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

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

Proof. Let $\{|\mathbf{v}_i\rangle\}_i$ be an orthonormal basis for $\mathbb{C}^N$. Let $\mathcal{S} = (S_1, \ldots, S_s)$ and $\mathcal{T} = (T_1, \ldots, T_t)$ 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. □

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 $|\mathbf{u}_i\rangle = \sum_p \alpha_{ip} |\mathbf{v}_p\rangle$. Let us represent $\mathbf{Q}_j$ in $\{|\mathbf{u}_i\rangle\}_i$ basis and $\mathbf{P}_j$ in $\{|\mathbf{v}_i\rangle\}_i$ basis. Therefore, $\mathbf{Q}_j\mathbf{P}_i$ can be written as:

$$\begin{aligned}\mathbf{Q}_j\mathbf{P}_i &= \sum_{l\in T_j} |u_l\rangle\langle u_l| \sum_{k\in S_i} |v_k\rangle\langle v_k| \\ &= \left(\sum_{l\in T_j}\left(\sum_{p\in[N]}\sum_{q\in[N]} \alpha_{lp}\alpha_{lq}\,|v_p\rangle\langle v_q|\right)\right)\left(\sum_{k\in S_i} |v_k\rangle\langle v_k|\right) \\ &= \sum_{l\in T_j}\sum_{k\in S_i}\left(\left(\sum_{p\in[N]}\sum_{q\in[N]} \alpha_{lp}\alpha_{lq}\,|v_p\rangle\langle v_q|\right)|v_k\rangle\langle v_k|\right) \\ &= \sum_{l\in T_j}\sum_{k\in S_i}\sum_{p\in[N]} \alpha_{lp}\alpha_{lk}\,|v_p\rangle\langle v_k| \quad (\because \langle v_q|v_k\rangle = 0 \texttt{ if } q \neq k \texttt{ since orthogonal})\end{aligned} \tag{6}$$

Similarly, $\mathbf{P}_i\mathbf{Q}_j$ can be written as:

$$\begin{aligned}
\mathbf{P}_i\mathbf{Q}_j &= \sum_{k\in S_i} |v_k\rangle\langle v_k| \sum_{l\in T_j} |u_l\rangle\langle u_l| \\
&= \sum_{k\in S_i} |v_k\rangle\langle v_k| \left(\sum_{l\in T_j}\left(\sum_{p\in[N]}\sum_{q\in[N]} \alpha_{lp}\alpha_{lq}|v_p\rangle\langle v_q|\right)\right) \\
&= \sum_{l\in T_j}\sum_{k\in S_i}\left(|v_k\rangle\langle v_k|\left(\sum_{p\in[N]}\sum_{q\in[N]} \alpha_{lp}\alpha_{lq}|v_p\rangle\langle v_q|\right)\right) \\
&= \sum_{l\in T_j}\sum_{k\in S_i}\sum_{q\in[N]} \alpha_{lk}\alpha_{lq}|v_k\rangle\langle v_q| \quad (\because \langle v_k|v_p\rangle = 0 \texttt{ if } p\neq k \texttt{ since orthogonal}) \\
&= \sum_{l\in T_j}\sum_{k\in S_i}\sum_{p\in[N]} \alpha_{lk}\alpha_{lp}|v_k\rangle\langle v_p|
\end{aligned} \tag{7}$$

Now, if $\mathbf{Q}_j\mathbf{P}_i = \mathbf{P}_i\mathbf{Q}_j$, from the values of the two compound projections, it is easy to see that they are Hermitian (and infact symmetric since none of the α_{ij} are non-real). We also have the following,

$$\forall k \in S_i : \forall p \in [N]\setminus S_i : \sum_{l\in T_j} \alpha_{lk}\alpha_{lp} = 0 \tag{8}$$

Since this is true for all $i \in [s]$ and $j \in [t]$ (and using the fact that $\sum_j \alpha_{ij}^2 = 1$), we get that the matrix formed by α_{ij} is a permutation matrix.
Therefore for two projective measurements to be commutative, both should be described using the same orthonormal basis for $\mathbb{C}^n$ and their partion sets should partion $[N]$ □

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.
Now Let us assume that there exist a adversary A that breaks Collapsing property with probability ρ for $\mathcal{H}$ then a reduction B can finds a collision with prob poly(ρ).
Notations:

- A Set S which is a subset of the set U($\{0,1\}^{n+1}$) which has the same image over f_k and has size l (for claw-free function $l = 2$).
- Another set V
- A Superposition φ over pairs (s,v) $\in S \times V$.
- A Binary Projective Measurement P = **(P,I-P)**

Adversary has two Algorithms $\mathcal{A}_1$ and $\mathcal{A}_2$ which are defined as follows:
$\mathcal{A}_1$: sends superposition φ.
$\mathcal{A}_2$: applies Measurement P and sends the mixed state obtained and bit b'.

