Crash Course in Quantum Computing

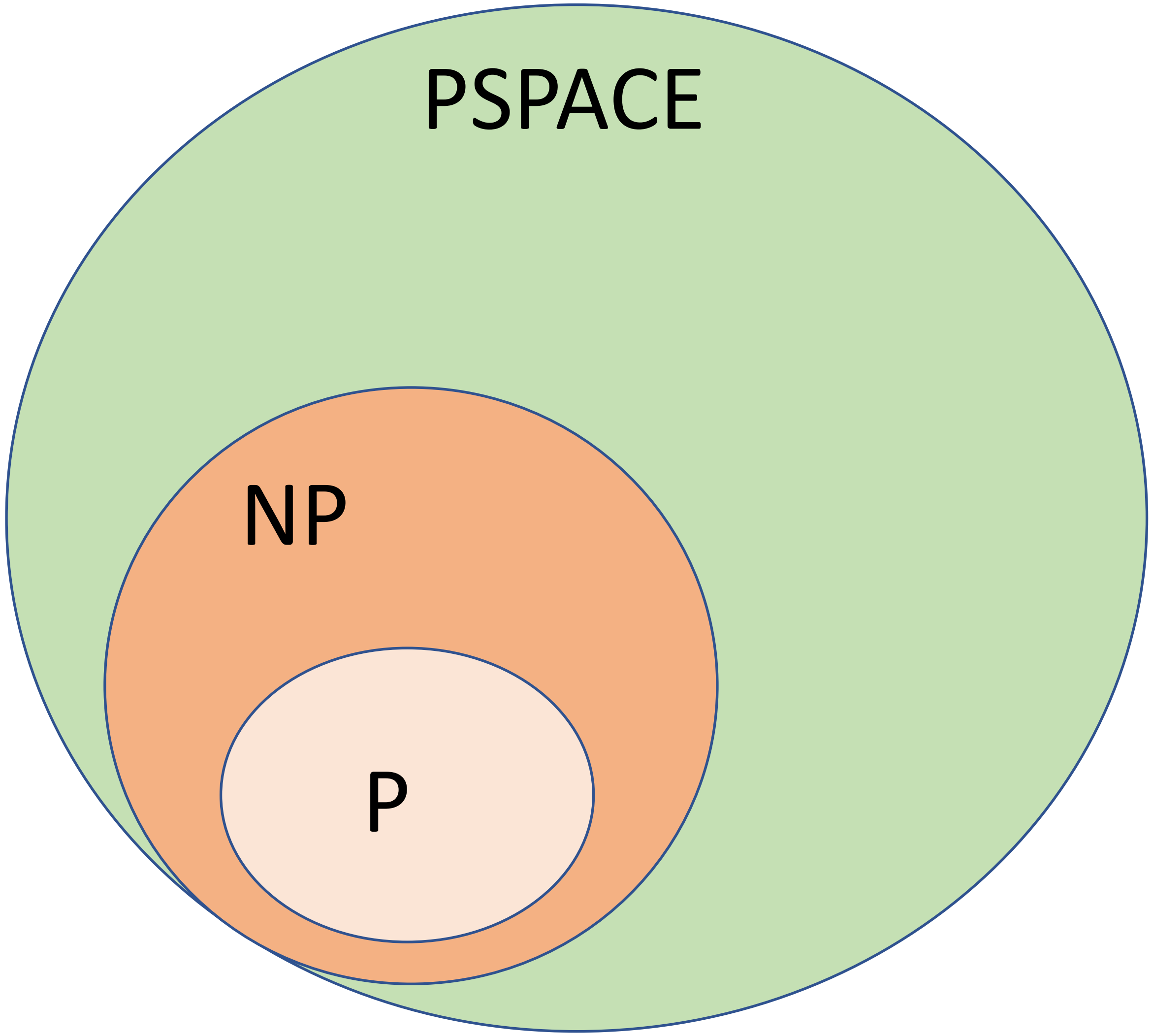
Hour 3: Advanced Quantum Information Theory

