

Logistics

- **HW6 due next Sunday**

- **Project**
  - Week10 office hour: slots available
  - Presentations
    - Pre-record your talk by zoom, powerpoint, ... Keep it 20 - 25 mins
    - Live Q&A in class
    - Participate in all talks and fill out peer-evaluation

Discussion on Google's experiment



Scratch