The Reduction is as follows:

1. Challenger C sends a key $k \in \mathcal{K}$ to B who passes the same to A.
2. A applies Algorithm $\mathcal{A}_1$ and sends superposition φ to B.
3. B applies projective measurement over φ to get a value i and the state φ'.
4. B sends φ' to A.
5. A applies Algorithm $\mathcal{A}_2$ over φ' and sends b' and the state φ'' to B.
6. B applies projective measurement over φ to get a value j.
7. B sends i,j to C.

We will show that the probability of finding a Collision is $\geq \frac{2}{l-1}\rho^2$ Now let us find the probability of finding a Collision, $Pr\Big[i,j \in S, i \neq j\Big]$.

We assume $\varphi = |\psi\rangle\langle\psi|$ for some pure state $|\psi\rangle = \Sigma_{i,v}\alpha_{i,v}|i,v\rangle$

The Probability of finding i in the first projective measurement is p_i =Tr$[(\mathbf{I}\otimes|i\rangle\langle i|)\varphi]$. here φ' becomes $\varphi_i := \frac{1}{p_i}(\mathbf{I}\otimes|i\rangle\langle i|)\varphi(\mathbf{I}\otimes|i\rangle\langle i|)$.

Now, When Algorithm $\mathcal{A}_2$ applies P, the resulting mixed state becomes $\varphi_i' = \mathbf{P}\varphi\mathbf{P} + \mathbf{(I\text{-}P)}\varphi\mathbf{(I\text{-}P)}$. On applying projective measurement again, the probability of getting j is Tr$[(\mathbf{I}\otimes|j\rangle\langle j|)\varphi_i']$. Now summing over all $i \in S$ and $j \in S/\{i\}$, we get the probability of getting distinct $i,j \in S$, which is

$$
\begin{aligned}
Pr\Big[i,j \in S, i \neq j\Big] &= \mathrm{Tr}\Bigg[\sum_{i,j\in S, i\neq j} \substack{(\mathbf{I}\otimes|j\rangle\langle j|)\mathbf{P}(\mathbf{I}\otimes|i\rangle\langle i|)\varphi(\mathbf{I}\otimes|i\rangle\langle i|)\mathbf{P} \\ +(\mathbf{I}\otimes|j\rangle\langle j|)\mathbf{(I\text{-}P)}(\mathbf{I}\otimes|i\rangle\langle i|)\varphi(\mathbf{I}\otimes|i\rangle\langle i|)\mathbf{(I\text{-}P)}}\Bigg] \\
&= 2\mathrm{Tr}\Bigg[\sum_{i,j\in S, i\neq j}(\mathbf{I}\otimes|j\rangle\langle j|)\mathbf{P}(\mathbf{I}\otimes|i\rangle\langle i|)\varphi(\mathbf{I}\otimes|i\rangle\langle i|)\mathbf{P}\Bigg] \\
&= 2\mathrm{Tr}\Bigg[\sum_{\substack{i,j\in S, i\neq j \\ v,v'\in V}}\alpha_{i,v}\alpha'_{i,v'}(\mathbf{I}\otimes|j\rangle\langle j|)\mathbf{P}(|v\rangle\langle v'|\otimes|i\rangle\langle i|)\mathbf{P}\Bigg] \\
&= \Bigg[\sum_{\substack{i,j\in S, i\neq j \\ v,v'\in V}}\alpha_{i,v}\alpha'_{i,v'}(|v'\rangle|i\rangle)\mathbf{P}(\mathbf{I}\otimes|j\rangle\langle j|)\mathbf{P}(|v\rangle|i\rangle)\Bigg] \\
&= \Bigg[\sum_{\substack{i,j\in S, i\neq j \\ v,v',v''\in V}}\alpha_{i,v}\alpha'_{i,v'}\langle v',i|\mathbf{P}|v'',j\rangle\langle v'',j|\mathbf{P}|v,i\rangle\Bigg]
\end{aligned}
$$

Now let's define a vector w as $w_{(i,j,v'')} := \Sigma_v\alpha_{i,v}\langle v'',j|\mathbf{P}|v,i\rangle$ where $i \neq j$, we have Probability $= 2|w^2|$.
To find ρ,

$$
\begin{aligned}
\rho &= \mathrm{Tr}[\mathbf{P}\varphi] - \mathrm{Tr}\Bigg[\mathbf{P}\sum_{i\in S}(\mathbf{I}\otimes|i\rangle\langle i|)\varphi(\mathbf{I}\otimes|i\rangle\langle i|)\Bigg] \\
&= \Bigg[\sum_{\substack{i,j\in S \\ v,v'\in V}}\alpha_{i,v}\alpha^\dagger_{j,v'}\langle v',i|\mathbf{P}|v,j\rangle - \sum_{\substack{i\in S \\ v,v'\in V}}\alpha_{i,v}\alpha^\dagger_{i,v'}\langle v',i|\mathbf{P}|v,i\rangle\Bigg] \\
&= \Bigg[\sum_{\substack{i,j\in S, i\neq j \\ v,v'\in V}}\alpha_{i,v}\alpha^\dagger_{j,v'}\langle v',i|\mathbf{P}|v,j\rangle\Bigg]
\end{aligned}
$$