BIU Winter School on Cryptography 2021

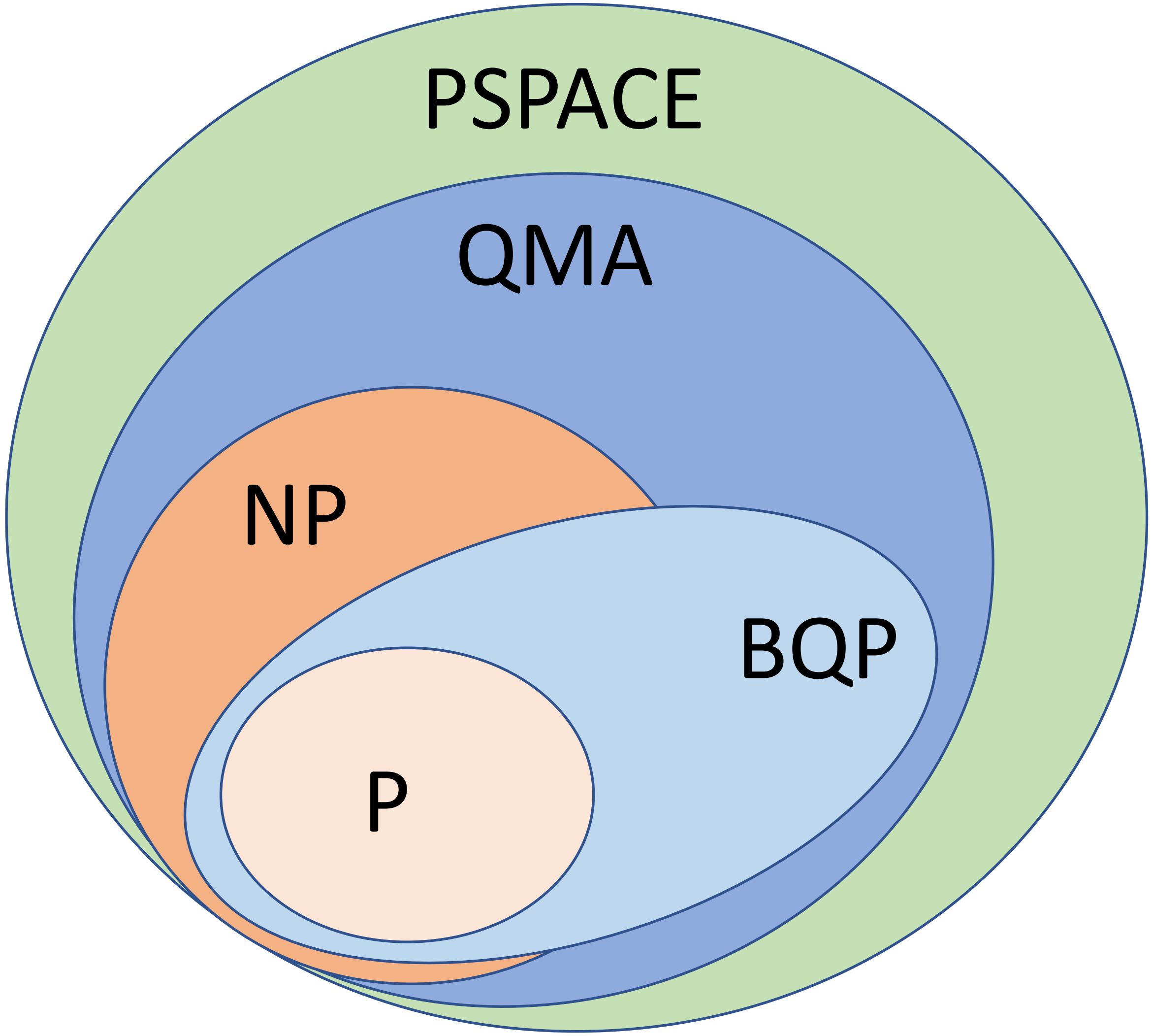
Lecturer: Henry Yuen

Quantum Complexity Theory

The Complexity Zoo



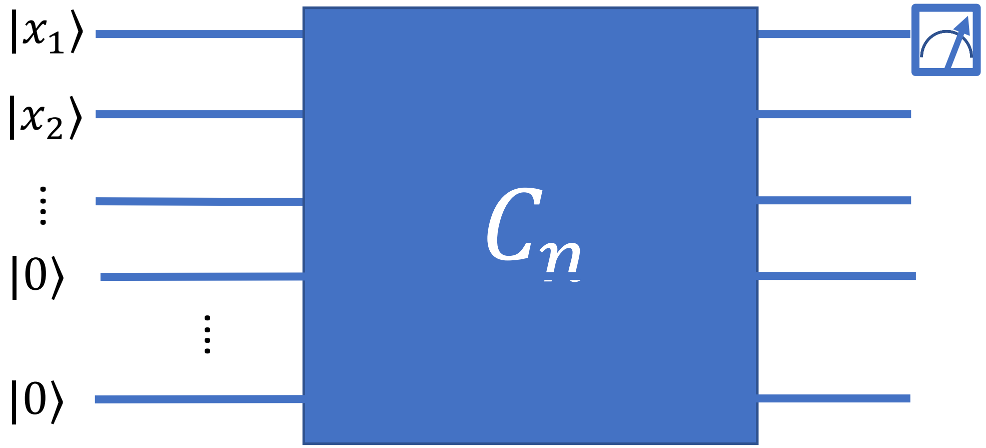
The Complexity Zoo



BQP

Language $L \subseteq \{0,1\}^*$ is in ***Bounded-Error Quantum Polynomial Time*** (***BQP***) if there exist a family of circuits $\{C_1, C_2, \ldots\}$ that are uniformly generated and satisfy:

- $|C_n| \leq O(n^c)$
- For all $x \in \{0,1\}^n$
  - If $x \in L \Longrightarrow \Pr[C_n \text{ } accepts \text{ } x] \geq \frac{2}{3}$ (Completeness)
  - If $x \notin L \Longrightarrow \Pr[C_n \text{ } accepts \text{ } x] \leq \frac{1}{3}$ (Soundness)



BQP

Problems in BQP:

- All problems in BPP
- Factoring, Discrete Logarithm
- Simulating quantum systems.

Canonical BQP-complete (promise) problem:

QCIRCUIT: given classical description of quantum circuit C, decide whether C accepts on the all zeroes input with probability at least $\frac{2}{3}$ or at most $\frac{1}{3}$.

QMA

