COL872
Problem Set 4

Mallika Prabhakar (2019CS50440)
Sayam Sethi (2019CS10399)
Satwik Jain (2019CS10398)

April 2023

Contents

1 Question 1

1.1 Question 1.1

Question 1.1

Question. *Give an example of two projective measurements $\mathcal{P}, \mathcal{Q}$ that are non-commutative*

Proof. Let us consider $s, t = 2$ and the projective measurements be defined as follows:

$$\begin{aligned}\mathcal{P} &= \left\{\mathbf{P}_0 = |0\rangle\langle 0| = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \mathbf{P}_1 = |1\rangle\langle 1| = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right\}\\ \mathcal{Q} &= \left\{\mathbf{Q}_0 = |+\rangle\langle +| = \begin{pmatrix}1/2 & 1/2\\ 1/2 & 1/2\end{pmatrix}, \mathbf{Q}_1 = |-\rangle\langle -| = \begin{pmatrix}1/2 & -1/2\\ -1/2 & 1/2\end{pmatrix}\right\}\end{aligned} \tag{1}$$

Let us apply the projective methods in both orders: i.e. $\mathbf{Q}_0\mathbf{P}_0$ and $\mathbf{P}_0\mathbf{Q}_0$ to the qubit $|0\rangle$, which is the probability of getting 00 on $|0\rangle$

$\mathbf{Q}_0\mathbf{P}_0|0\rangle = |+\rangle$ with probability $= \frac{1}{2}$

$$\mathbf{Q}_0\mathbf{P}_0|0\rangle = \begin{pmatrix}1/2 & 1/2\\ 1/2 & 1/2\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}1/2\\ 1/2\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle \tag{2}$$

$\mathbf{P}_0\mathbf{Q}_0|0\rangle = |0\rangle$ with probability $= \frac{1}{4}$

$$\mathbf{P}_0\mathbf{Q}_0|0\rangle = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1/2 & 1/2\\ 1/2 & 1/2\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}1/2\\ 0\end{pmatrix} = \frac{1}{2}|0\rangle \tag{3}$$

Since both the residual states and respective probabilities of seeing 00 after both measurements are different, the two are NOT commutative

□

1.2 Question 1.2

Question 1.2: Show that the projective measurements $\mathcal{P} = \{\mathbf{P}_i\}_{i\in[s]}$ and $\mathcal{Q} = \{\mathbf{Q}_i\}_{i\in[t]}$ are commutative.

Question. *question*

Proof. proof □

1.3 Question 1.3

Question 1.3: Is this the only case in which projective measurements are commutative? Prove or disprove.

Question. *question*

Proof. proof □

2 Question 2

2.1 Question 2.1

Question 2: Collapsing hash from claw-free functions

Question. *Show that* $\{H_k \equiv f_k\}_{k \in K}$ *is a collapsing hash function.*

Proof. We will Begin the proof by stating that the claw free function is a post-quantum CRHF. This can be said because For two bit-strings (x_0, x_1) in the domain of claw-free function, there can be two cases:

1. x_0 and x_1 have the same first bit. In this case no collision is possible between x_0 and x_1 as the claw-free function $f_k(b, \cdot)$ is injective $\forall k \in \mathcal{K}, b \in \{0, 1\}$
2. x_0 and x_1 have different first bit. In this case as well there is no collision possible due to the security definition of claw free function.

□

2.2 Question 2.2

Question 2: Collapsing hash from claw-free functions

Question. *Construct a hash function family* $\mathcal{H}' = \{\mathcal{H}'_k : \{0,1\}^{n+2} \to \{0,1\}^n\}$ *using* $\mathcal{F}$*, and prove that* $\mathcal{H}'$ *is collapsing, assuming* $\mathcal{F}$ *is a claw-free function family.*

Proof. proof □

3 Question 3

3.1 Question 3.1

Question 3: Quantum Proof of Knowledge for Blum's protocol

Question. *Show that* $p'_{Ext} \geq poly(\varepsilon)$.