Now if we define x as vector $x_(i,j,v'') := \alpha_{j,v''}$, we have $\rho = x\cdot w$. Also,

$$
|x|^2 = \sum_{\substack{i,j\in S, i\neq j \\ v''\in V}}|\alpha_{j,v''}|^2 = \sum_{j\in S, v''\in V}(l-1)|\alpha_{j,v''}|^2 = l-1
$$

Therefore, by applying Cauchy-Schwartz Inequality, we have $|w|^2|x|^2 \geq |w \cdot x|^2$. From this we get the required probability for finding a Collision.
Now as we know via security of claw-free function, no q.p.t adversary can find a collision, the probability of finding a collision is negligible and from this we can say that for the case of claw-free function,an adversary can break Collapsing property with only negligible probability and thus $\{H_k \equiv f_k\}_{k \in K}$ is a collapsing hash function. □

2.2 Question 2.2

Question 2: Collapsing hash from claw-free functions

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

Proof. We can define the hash function family $\mathcal{H}'$ as

$$\mathcal{H}' = \{\mathcal{H}'_k : \mathcal{H}'_k \equiv f_k(x, (f_k(y,z))), x, y \in \{0,1\}, z \in \{0,1\}^n\}$$

We have to show the collapsing property, We will show this via Hybrids:

In all the Worlds, Adversary sends $\psi = \sum_{\substack{x,y,z \\ f_k(x,f_k(y,z))=h}} |x,y,z\rangle$.

World-0:

1. Adversary gets back ψ from the challenger.

Hybrid-0:

1. Adversary gets back ψ measured at $x = x'$ from the challenger,
   $\psi = \sum_{\substack{y,z \\ f_k(x',f_k(y,z))=h}} |x',y,z\rangle$.

Hybrid-1:

1. Adversary gets back ψ measured at $x = x', y = y'$ from the challenger,
   $\psi = \sum_{\substack{z \\ f_k(x',f_k(y',z))=h}} |x',y',z\rangle$.

World-1:

1. Adversary gets back ψ measured at $x = x', y = y', z = z'$ from the challenger,
   $\psi = |x',y',z'\rangle ; f_k(x', f_k(y',z')) = h$.

Claim 2.1. *World-0 and Hybrid-0 are Computationally indistinguishable.*

Proof. Let us assume The worlds are far apart, If an adversary can distinguish, from this we can have a reduction that breaks the collapsing property of f_k.
Reduction:

1. Challenger sends key k to reduction B which is passed on to Adversary A.
2. A sends state $\psi = \sum_{\substack{x,y,z \\ f_k(x,f_k(y,z))=h}} |x,y,z\rangle$ to B.
3. B applies f_k to get $\sum_{\substack{x,y,z \\ f_k(x,f_k(y,z))=h}} |x,y,z\rangle\,|f_k(y,z)\rangle$ and sends first part of $\sum_{\substack{x,y,z \\ f_k(x,f_k(y,z))=h}} |x\rangle\,|f_k(y,z)\rangle \otimes |y,z\rangle$ to Challenger C.
4. C chooses bit b and accordingly sends $|\varphi\rangle$ to B.
5. B un-entangles register containing result of f_k application and sends the x,y,z registers to A where x can be measured or not depending upon bit b.
6. A sends it's guess b' to B who passes the same to C.

Now in the case when b=0, the reduction acts like World-0 and when b=1, behaves like Hybrid-0. Now if A is able to win with non-negligible probability then B can also win with a non-negligible probability.

□

Claim 2.2. *Hybrid-0 and Hybrid-1 are Computationally indistinguishable.*

Proof. Let us assume The worlds are far apart, If an adversary can distinguish, from this we can have a reduction that breaks the collapsing property of f_k.
Reduction:

1. Challenger sends key k to reduction B which is passed on to Adversary A.
2. A sends state $\psi = \sum_{\substack{x,y,z \\ f_k(x,f_k(y,z))=h}} |x,y,z\rangle$ to B.
3. B measures register x to get $x = x'$ and sends $\sum_{\substack{y,z \\ f_k(x',f_k(y,z))=h}} |y,z\rangle$ to Challenger C.
4. C chooses bit b and accordingly sends $|\varphi\rangle$ to B.
5. B sends the x,y,z registers to A where $x = x'$ and y can be measured or not depending upon bit b.
6. A sends it's guess b' to B who passes the same to C.

