8.372 Quantum Information Science III **Fall 2024**

Lecture 1: September 5, 2024

Scribe: David D. Dai *Bit commitment and purifications*

1.1 Class Introduction

Topics

1. Quantum information theory and its mathematical foundations
2. Basic tools: norms, randomness, quantum entropies, and symmetry (group representations)
3. Applications: cryptography, many-body physics, optimization, and complexity / algorithms

Websites

1. Canvas: shell linking to everything else, email announcements
2. Piazza: discussion, questions (threaded conversations)
3. Gradescope: submit homework
4. Gitlab: lecture notes, homework problems
5. Overleaf: scribing

1.2 Information-Theoretically Secure Quantum Cryptography

Information-theoretically secure cryptography is secure against an adversary with infinite computational resources and time. This is stronger than security based on computational assumptions, such as RSA, which is based on the hardness of factoring. Some primitives that we might want to perform are:

1. Quantum key distribution: Alice and Bob want to share a secure random key and prevent eavesdropper Eve from learning the key. The goal is for Alice and Bob to finish the protocol with an identical key that Eve knows nothing about, or to abort.
2. Coin flipping: Alice and Bob are remote and need to simulate a fair coin flip. Letting the probability that the coin is 1 be p, there are two cases:
   - Strong: $p \in \left[\frac{1}{2} - \epsilon, \frac{1}{2} + \epsilon\right]$ for some small ϵ no matter what. Alice and Bob cannot bias the coin in either direction.
   - Weak: Alice can bias $p \in \left[\frac{1}{2} - \epsilon, 1\right]$ and Bob can bias $p \in \left[0, \frac{1}{2} + \epsilon\right]$. This is useful if Alice prefers 0 and Bob prefers 1. For example, most people prefer to serve first in a sports match.
3. Oblivious transfer: Alice has a database $(x_0, x_1, x_2, \ldots)$, and Bob wants to access a specific value x_i. Bob doesn't want to reveal i to Alice, and Alice doesn't want to reveal the other values in the database to Bob.

4. Bit commitment: Alice writes a message, seals it in an envelope, and hands it to Bob (*commit* phase). Bob cannot read the message by himself (*hiding* property). Later, Alice can send instructions to Bob to reveal her earlier message (*reveal* phase). However, she cannot change the message after having committed it earlier (*binding* property). After the protocol concludes, Bob either learns the message (*valid* property) if nobody cheated, or he rejects.

Aside from quantum key distribution, all of these primitives have a similar trust model in which both parties are potentially honest or potentially adversarial. This situation is known as "two-party cryptography". Not all of these primitives are independent: oblivious transfer > bit commitment > strong coin flip > weak coin flip. Only weak coin flip and quantum key distribution are possible.

1.3 State Purification

The set of density matrices for a d-dimensional quantum system is:

$$D_d = \{\rho \in \mathcal{C}^{d\times d} : \rho \geq 0, \operatorname{Tr}\rho = 1\}, \tag{1.1}$$

where $\rho \geq 0$ means that ρ is positive semidefinite. Density matrices can be interpreted as a random ensemble of pure states, or as the marginal resulting from looking only at a small subsystem of a larger global pure state. In the marginal case, $\rho_A = \operatorname{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$, where $|\psi_{AB}\rangle$ is the global pure state, ρ_A is the density matrix for subsystem A, and Tr_B is the partial trace over the rest of the composite system.

We are interested in the inverse problem: given some fixed ρ_A, what is the set of all $|\psi_{AB}\rangle$ for which ρ_A is the reduced density matrix for subsystem A? Let d_A (d_B) be the dimension of subsystem A (B). Then the global pure states are:

$$|\psi_{AB}\rangle = \sum_{ij} C_{ij}\,|i\rangle \otimes |j\rangle\,, \quad \sum_{ij} |C_{ij}|^2 = 1. \tag{1.2}$$

The corresponding density matrix for subsystem A is:

$$\begin{aligned}
\rho_A &= \operatorname{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|) \\
&= \sum_k I \otimes \langle k| \sum_{ij} C_{ij}\,|i\rangle \otimes |j\rangle \sum_{i'j'} C_{i'j'}\,\langle i'| \otimes \langle j'|\, I \otimes |k\rangle \\
&= \sum_{ii'} \left[CC^\dagger\right]_{ii'} |i\rangle\langle i'|\,. \\
&= CC^\dagger
\end{aligned} \tag{1.3}$$

For all C, we can perform an SVD:

$$C = UDV^\dagger \to \rho_A = CC^\dagger = UD^2U^\dagger. \tag{1.4}$$

Except for the requirement that it be an isometry, V is unconstrained. D^2 is fixed because it corresponds to ρ_A's eigenvectors. U is also fixed up to rotations within eigenspaces, i.e. $U \to UR$ for unitary R such that $RD = DR$. Because R can be commuted through D as $(UR)DV^\dagger = UDRV^\dagger = UD(VR^\dagger)^\dagger$, the freedom in U can be folded into the freedom in V.

