**8.S372/18.S996 Quantum Information Science III** **Fall 2020**

# Lecture 2: Sep 3, 2020

*Lecturer: Aram Harrow* *Scribe: Andrey Boris Khesin, Michael DeMarco*

Today

- unitary freedom of purifications
- applications to bit commitment
- norms, trace distance and fidelity

We can use matrix considerations from the previous lecture to see how to purify quantum states. Recall that we can write:

$$|\psi\rangle = \sum_{i,j} c_{i,j} |i\rangle \otimes |j\rangle \equiv vec(C) \tag{2.8}$$

$$\psi_A = CC^\dagger \tag{2.9}$$

$$C = UDV^\dagger \implies \psi_A = UD^2U^\dagger \tag{2.10}$$

Now, given $\psi_A$, $\exists U, D$ s.t. $\psi_A = UD^2U^\dagger$. We can choose $C = UD$ or $C = UDV^\dagger$ for any unitary $V$. This allows to purify any density matrix.

Besides the choice of $V$, there is another redundancy inherent in this formalism. Suppose that we have two matrices (of the same size) $C, \tilde{C}$ such that $CC^\dagger = \tilde{C}\tilde{C}^\dagger$, with $C = UDV^\dagger$ and $\tilde{C} = \tilde{U}\tilde{D}\tilde{V}^\dagger$. Then $UD^2U^\dagger = \tilde{U}\tilde{D}^2\tilde{U}^\dagger \implies D = \tilde{D}$, with $D = \text{diag}(\lambda_1\ \lambda_1\ \lambda_1\ \lambda_2\ \lambda_2\ \lambda_3)$. We have the freedom to right multiply $U$ by any unitary matrix that commutes with $D$, i.e. which acts block-diagonally on the degenerate eigenvalues in $D$:

$$CC^\dagger = \tilde{C}\tilde{C}^\dagger UD^2U^\dagger = \tilde{U}\tilde{D}^2\tilde{U}^\dagger \implies D = \tilde{D}U = \tilde{U}R \text{ for some } R \text{ such that } [R, D] = 0 \tag{2.11}$$

These considerations allow us to prove:

**Theorem 1** *Given states $|\psi\rangle_{AB}$ and $|\gamma\rangle_{AB}$, $\psi_A = \gamma_A \iff$ there exists a unitary $W$ s.t. $(I \otimes W)|\psi\rangle = |\gamma\rangle$.*

Proof: $\Longleftarrow$ is easy. $\Longrightarrow$ : Let $|\psi\rangle = vec(X)$, $|\gamma\rangle = vec(Y) = \sum_{i,j} Y_{i,j} |i\rangle \otimes |j\rangle$, with $XX^\dagger = YY^\dagger$, $X = U_1D_1V_1^\dagger$, $Y = U_2D_2V_2^\dagger$ Now, $U_1D_1^2U_1^\dagger = U_2D_2^2U_2^\dagger \implies D_1 = D_2$ Hence $U_2 = U_1R$, for some $R$ s.t. $[R, D_1] = 0$.

On the other hand, this implies that:

$$(I \otimes W) |\psi\rangle = (I \otimes W) \sum_{i,j} X_{i,j} |i\rangle \otimes |j\rangle = \tag{2.12}$$

$$\sum_{i,j} X_{i,j} |i\rangle \otimes W |j\rangle = \tag{2.13}$$

$$\sum_{i,j,k} X_{i,j} W_{j,k} |i\rangle \otimes |k\rangle = vec(XW) \tag{2.14}$$

(Note that applying unitary to the 1st system is represented by left-multiplication on $X$) Now, since $W = V_1 R V_2^\dagger$, $XW = (U_1 D_1 V_1^\dagger)(V_1 R V_2^\dagger) = U_2 D_2 V_2^\dagger = Y$ and so the proof is complete.

Corollary: Consider two states $|\psi\rangle_{AB}$, $|\gamma\rangle_{AB'}$. Then $\psi_A = \gamma_A \iff$ either there is an isometry $V : B \to B'$ or $V : B' \to B$ that relates them. (This allows us to relax the condition that $C, \tilde{C}$ be of the same size.

**Quantum Key Distribution** We now turn to the BB84 cryptosystem as applied to quantum key distribution (QKD). Alice chooses a random bit $r$, and a random basis $b \in \{X, Z\}$

($Z$ basis: $|0\rangle$, $|1\rangle$ $\quad X$ basis: $|+\rangle$, $|-\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$)

Alice sends this to Bob, and he measures in a random basis $m \in \{X, Z\}$. Bob tells Alice he's measured, then both reveal bases, discard if $b! = m$, otherwise keep answer. Repeat $N$ times, get about $\frac{N}{2}$ bits. If Eve measures, she will introduce errors, which Alice and Bob can detect.At the end of this, Alice and Bob have a "key", a shared secret random string.