Now in the case when b=0, the reduction acts like Hybrid-0 and when b=1, behaves like Hybrid-1. Now if A is able to win with non-negligible probability then B can also win with a non-negligible probability.

□

Claim 2.3. *Hybrid-1 and World-1 are Computationally indistinguishable.*

Proof. In both the worlds, we have measured the first 2 bits x and y. According to the definition of claw-free function, For a fixed starting bit, the function acts like a injection and therefore the superposition will contain a single element and the ψ will be identical for both the worlds which is indistinguishable as identical qubits are indistinguishable. □

Fro the above three claims we can say that the words World-0 and World-1 are Computationally indistinguishable. From this we can infer the fact that $\mathcal{H}'$ is collapsing. □

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. Let us begin by defining $|\psi_b\rangle = U_b |\psi_{msg_1}\rangle$.
We can say that Prob. of seeing a accept in both $\geq$ prob of seeing accept in first measurement $\times$ prob. of seeing accept in second measurement given an accept in first measurement,i.e.,

$$p'_{ext} \geq p_0 \cdot p_{1|0}$$

where p_0 is the probability of seeing accept in first measurement (Δ_0) and $p_{1|0}$ is the probability of seeing accept in second measurement Δ_1 if an accept was seen in the first measurement.

As we will take a projective measurement over n qubits of the state(according to the dimension of **I**), we can write state $|\psi_b\rangle$ as split between two states: One which gives the measurement and is along the projection and the second which is perpendicular to the measurement basis. In this way $|\psi_b\rangle$ can be written as

$$|\psi_b\rangle = \sqrt{p_b} |w_b\rangle |v_b\rangle + \sqrt{1-p_b} |w_b^{\perp}\rangle \tag{9}$$

Here $|w_b^{\perp}\rangle$ may not necessarily have a physical significance. $|w_b\rangle$ contains the first n qubits of the state which take part in the measurement Δ_b and $|v_b\rangle$ is the remaining state when measurement is done on first n bits from space $N/2^n$.
Also $\| \langle v_b| \langle w_b| |w_b^{\perp}\rangle \|^2 = 0$
Now let us define $|\widetilde{\psi_0}\rangle$ as the state after the $|\psi_0\rangle$ is measured ($\Delta_0 U_0 |\psi_{msg_1}\rangle$) and will be $|\widetilde{\psi_0}\rangle = |w_b\rangle |v_b\rangle$ and define $|\widetilde{\psi_1}\rangle = U_1 U_0^{\dagger} |\widetilde{\psi_0}\rangle$ before applying the second measurement Δ_1. We have,

$$\begin{aligned}
|\widetilde{\psi_1}\rangle &= U_1 U_0^{\dagger} |\widetilde{\psi_0}\rangle \\
&= U_1 U_0^{\dagger} |w_b\rangle |v_b\rangle \\
&= U_1 \left(U_0^{\dagger} \frac{|\psi_0\rangle}{\sqrt{p_0}} - U_0^{\dagger} \sqrt{\frac{1-p_0}{p_0}} |w_0^{\perp}\rangle \right) \\
&= U_1 \frac{|\psi_{msg_1}\rangle}{\sqrt{p_0}} - U_1 U_0^{\dagger} \sqrt{\frac{1-p_0}{p_0}} |w_0^{\perp}\rangle \\
&= \frac{|\psi_1\rangle}{\sqrt{p_0}} - U_1 U_0^{\dagger} \sqrt{\frac{1-p_0}{p_0}} |w_0^{\perp}\rangle \\
&= \frac{1}{\sqrt{p_0}} \left(\sqrt{p_1} |w_1\rangle |v_1\rangle + \sqrt{1-p_1} |w_1^{\perp}\rangle - U_1 U_0^{\dagger} \sqrt{1-p_0} |w_0^{\perp}\rangle \right)
\end{aligned}$$

Where we use the Equation 11 and the definitions of U_0 and U_1.

Now we apply measurement of $|\widetilde{\psi}_1\rangle$. As we are trying to find a lower bound, probability to see accept is minimized when $U_1 U_0^\dagger |w_0^\perp\rangle = |w_1\rangle |v_1\rangle$. From here, it follows that

$$\begin{aligned} p_{1|0} &= \langle\widetilde{\psi}_1| \Delta_1 |\widetilde{\psi}_1\rangle \\ &\geq \frac{1}{p_0}\left(\sqrt{p_1} - \sqrt{1-p_0}\right)^2 \\ &\geq \frac{1}{p_0}\left(\sqrt{p_1} - \sqrt{p_1-\varepsilon}\right)^2 \\ &\geq \frac{\varepsilon^2}{4p_0} \end{aligned}$$

Therefore $p'_{ext} \geq p_0 \cdot p_{1|0} \geq \frac{\varepsilon^2}{4}$

Reference : Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two Provers in Isolation. In Dong Hoon Lee and Xiaoyun Wang, editors, Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings, volume 7073 of Lecture Notes in Computer Science, pages 407–430, 2011.