Language $L \subseteq \{0,1\}^*$ is in ***Quantum Merlin-Arthur*** (***QMA***) if there exist a family of *verifier* circuits $\{C_1, C_2, \ldots\}$ that are uniformly generated and satisfy:

- $|C_n| \leq n^c$
- For all $x \in \{0,1\}^n$
  - If $x \in L \Longrightarrow \exists|\psi\rangle, \Pr[C_n\ accepts\ |x\rangle \otimes |\psi\rangle] \geq \frac{2}{3}$ (Completeness)
  - If $x \notin L \Longrightarrow \forall|\psi\rangle, \Pr[C_n\ accepts\ |x\rangle \otimes |\psi\rangle] \leq \frac{1}{3}$ (Soundness)

QMA

Problems in QMA:

- All problems in BQP
- All problems in NP
- Finding minimum energy states of quantum systems (the Local Hamiltonians problem)

Canonical QMA-complete (promise) problem:

Q-VER-CIRCUIT: given classical description of quantum circuit C, decide if

- There exists a quantum state $|\psi\rangle$ such that C accepts $|\psi\rangle \otimes |0 \cdots 0\rangle$ with probability at least $\frac{2}{3}$, or
- All states $|\psi\rangle$ are accepted with probability at most $\frac{1}{3}$.