Proof. proof ☐

3.2 Question 3.2

Question x: description

Question. *Let* $|\psi\rangle$ *be a pure state, and* $\mathbf{P} = (\mathbf{P}, \mathbf{I} - \mathbf{P})$ *any projective measurement such that* $\mathrm{Tr}\left(\mathbf{P} \cdot |\psi\rangle\langle\psi|\right) = 1 - \epsilon$*. Let* $\rho = |\psi\rangle\langle\psi|$ *and* ρ' *the post-measurement state, conditioned on measurement output being* 0*. Show a bound on* $||\rho - \rho'||_{tr}$ *in terms of* ϵ*.*

Proof. The post-measurement state and ρ' can be computed as follows:

$$\begin{aligned} |\psi'\rangle &= \frac{\mathbf{P}|\psi\rangle}{\sqrt{\mathrm{Tr}\left(\mathbf{P} \cdot |\psi\rangle\langle\psi|\right)}} = \frac{\mathbf{P}|\psi\rangle}{\sqrt{1-\epsilon}} \\ \rho' = |\psi'\rangle\langle\psi'| &= \frac{\mathbf{P}|\psi\rangle\langle\psi|\mathbf{P}^\dagger}{\mathrm{Tr}\left(\mathbf{P} \cdot |\psi\rangle\langle\psi|\right)} = \frac{\mathbf{P}\rho\mathbf{P}}{1-\epsilon} \end{aligned} \tag{4}$$

Note that the post-measurement state ρ' is also a pure state. We now state and prove the following claim,

Claim 3.1. *For any two pure states,* $|\psi\rangle$ *and* $|\phi\rangle$*, we have*

$$||\,|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\,||_{tr} = \sqrt{1 - |\langle\psi|\phi\rangle|^2} \tag{5}$$

Proof. Since $|\psi\rangle$ and $|\phi\rangle$ are pure states, we can represent $|\phi\rangle$ as a rotation of $|\psi\rangle$ by some angle θ. Therefore, we can write $\rho_\psi - \rho_\phi$ as,

$$\begin{aligned} |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| &= |\psi\rangle\langle\psi| - \Big((\cos\theta\,|\psi\rangle + \sin\theta\,|\psi^\perp\rangle)(\cos\theta\,\langle\psi| + \sin\theta\,\langle\psi^\perp|)\Big) \\ &= (1-\cos^2\theta)\,|\psi\rangle\langle\psi| - \sin\theta\cos\theta\,|\psi\rangle\langle\psi^\perp| - \sin\theta\cos\theta\,|\psi\rangle\langle\psi^\perp| \\ &- \sin^2\theta\,|\psi^\perp\rangle\langle\psi^\perp| \end{aligned} \tag{6}$$

Now, if we represent this matrix in the $|\psi\rangle, |\psi^\perp\rangle$ basis, we get the eigenvalues as $\sin\theta$ and $-\sin\theta$. Therefore, the trace norm will be,

$$\begin{aligned} ||\rho_\psi - \rho_\phi||_{tr} &= \sum_i \|\lambda_i|, \text{(trace norm is sum of absolute values of eigenvalues)} \\ &= 2|\sin\theta| = 2\sqrt{1-\cos^2\theta} \\ &= 2\sqrt{1 - |\langle\phi|\psi\rangle|^2} \end{aligned} \tag{7}$$

Hence, we have proven the result of the claim. ☐

Now, since we started with a pure state $|\psi\rangle$, the post-measurement state will also be a pure state (conditioned on the output). Therefore, we get the trace distance as,

$$\begin{aligned}
||\rho - \rho'||_{tr} &= 2\sqrt{1 - |\langle\psi|\psi'\rangle|^2} \\
&= 2\sqrt{1 - \left|\mathrm{Tr}\left(\langle\psi| \frac{\mathbf{P}|\psi\rangle}{\sqrt{1-\epsilon}}\right)\right|^2} \\
&= 2\sqrt{1 - \left|\mathrm{Tr}\left(\frac{\mathbf{P}|\psi\rangle\langle\psi|}{\sqrt{1-\epsilon}}\right)\right|^2} \\
&= 2\sqrt{1 - \left(\sqrt{1-\epsilon}\right)^2} \\
&= 2\sqrt{\epsilon}
\end{aligned} \tag{8}$$

□

3.3 Question 3.3

Question x: description

Question. *question*

Proof. proof □

3.4 Question 3.4

Question x: description

Question. *question*

Proof. proof □

4 Question 4

4.1 Question 4

Question x: description

Question. *question*

Proof. proof □

5 Question 5

5.1 Question 5.1

Question x: description

Question. *question*

Proof. proof □

5.2 Question 5.2

Question x: description

Question. *question*

Proof. proof □

5.3 Question 5.3

Question x: description

Question. *question*

Proof. proof □