□

3.2 Question 3.2

Question 3.2

Question. *Let $|\psi\rangle$ be a pure state, and $\mathbf{P} = (\mathbf{P}, \mathbf{I}-\mathbf{P})$ any projective measurement such that $\mathrm{Tr}(\mathbf{P} \cdot |\psi\rangle\langle\psi|) = 1-\epsilon$. 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:

$$\begin{aligned} |\psi'\rangle &= \frac{\mathbf{P}|\psi\rangle}{\sqrt{\mathrm{Tr}(\mathbf{P} \cdot |\psi\rangle\langle\psi|)}} = \frac{\mathbf{P}|\psi\rangle}{\sqrt{1-\epsilon}} \\ \rho' &= |\psi'\rangle\langle\psi'| = \frac{\mathbf{P}|\psi\rangle\langle\psi|\mathbf{P}^\dagger}{\mathrm{Tr}(\mathbf{P} \cdot |\psi\rangle\langle\psi|)} = \frac{\mathbf{P}\rho\mathbf{P}}{1-\epsilon} \end{aligned} \tag{10}$$

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*

$$|| \, |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \, ||_{tr} = \sqrt{1 - |\langle\psi|\phi\rangle|^2} \tag{11}$$

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,

$$\begin{aligned} |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| &= |\psi\rangle\langle\psi| - \Big((\cos\theta\,|\psi\rangle + \sin\theta\,|\psi^\perp\rangle)(\cos\theta\,\langle\psi| + \sin\theta\,\langle\psi^\perp|)\Big) \\ &= (1-\cos^2\theta)\,|\psi\rangle\langle\psi| - \sin\theta\cos\theta\,|\psi\rangle\langle\psi^\perp| - \sin\theta\cos\theta\,|\psi\rangle\langle\psi^\perp| \\ &\quad - \sin^2\theta\,|\psi^\perp\rangle\langle\psi^\perp| \end{aligned} \tag{12}$$

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,

$$\begin{aligned} ||\rho_\psi - \rho_\phi||_{tr} &= \sum_i \|\lambda_i|, \text{ (trace norm is sum of absolute values of eigenvalues)} \\ &= 2|\sin\theta| = 2\sqrt{1-\cos^2\theta} \\ &= 2\sqrt{1-|\langle\phi|\psi\rangle|^2} \end{aligned} \tag{13}$$

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,

$$\begin{aligned} ||\rho - \rho'||_{tr} &= 2\sqrt{1-|\langle\psi|\psi'\rangle|^2} \\ &= 2\sqrt{1-\left|\mathrm{Tr}\left(\langle\psi|\,\frac{\mathbf{P}\,|\psi\rangle}{\sqrt{1-\epsilon}}\right)\right|^2} \\ &= 2\sqrt{1-\left|\mathrm{Tr}\left(\frac{\mathbf{P}\,|\psi\rangle\langle\psi|}{\sqrt{1-\epsilon}}\right)\right|^2} \\ &= 2\sqrt{1-\left(\sqrt{1-\epsilon}\right)^2} \\ &= 2\sqrt{\epsilon} \end{aligned} \tag{14}$$

□

3.3 Question 3.3

Question 3.3

Question. *Show that if two states ρ, ρ' 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 eigenvalues 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. *Using the gentle measurement lemma, give an alternate proof for Question* **??**.

Proof. Consider the partial measurement $\mathbf{\Delta}_0 \cdot \mathbf{U}_0$ followed by the application of the unitary $\mathbf{U}_1 \cdot \mathbf{U}_0^\dagger$. The probability of success (over all input states by the prover) for the partial measurement is p_0. Therefore, the trace distance between directly applying $\mathbf{U}_1$ and applying $\mathbf{U}_1\mathbf{U}_0^\dagger\mathbf{\Delta}_0\mathbf{U}_0$ will be atmost $2\sqrt{1-p_0}$ from the proofs of Question 3.2 and Question 3.3. Now, on applying $\mathbf{\Delta}_1$ to the modified state, we will see a 1 with probability at least $p_1 - \sqrt{1-p_0}$, since half of the trace distance is the maximum probability with with any projective measurement can distinguish between the two states and p_1 is the probability of seeing a 1 in the case of no application of $\mathbf{\Delta}_0$. Now, we obtain the probability of the extractor as,

$$\begin{aligned} p'_{ext} &= p_0 \cdot (p_1 - \sqrt{1-p_0}) \\ &= p_0 \cdot (1 + 2\epsilon - \sqrt{1-p_0}) \\ &\geq 2\epsilon \cdot (1 + 2\epsilon - \sqrt{1-2\epsilon}), \text{ substituting } p_0 = 2\epsilon \\ &\geq \mathcal{O}(\epsilon^2) \end{aligned} \tag{15}$$