Local Hamiltonians problem

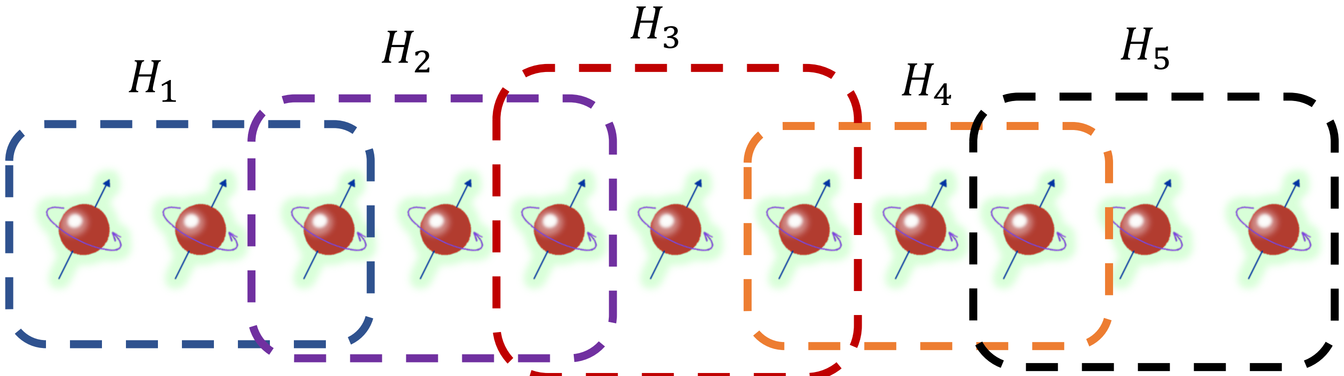
(k, α, β)**-Local Hamiltonians problem**: given classical description of measurements $\{H_1, H_2, \ldots, H_m\}$ on n qubits where each H_i

- Acts on k qubits
- Is a two-outcome measurement (with outcomes labelled "Accept" and "Reject"),

decide whether there exists a quantum state $|\psi\rangle$ such that

- <u>YES case:</u> $\sum p_i \leq \alpha$
- <u>NO case:</u> $\sum p_i \geq \beta$

where p_i = $\Pr[\text{measuring} |\psi\rangle \text{ using } H_i \text{ yields "Reject"}]$



Local Hamiltonians problem

(k, α, β)**-Local Hamiltonians problem**: given classical description of measurements $\{H_1, H_2, \ldots, H_m\}$ on n qubits where each H_i

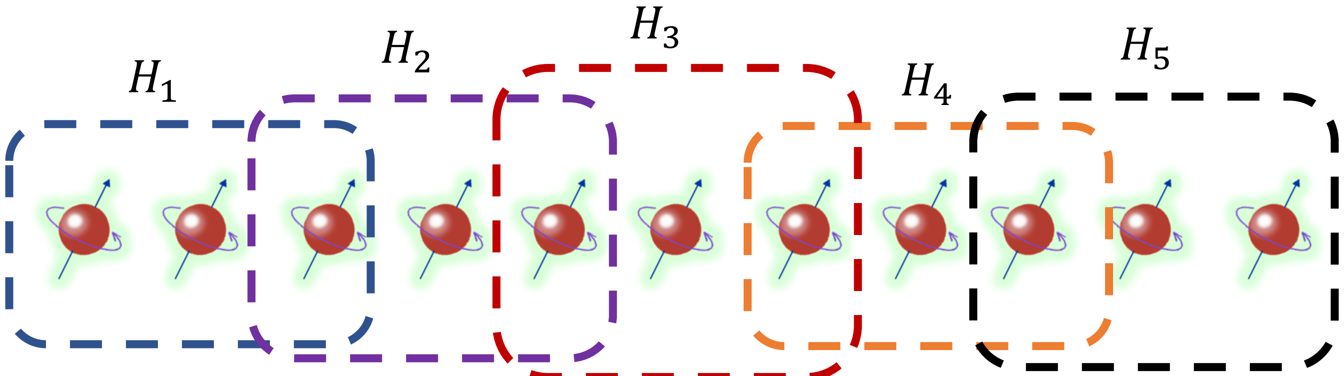
- Acts on k qubits
- Is a two-outcome measurement (with outcomes labelled "Accept" and "Reject"),

decide whether there exists a quantum state $|\psi\rangle$ such that

- <u>YES case:</u> $\sum p_i \leq \alpha$
- <u>NO case:</u> $\sum p_i \geq \beta$

