

# COL872

## Problem Set 4

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

April 2023

### Contents

<b>1</b>	<b>Question 1</b>	<b>2</b>
1.1	Question 1.1 . . . . .	2
1.2	Question 1.2 . . . . .	2
1.3	Question 1.3 . . . . .	3
<b>2</b>	<b>Question 2</b>	<b>4</b>
2.1	Question 2.1 . . . . .	4
2.2	Question 2.2 . . . . .	4
<b>3</b>	<b>Question 3</b>	<b>5</b>
3.1	Question 3.1 . . . . .	5
3.2	Question 3.2 . . . . .	5
3.3	Question 3.3 . . . . .	6
3.4	Question 3.4 . . . . .	6
<b>4</b>	<b>Question 4</b>	<b>7</b>
4.1	Question 4 . . . . .	7
<b>5</b>	<b>Question 5</b>	<b>8</b>
5.1	Question 5.1 . . . . .	8
5.2	Question 5.2 . . . . .	8
5.3	Question 5.3 . . . . .	8

# 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:

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

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  $= \frac{1}{2}$

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

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

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

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

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

*Proof.* Let  $\{|v_i\rangle\}_i$  be an orthonormal basis for  $\mathbb{C}^N$ . Let  $\mathcal{S} = (S_1, \dots, S_s)$  and  $\mathcal{T} = (T_1, \dots, T_t)$  be two partitions of  $[N]$ . Let  $\mathbf{P}_i = \sum_{k \in S_i} |v_k\rangle\langle v_k|$  for each  $i \in [s]$  and  $\mathbf{Q}_j = \sum_{l \in T_j} |v_l\rangle\langle v_l|$  for each  $j \in [t]$ .

$$\begin{aligned}
\mathbf{Q}_j \mathbf{P}_i &= \sum_{l \in T_j} |v_l\rangle \langle v_l| \sum_{k \in S_i} |v_k\rangle \langle v_k| \\
&= \sum_{l \in T_j} \sum_{k \in S_i} |v_l\rangle \langle v_l| |v_k\rangle \langle v_k| \\
&= \sum_{l \in T_j} \sum_{k \in S_i} |v_l\rangle \langle v_l| v_k\rangle \langle v_k| \\
&= \sum_{m \in T \cap S} |v_m\rangle \langle v_m|
\end{aligned} \tag{4}$$

We considered the set  $T \cap S$  because  $\{\mathbf{v}_i\}_i$  is a set of orthonormal vectors and resultant matrix will only involve values where  $k = l$  since the inner product would be zero in all other cases. Similarly, for  $\mathbf{P}_i \mathbf{Q}_j$ , we obtain the same matrix:

$$\mathbf{P}_i \mathbf{Q}_j = \sum_{k \in S_i} |v_k\rangle \langle v_k| \sum_{l \in T_j} |v_l\rangle \langle v_l| = \sum_{m \in T \cap S} |v_m\rangle \langle v_m| \tag{5}$$

Since the resultant matrix is same for both ways of application of measurement, the projective measurements  $\mathcal{P}$  and  $\mathcal{Q}$  are commutative.  $\square$

### 1.3 Question 1.3

#### Question 1.3

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

*Proof.* Using the same notation as in Question 1.21.2. Let us define another orthonormal basis for  $\mathbb{C}^n$  as  $\{|\mathbf{u}_i\rangle\}_i$   $\square$

## 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.

So In both the cases we have no q.p.t that can give a collision and thus claw free function is a collision resistant hash function.

□

### 2.2 Question 2.2

Question 2: Collapsing hash from claw-free functions

**Question.** Construct a hash function family  $\mathcal{H}' = \{\mathcal{H}'_k : \{0, 1\}^{n+2} \rightarrow \{0, 1\}^n\}$  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  $p'_{Ext} \geq \text{poly}(\epsilon)$ .

*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  $\text{Tr}(\mathbf{P} \cdot |\psi\rangle\langle\psi|) = 1 - \epsilon$ . Let  $\rho = |\psi\rangle\langle\psi|$  and  $\rho'$  the post-measurement state, conditioned on measurement output being 0. Show a bound on  $\|\rho - \rho'\|_{tr}$  in terms of  $\epsilon$ .