Therefore, the success probability of the extractor is a polynomial in ϵ. □

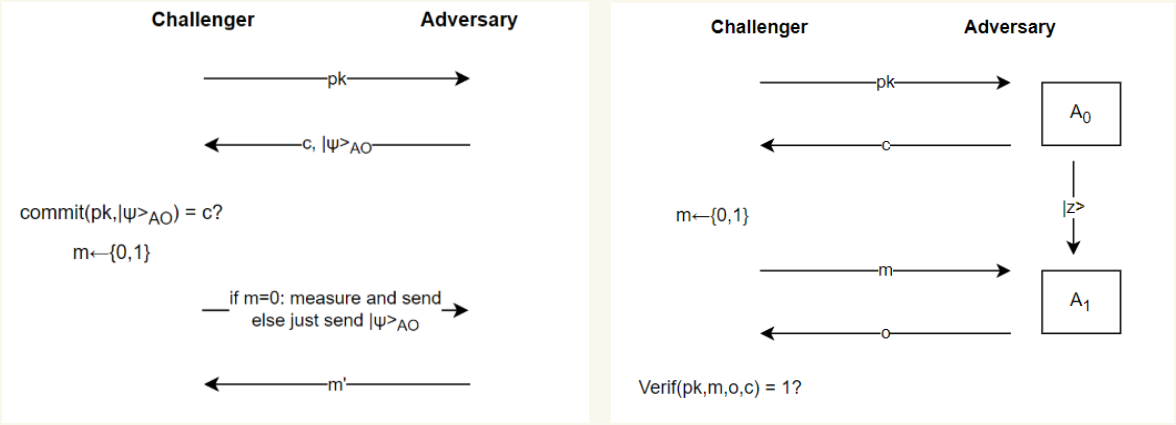
4 Question 4

4.1 Question 4

Question 4

Question. *Let Commit be a single-bit commitment scheme. Show that if Commit satisfies the collapse-binding property, then it also satisfies prof-binding.*

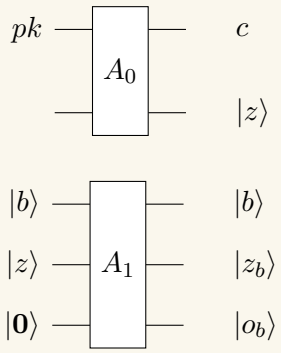
Proof. To prove that collapse binding implies prof binding, we will show a reduction where if the adversary breaks prof binding with some non negligible probability ϵ, the reduction breaks collapse-binding with some non negligibile probability $\mathcal{O}(\epsilon)$. Let the games for collapse-binding and sum-binding be defined as follows:



(a) Collapse-binding (b) Prof binding

Figure 1: Games for the two commitment schemes

The collapse binding game is exactly as defined in the class. For prof binding, the game is same as in the classical setting but the adversary can do quantum analysis on the same. The circuits A_0 and A_1 are defined as follows with z being a quantum state obtained by A_0 after calculating c and remaining terms having the same meaning.



The reduction is now defined as follows:

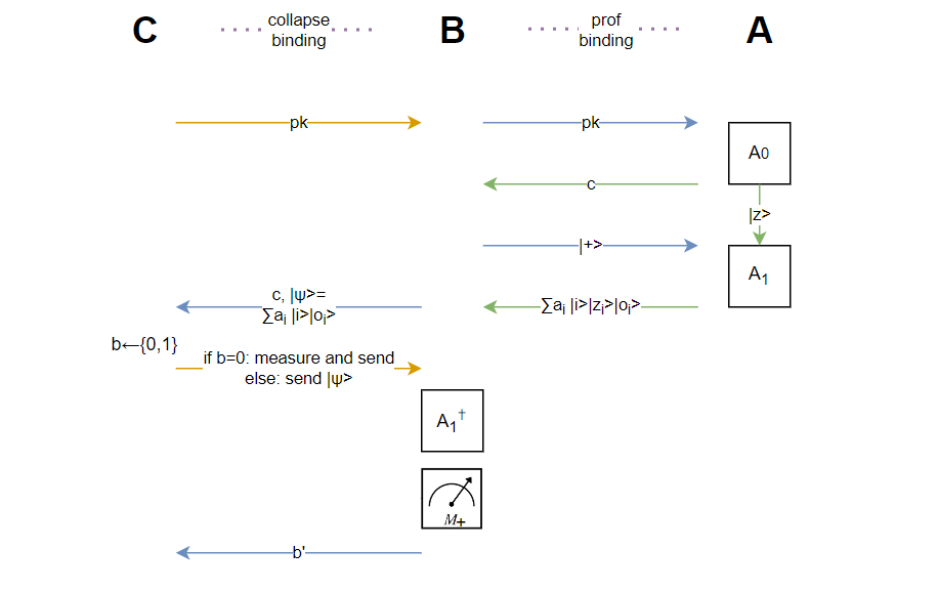


Figure 2: Reduction

The Reduction **B** has full access to the adversary **A** which breaks prof binding with non negligible probability ϵ. Reduction forwards the public key sent by the challenger (**C**) and then interacts with **A** to obtain a superposition $\sum_i \alpha_i |i\rangle |z_i\rangle |o_i\rangle$ where i can take values 0, 1. From this, **B** extracts the registers $|i\rangle$ and $|O_i\rangle$ to create $|\psi\rangle$ which is a super position of 0, 1 with their openings for the same commitment c. B forwards $c, |\psi\rangle$ to the challenger. Challenger checks the validity of the commitment and the openings. It then chooses a bit $b \leftarrow \{0,1\}$ and if $b = 0$, it measures $|\psi\rangle$ and sends it to **B**. Else it sends $|\psi\rangle$ without measuring. **B** now analyses and sends b' to **C** and succeeds with high probability.

B succeeds at identifying if $|\psi\rangle$ has been measure before as it applies $A_1^\dagger$ (since A_1 is a unitary, $A_1^\dagger$ exists) to $|\psi\rangle$. If $|\psi\rangle$ was not measure before, we get exactly the $|+\rangle$ state. On measuring it along the Hadamard basis, this is confirmed and **B** outputs $b' = 1$ which is true and hence succeeds with probability 1. On the other hand, if $|\psi\rangle$ was measure by **C**, we get either $|0\rangle |z_0\rangle |o_0\rangle$ state or $|1\rangle |z_1\rangle |o_1\rangle$ state, and on measuring using $\mathcal{M}_+$, we so not get the $|+\rangle$ state with probability 1/2. Therefore, in the case verification passes, **B** can distinguish measurement of $|\psi\rangle$ and hence break collapse-binding with probability $1/2 \times 1 + 1/2 \times 1/2 = 1/4$.
Probability of verification being successful directly depends on the advantage of the adversary **A** in the prof binding game. Following a similar notion as in Blum's protocol, assuming the verification passing is $\epsilon - good$,
$\Pr[\textbf{B}$ identifies b correctly $\mid$ verification is $\epsilon - good] = 3/4$
Therefore, if a Commit scheme satisfies the collapse-binding property, then it also satisfies prof-binding.

□

5 Question 5

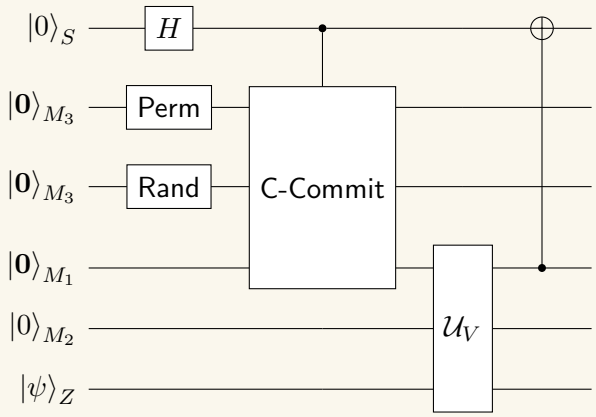
5.1 Question 5.1

Question 5.1

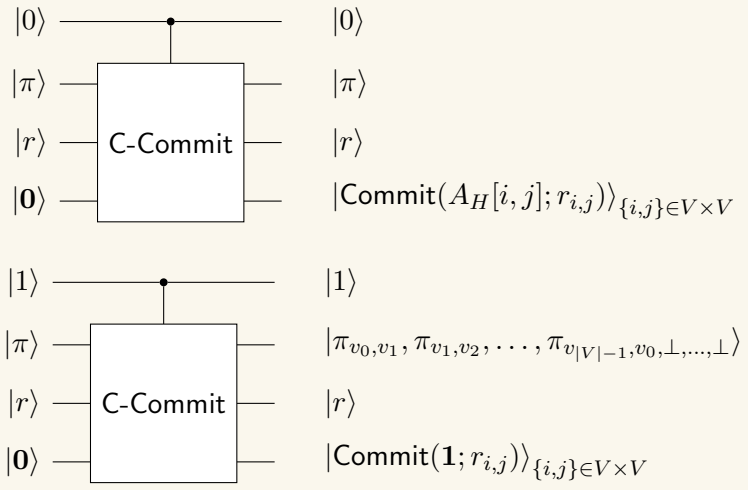
Question. *Similar to the graph-isomorphism protocol, construct a unitary* $\mathbf{Q}$ *for Blum's protocol such that,*

$$\mathbf{Q}\,|\mathbf{0}\rangle\,|\psi\rangle = \sqrt{p_\psi}\,|0\rangle\,|\psi_0\rangle + \sqrt{1-p_\psi}\,|1\rangle\,|\psi_1\rangle \tag{16}$$