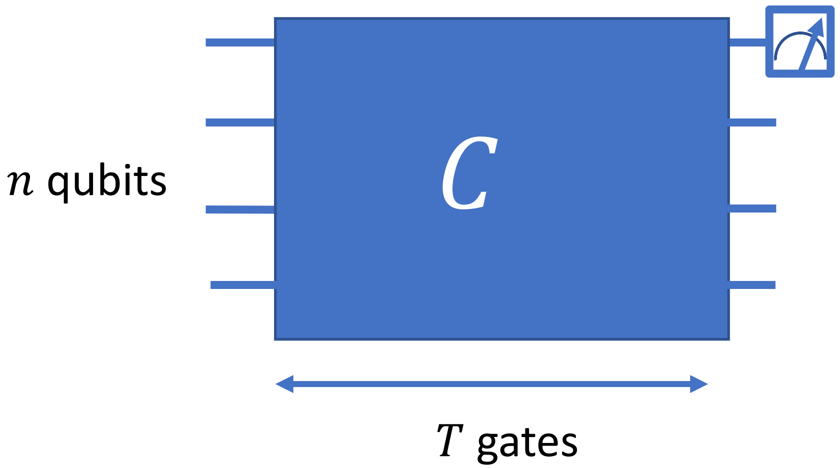
where p_i = $\Pr[\text{measuring} |\psi\rangle \text{ using } H_i \text{ yields "Reject"}]$

The (k, α, β)-Local Hamiltonians problem is **QMA**-complete for $k = 3, \beta - \alpha \geq \frac{1}{poly(n)}$



QMA-completeness of Local Hamiltonians

Instance of **Q-VER-CIRCUIT**



Instance of **3-Local Hamiltonians**

3-Local Measurements $\{H_1, H_2, \ldots, H_m\}$ where

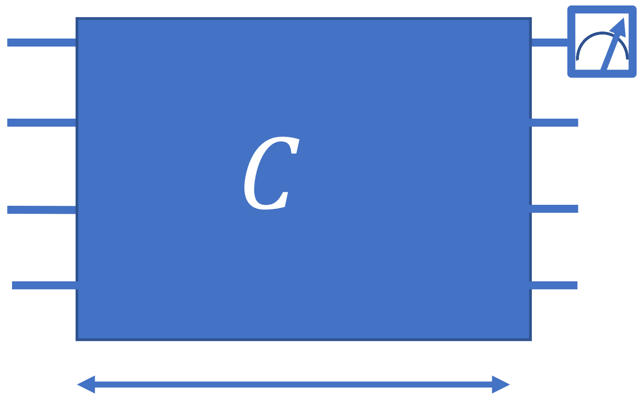
- YES case: there exists a quantum state $|\psi\rangle$ such that $\sum p_i \leq \exp(-n)$
- NO case: for all quantum states $|\psi\rangle$, $\sum p_i \geq \Omega\left(\frac{1}{T^3}\right)$

where p_i = $\Pr[\text{measuring} |\psi\rangle \text{ using } H_i \text{ yields "Reject"}]$

Assume that WLOG completeness and soundness errors are exponentially small.

QMA-completeness of Local Hamiltonians

Instance of **Q-VER-CIRCUIT**



Let $|\theta\rangle$ be such that C accepts $|\theta\rangle \otimes |0 \cdots 0\rangle$ with probability at least $1 - \exp(-n)$.

Witnesses of YES instances of **Q-VER-CIRCUIT** are mapped to witnesses of YES instances of **3-Local Hamiltonians** in the following way:

$$|\psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |\hat{t}\rangle \otimes |\psi_t\rangle$$

"history state"

where

- $|\psi_0\rangle = |\theta\rangle \otimes |0 \cdots 0\rangle$
- $|\psi_t\rangle = G_t |\psi_{t-1}\rangle$ for $t \geq 1$

$$\sum \Pr[\text{measuring} |\psi\rangle \text{ using } H_i \text{ yields "Reject"}] \leq \exp(-n)$$

Mixed States

Probabilistic mixtures of pure quantum states

- Up till now, we've represented quantum states as unit vectors in $\mathbb{C}^d$. These are called ***pure states***.