Therefore, the set of all purifications of ρ_A is:

$$\begin{gathered} \rho_A = UD^2U^\dagger \text{ (Eigendecomposition)} \\ \{\psi_{AB} = UDV^\dagger : V^\dagger V = I\}. \end{gathered} \tag{1.5}$$

The dimensions are:

$$\begin{aligned} \dim U &= d_A \times r, \\ \dim D &= r \times r, \\ \dim V &= d_B \times r, \end{aligned} \tag{1.6}$$

where r is the number of nonzero eigenvalues of ρ_A. For some V_1 with $\dim V_1 = d_{B_1} \times r$ and V_2 with $\dim V_2 = d_{B_2} \times r$, we can always find either an isometry W such that $V_2 = WV_1$ or $V_1 = WV_2$. To prove this, take $d_{B_2} \geq d_{B_1}$ WLOG. We can always complete the basis using Gram-Schmidt to create a $d_{B_1} \times d_{B_1}$ unitary $\tilde{V_1}$ which has V_1 as its first r columns. Additionally, use Gram-Schmidt to create $d_{B_2} \times d_{B_1}$ isometry $\tilde{V_2}$ that agrees with V_2 in its first r columns. Then the isometry between V_1 and V_2 is $W = \tilde{V_2}\tilde{V}_1^\dagger$. W clearly maps V_1 to V_2, and it is an isometry because $W^\dagger W = (\tilde{V_2}\tilde{V}_1^\dagger)^\dagger(\tilde{V_2}\tilde{V}_1^\dagger) = \tilde{V_1}\tilde{V}_2^\dagger\tilde{V_2}\tilde{V}_1^\dagger = I$.

We can also see that an isometry performed on subsystem B does not change ρ_A. In general, we have:

$$\begin{aligned} U \otimes V \left|\psi_{AB}\right\rangle &= \sum_{ij} C_{ij}\, U\left|i\right\rangle \otimes V\left|j\right\rangle, \\ &= \sum_{ii'jj'} U_{i'i}C_{ij}V_{j'j}\left|i'\right\rangle \otimes \left|j'\right\rangle, \\ &= \sum_{ij} \left[UCV^T\right]_{ij}\left|i\right\rangle \otimes \left|j\right\rangle. \end{aligned} \tag{1.7}$$

Since $\left(CV^T\right)\left(CV^T\right)^\dagger = C\left(V^\dagger V\right)^* C^\dagger = CC^\dagger$, $I \otimes V\left|\psi_{AB}\right\rangle$ and $\left|\psi_{AB}\right\rangle$ are purifications of the same ρ_A.

Putting the two directions together, we have the theorem: $\left|\psi_{AB}\right\rangle$ and $\left|\gamma_{AB'}\right\rangle$ purify the same density matrix ρ_A if and only if there exists some isometry W on the auxiliary spaces B and B' such that $I_A \otimes W\left|\psi_{AB}\right\rangle = \left|\gamma_{AB'}\right\rangle$ or $I_A \otimes W\left|\gamma_{AB'}\right\rangle = \left|\psi_{AB}\right\rangle$. The backward direction is very intuitive. Imagine that subsystem A is held by Alice on Earth, and subsystem B is held by Bob on Mars. By causality, an action that Bob takes alone is undetectable by Alice, i.e. cannot affect Alice's density matrix.

1.4 Proof that (Perfect) Bit Commitment is Impossible

There are three pictures of quantum operations: trace-preserving completely positive maps, Kraus operators, and isometries followed by partial traces. All are equivalent, and we use "isometry followed by partial trace" here for convenience. We can actually ignore the partial trace: there is no difference between irreversibly throwing away the environment and merely not looking at it again. Ignoring the partial trace also allows for the possibility that a dishonest player may keep the environment and analyze it to gain an advantage instead of discarding it as instructed.

Then after the commit phase, Alice and Bob share the global pure state $|\psi_{AB}^{(b)}\rangle$ for committed bit b. By the hiding property, $\rho_B^{(0)} = \rho_B^{(1)}$. Then by the above theorem, there exists some unitary U in Alice's Hilbert space such that $U \otimes I_B\, |\psi_{AB}^{(0)}\rangle = |\psi_{AB}^{(1)}\rangle$, which violates the binding property. Therefore, exact bit commitment is impossible.