### Coin Flipping

In quantum mechanics, strong coin-flipping is impossible, weak coin-flipping with any bias $\epsilon > 0$ is possible. Alice can choose any bias between 0 and $\frac{1}{2} + \epsilon$, Bob can choose anything in $[\frac{1}{2} - \epsilon, 1]$.

### Bit Commitment

In bit commitment, Alice and Bob do not trust each other, so we want to devise a way for Alice to commit a bit to Bob, and we would like to store this bit for a while, without Bob being able to see it nor Alice being able to change it, before revealing it to Bob. Formally, there are two phases: Commit and Reveal. In the commit phase, Alice commits to a bit $b$, and then in the reveal phase Bob learns $b$.

A secure bit commitment most satisfy:

1. Valid: If both players are honest, Bob learns $b$ and doesn't abort
2. Hiding: After Commit phase, Bob can't learn $b$
3. Binding: During Reveal phase, Alice can convince Bob to accept only one value of $b$.

Related to bit commitment is oblivious transfer (OT): stronger than Bit Commitment, equivalent to secure multi-party computation. Alice chooses bits $(x_0, x_1)$. Bob inputs $b$, learns $x_b$. Alice learns nothing.

Generically, OT > BC > strong coin flipping.

Many of these things are possible quantumly with computational assumptions, but impossible without them. (See Urmila Mahadev + others… LWE=learning with errors)

**Theorem 2** *Information-theoretically secure quantum bit commitment is impossible.*

**Detour: Quantum Channels**

QCs encode Noisy quantum operation $\rho_A \to N(\rho_B)$ Which $N$ are allowed? (Analogous to unitary or stochastic matrices for pure-state quantum mechanics or probability)? We allow the following operations:

1. TPCP maps = Trace-preserving, completely positive linear maps
2. Kraus decomposition. $N(\rho) = \sum_k E_k \rho E_k^\dagger$, where $\{E_k\}$ are Kraus operators
3. $N(\rho) = \mathrm{tr}_E[V \rho V^\dagger]$, where $V : A \to B \otimes E$ is an isometry.

For our purposes, we will take the third option.

Now a secure bitcommitment protocol looks like Alice and bob exchanging bits, a commit phase, more exchanges, and then a reveal phase:

Alice → Bob

←

→

←

Commit phase: state is $\rho_0$ or $\rho_1$

←

→

←

→

Reveal phase

We will modify this to make players "honest but curious": Bob will try to discover the content of the bit during the commit phase, but would not act on any information he discovers. Quantumly, this means that whenever Alice or Bob does a noisy operation, just do the isometry, skip the partial trace. This means that, if the committed bit is $A$ and $B$ is whatever systems are introduced during the player's attempt to discover or cheat, the global state of $AB$ is always pure.

At commit phase, state is $|\psi_b\rangle_{AB}$ for $b \in \{0, 1\}$. Suppose that protocol is perfectly hiding. $\implies \psi_0^B = \psi_1^B$. $|\psi_0\rangle_{AB} = (W \otimes I) |\psi_1\rangle_{AB}$. $\implies$ not at all binding. Done.

As a generalizatino, can we have a protocol that is $\epsilon$-hiding, $\delta$-valid? IE Bob can only learn $\epsilon$ information, Alice gets caught with probability $1 - \delta$. We would then need need a robust version of purification uniqueness: If $\psi_A \sim \gamma_A$, does there exist $W$ s.t. $\langle\psi| (I \otimes W) |\gamma\rangle \sim 1$? And that leads us to norms.

**Norms**

A *Norm* is a function $|| \cdot || : x \mapsto ||x||$. Such that:

1. $||cv|| = |c|||v||$ for scalar $c$.
2. $||v + w|| \leq ||v|| + ||w||$
3. $||v|| = 0 \leftrightarrow v = 0$ (separating).

In effect, norms measure the distance between states or matrices. We should think of them as generalizations of the overlaps $|| \langle\phi| |\psi\rangle ||$ in regular quantum mechanics.

$L_p$ norms are widely used for vectors:

- $||x||_{L_p} = \left(\sum_i |x_i|^p\right)^{\frac{1}{p}}$
- $L_2 =$ Euclidean
- $L_1 =$ Manhattan
- $L_\infty = max_i|x_i|$

For matrices, we have $S_p =$ Schatten-$p$ norms:

- $||X||_{S_p} = ||svals(X)||_{L_p}$
- $||X||_{S_1} =$ sum of svals = "trace norm"
- $||X||_{S_\infty} =$ biggest singular value

Note that every formulation of quantum mechanics comes with its own natural norm/geometry:

- Pure-state quantum mechanics: $L_2$ unit sphere.
- Probabilities: non-negative vectors in $L_1$ unit sphere
- Density matrices: Positive semi-definite matrices in $S_1$ unit sphere
- Measurement operators: life in $S_\infty$