- Describing a quantum system using a pure state $|\psi\rangle$ indicates that state of the system is ***determined***.

- **Ex**: taking a qubit in the $|0\rangle$ state, and applying H to it.

- What if someone flips a coin and hands you either $|0\rangle$ or $|+\rangle$ depending on the coin? If you do not see the coin, then the state given to you is a ***mixed state***. We can describe this as a probabilistic mixture:

$$\left(\frac{1}{2}, |0\rangle\right), \left(\frac{1}{2}, |+\rangle\right)$$

Density matrices

- A d-dimensional density matrix is a matrix $\rho \in \mathbb{C}^{d \times d}$ such that
  - ρ is positive semidefinite
  - $Tr(\rho) = 1$

- Density matrices describe mixed states.

- A pure state $|\psi\rangle \in \mathbb{C}^d$ corresponds to density matrix $|\psi\rangle\langle\psi|$.

- A mixture $\{(p_1, |\psi_1\rangle), \ldots, (p_k, |\psi_k\rangle)\}$ corresponds to density matrix $\sum_i p_i \, |\psi_i\rangle\langle\psi_i|$

Density matrices

- **Ex**: $|0\rangle, |1\rangle$

- **Ex:** $\left(\frac{1}{2}, |0\rangle\right), \left(\frac{1}{2}, |+\rangle\right)$

Density matrices

- **Ex:** $\left(\frac{1}{2}, |0\rangle\right), \left(\frac{1}{2}, |1\rangle\right)$

- **Ex:** $\left(\frac{1}{2}, |+\rangle\right), \left(\frac{1}{2}, |-\rangle\right)$

Projective measurements

$M = \{M_1, M_2, \ldots, M_k\}$ is a k-outcome projective measurement if

- Each M_i is a Hermitian projection matrix, i.e., $M_i^\dagger = M_i$ and $M_i^2 = M_i$
- $M_1 + M_2 + \cdots + M_k = I$

Measuring a pure state $|\psi\rangle$ using M yields

- outcome i with probability $\| M_i |\psi\rangle \|^2$
- Post-measurement state $\frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|^2}$

Projective measurements

$M = \{M_1, M_2, \ldots, M_k\}$ is a k-outcome projective measurement if

- Each M_i is a Hermitian projection matrix, i.e., $M_i^\dagger = M_i$ and $M_i^2 = M_i$
- $M_1 + M_2 + \cdots + M_k = I$

Measuring a pure state $|\psi\rangle$ using M yields

- outcome i with probability $\| M_i |\psi\rangle \|^2$
- Post-measurement state $\frac{M_i|\psi\rangle}{\| M_i |\psi\rangle \|^2}$

Ex: measuring according to orthonormal basis $B = \{|b_0\rangle, \ldots, |b_{d-1}\rangle\}$ corresponds to projectors $M_i = |b_i\rangle\langle b_i|$

Density matrices

- Density matrices encode everything that is physically relevant about a probabilistic mixture of pure states.

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

- **Measurement**: Let $M = \{M_1, M_2, \ldots, M_k\}$ denote a k-outcome projective measurement. Then measuring ρ with M yields outcome i with probability $Tr(M_i\, \rho)$

- **Post-measurement state**: $\rho \mapsto \frac{M_i \rho M_i}{Tr(M_i\, \rho)}$

Density matrices

- **Ex:** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\rho = |\psi\rangle\langle\psi|$, measure using standard basis.

- **Ex:** $\rho = \frac{I}{2}$, measure using basis $B = \{|b_0\rangle, |b_1\rangle\}$

Quantum One-Time Pad

- **Classical one-time pad**: Fix message $m \in \{0,1\}^n$. Let s be uniformly random n-bit string. Marginal distribution of $m \oplus s$ is uniformly random.

Quantum One-Time Pad

- **Classical one-time pad**: Fix message $m \in \{0,1\}^n$. Let s be uniformly random n-bit string. Marginal distribution of $m \oplus s$ is uniformly random.