*Proof.* The post-measurement state and  $\rho'$  can be computed as follows:

$$\begin{aligned} |\psi'\rangle &= \frac{\mathbf{P}|\psi\rangle}{\sqrt{\text{Tr}(\mathbf{P} \cdot |\psi\rangle\langle\psi|)}} = \frac{\mathbf{P}|\psi\rangle}{\sqrt{1 - \epsilon}} \\ \rho' &= |\psi'\rangle\langle\psi'| = \frac{\mathbf{P}|\psi\rangle\langle\psi|\mathbf{P}^\dagger}{\text{Tr}(\mathbf{P} \cdot |\psi\rangle\langle\psi|)} = \frac{\mathbf{P}\rho\mathbf{P}}{1 - \epsilon} \end{aligned} \quad (6)$$

Note that the post-measurement state  $\rho'$  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

$$\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_{tr} = \sqrt{1 - |\langle\psi|\phi\rangle|^2} \quad (7)$$

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

$$\begin{aligned} |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| &= |\psi\rangle\langle\psi| - \left( (\cos\theta|\psi\rangle + \sin\theta|\psi^\perp\rangle)(\cos\theta\langle\psi| + \sin\theta\langle\psi^\perp|) \right) \\ &= (1 - \cos^2\theta)|\psi\rangle\langle\psi| - \sin\theta\cos\theta(|\psi\rangle\langle\psi^\perp| + |\psi^\perp\rangle\langle\psi|) - \sin^2\theta|\psi^\perp\rangle\langle\psi^\perp| \end{aligned} \quad (8)$$

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,

$$\begin{aligned} \|\rho_\psi - \rho_\phi\|_{tr} &= \sum_i \|\lambda_i\|, \text{ (trace norm is sum of absolute values of eigenvalues)} \\ &= 2|\sin\theta| = 2\sqrt{1 - \cos^2\theta} \\ &= 2\sqrt{1 - |\langle\phi|\psi\rangle|^2} \end{aligned} \quad (9)$$

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,

$$\begin{aligned}
\|\rho - \rho'\|_{tr} &= 2\sqrt{1 - |\langle\psi|\psi'\rangle|^2} \\
&= 2\sqrt{1 - \left| \text{Tr} \left( \langle\psi| \frac{\mathbf{P}|\psi\rangle}{\sqrt{1-\epsilon}} \right) \right|^2} \\
&= 2\sqrt{1 - \left| \text{Tr} \left( \frac{\mathbf{P}|\psi\rangle\langle\psi|}{\sqrt{1-\epsilon}} \right) \right|^2} \\
&= 2\sqrt{1 - (\sqrt{1-\epsilon})^2} \\
&= 2\sqrt{\epsilon}
\end{aligned} \tag{10}$$

□

### 3.3 Question 3.3

Question x: description

**Question.** Show that if two states  $\rho, \rho'$  satisfy  $\|\rho - \rho'\|_{tr} \leq \epsilon$ , then for any unitary matrix  $\mathbf{U}$ ,  $\|\mathbf{U} \cdot \rho \cdot \mathbf{U}^\dagger - \mathbf{U} \cdot \rho' \cdot \mathbf{U}^\dagger\|_{tr} \leq \epsilon$ .

*Proof.* Since any unitary matrix is just a change of basis matrix, it does not change the eigen values of any matrix. Hence, the trace distance does not change since it is the sum of absolute values of the eigen values. Also,  $\mathbf{U} \cdot \rho \cdot \mathbf{U}^\dagger$  is the density matrix corresponding to the the density matrix in the changed basis wrt  $\mathbf{U}$ . Therefore, the given inequality in the question holds. □

### 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	
<b>Question.</b> <i>question</i>	
<i>Proof.</i> proof	<input type="checkbox"/>

### 5.2 Question 5.2

Question x: description	
<b>Question.</b> <i>question</i>	
<i>Proof.</i> proof	<input type="checkbox"/>

### 5.3 Question 5.3

Question x: description	
<b>Question.</b> <i>question</i>	
<i>Proof.</i> proof	<input type="checkbox"/>