- **Quantum one-time pad**: Fix qubit $|\psi\rangle \in \mathbb{C}^2$. Sample uniformly random bits $a, b \in \{0,1\}$. Apply $Z^a X^b$ to $|\psi\rangle$.

- The ensemble $\left\{\left(\frac{1}{4}, Z^a X^b|\psi\rangle\right)\right\}$ looks uniformly random.

Quantum One-Time Pad

- **Classical one-time pad**: Fix message $m \in \{0,1\}^n$. Let s be uniformly random n-bit string. Marginal distribution of $m \oplus s$ is uniformly random.

- **Quantum one-time pad**: Fix qubit $|\psi\rangle \in \mathbb{C}^2$. Sample uniformly random bits $a, b \in \{0,1\}$. Apply $Z^a X^b$ to $|\psi\rangle$.

- The ensemble $\left\{\left(\frac{1}{4}, Z^a X^b |\psi\rangle\right)\right\}$ looks uniformly random.

- Corresponding density matrix:

$$\frac{1}{4}(|\psi\rangle\langle\psi| + X|\psi\rangle\langle\psi|X + Z|\psi\rangle\langle\psi|Z + ZX|\psi\rangle\langle\psi|XZ) = \frac{I}{2}$$

Density matrices of multiple systems

- Given two quantum systems described by density matrices ρ, σ, their joint system is described by the density matrix $\rho \otimes \sigma$.

- n copies of ρ is abbreviated $\rho^{\otimes n}$

- Not all density matrices on multiple systems can be written as $\rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \cdots$.

- But doesn't mean entangled! For example, $\rho = \frac{1}{2}|00\rangle\langle 00 \Big| + \frac{1}{2}\Big| 11\rangle\langle 11|$ is a mixture of classical states; has *classical correlations*.

Traces and partial traces

- $Tr(\rho \otimes \sigma) = Tr(\rho) \cdot Tr(\sigma)$

- Given density matrix ρ_{AB} on systems AB, can obtain density matrix on system A only via the ***partial trace***:

$$\rho_A = Tr_B(\rho_{AB})$$

- $Tr_B(\cdot)$ denotes "tracing out" (a.k.a. marginalizing over) the B subsystem.

- Partial trace $Tr_B(\cdot)$ defined as $Tr_B(|a_1, b_1\rangle\langle a_2, b_2|) = \langle a_2|a_1\rangle \cdot |b_1\rangle\langle b_2|$ for all vectors $|a_1\rangle, |a_2\rangle, |b_1\rangle, |b_2\rangle$.

Density matrices

- **Ex:** $\rho = |0\rangle\langle 0| \otimes |+\rangle\langle +|$

- **Ex:** $\rho = |EPR\rangle\langle EPR|$

Distinguishability of density matrices

Given two density matrices ρ and σ of the same dimension, we can measure how close they are via the ***trace distance***:

$$D(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}Tr(|\rho - \sigma|)$$

Operational meaning: Trace distance $D(\rho, \sigma)$ is equivalently defined as maximum probability of distinguishing between ρ, σ using ANY possible quantum operation (measurements or unitaries).

Distinguishability of density matrices

Nice properties:

1. Nonnegative: $D(\rho, \sigma) \geq 0$, and achieves 0 if and only if $\rho = \sigma$.

2. Symmetric: $D(\rho, \sigma) = D(\sigma, \rho)$

3. Triangle inequality: $D(\rho, \sigma) \leq D(\rho, \tau) + D(\tau, \sigma)$

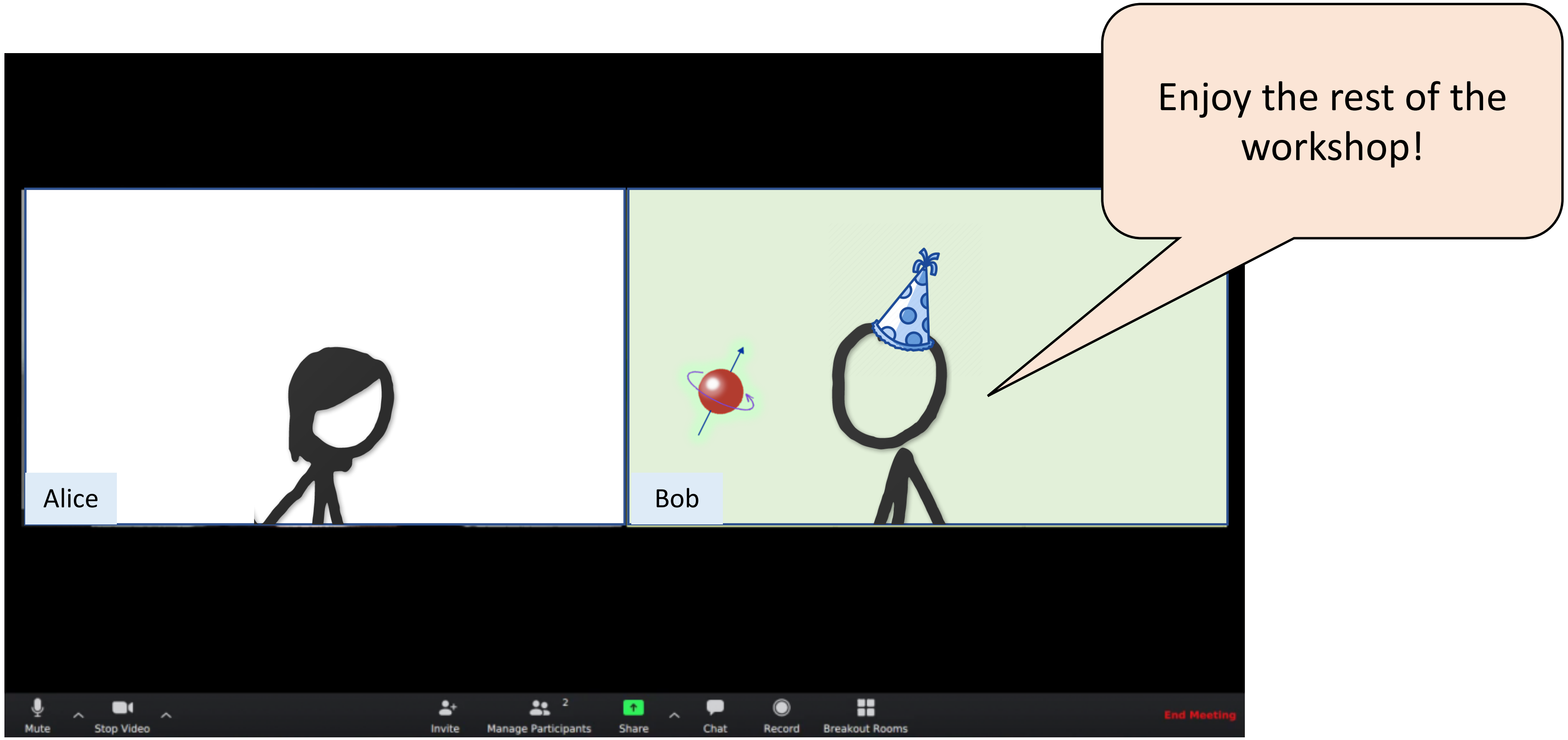
4. Convex: $D(\sum_i p_i \, \rho_i, \sigma) \leq \sum_i p_i \, D(\rho_i, \sigma)$

5. Does not increase when tracing out systems: $D(\rho_A, \sigma_A) \leq D(\rho_{AB}, \sigma_{AB})$

6. Unitarily invariant: $D\left(U\rho U^\dagger, U\sigma U^\dagger\right) = D(\rho, \sigma)$

Density matrices

- **Ex:** $\rho = \frac{1}{2}|0,0\rangle\langle 0,0| + \frac{1}{2}|1,1\rangle\langle 1,1|$ $\sigma = \frac{1}{2}|0,1\rangle\langle 0,1| + \frac{1}{2}|1,0\rangle\langle 1,0|$


Enjoy the rest of the workshop!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

FIN