Proof. Since the simulator (and prover) need to handle M_3 of different sizes, we define a register state (the register is of n qubits) as $\perp_n$ which corresponds to undefined. This is equivalent to having a register of $n+1$ qubits and the value in the last n registers is valid iff the first qubit is 1, else all the last n qubits have an invalid value. Now, we define the unitary $\mathbf{Q}$ as,



Here, H is the Hadamard gate, Perm creates a uniform superposition of all permutations on graph G with n vertices, Rand creates a uniform superposition for the randomness used by the commitment scheme (is effectively a Hadamard gate of appropriate size). The operator C-Commit takes in a control bit and two inputs (the message and the randomness) and stores the output in the third register. Depending on the control bit, it works as follows,



Note that the verifier cannot perform any computation on those registers that contain a $\perp$. This is simply possible in the case of a classical circuit by sending inputs of different sizes, however, since in the case of quantum circuits the input and output sizes are fixed. Since the circuit given has no measurement, it is a unitary of the form:

$$\mathbf{Q}\,|\mathbf{0}\rangle\,|\psi\rangle = \sqrt{p_\psi}\,|0\rangle_S\,|\psi_0\rangle + \sqrt{1-p_\psi}\,|1\rangle_S\,|\psi_1\rangle \tag{17}$$

□

5.2 Question 5.2

Question 5.2

Question. *Unlike the GI protocol, we cannot say that $p_\psi = 0.5$ for all $|\psi\rangle$. Prove that if $|p_\psi - 0.5|$ is non-negligible, then there exists a q.p.t. algorithm that can break computational hiding property of the commitment scheme.*

Proof. Consider a verifier V^* for which $p_\psi = 1/2 - \epsilon$ where ϵ is non-negligible. Intuitively, such a verifier is able to determine if the commitment was for a graph or for a string of all 1's and then sends the opposite bit with non-negligible success. We use the following algorithm to break the computational hiding property of the commitment scheme:

$\mathcal{A}$ that breaks computational hiding

1. $\mathcal{A}$ samples a random permutation π and sets $m_0 = A_{\pi(G)}$. It sets $m_1 = 1^{|A|}$. It forwards these messages to the hiding property challenger $\mathcal{C}$.
2. The adversary forwards the commitment that it receives from the challenger to $\mathcal{U}_{V^*}$ and receives the bit in register M_2. It measures this bit b' and it sends $1 - b'$ to the challenger.

Figure 3: Adversary that breaks computational hiding property of the commitment scheme using V^*

The interaction between the adversary $\mathcal{A}$ and the challenger using $\mathcal{U}_{V^*}$ can be represented as a quantum circuit similar to the circuit given in Question 5.1, with the only difference being that $|r\rangle$ is not sampled by $\mathcal{A}$ and the commitment is done by $\mathcal{C}$. Additionally, $\mathcal{A}$ flips the bit in register M_2. Also, the register S corresponds to the bit chosen by the challenger and the CNOT gate corresponds to the check done by the challenger for the adversary's input. Therefore, the winning probability of $\mathcal{A}$ will be $1/2 + \epsilon$.
Thus, the probability p_ψ must be negligibly close to $1/2$. □

5.3 Question 5.3

Question x: description

Question. *Use the above to prove that the simulator's output is computationally indistinguishable from the verifier's view in the real-world.*

Proof. Since $|p_\psi - 0.5|$ is negligible, we can bound the value of p_ψ between $1/2 - \mu$ and $1/2 + \mu$ where μ is negligible. Now, consider the following alternating projections on the starting state $|\mathbf{0}\rangle |\psi\rangle$ (we assume that ψ_b is a qubit of n bits and ψ is of m bits),

$$\begin{aligned} \mathbf{\Delta} &= (\mathbf{\Delta}_0 = |\mathbf{0}\rangle \langle \mathbf{0}| \otimes \mathbf{I}_m, \mathbf{I} - \mathbf{\Delta}_0) \\ \mathbf{\Pi} &= \left(\mathbf{\Pi}_0 = \mathbf{Q}^\dagger \cdot (|0\rangle \langle 0| \otimes \mathbf{I}_n) \cdot \mathbf{Q}, \mathbf{I} - \mathbf{\Pi}_0\right) \end{aligned} \tag{18}$$

Now, consider the t invariant sub-spaces $\{S_j\}_{j\in[t]}$ for $\mathbf{\Pi}, \mathbf{\Delta}$. Note that $|\mathbf{0}\rangle |\psi\rangle$ is an eigenvector for $\mathbf{\Delta}$ with eigenvalue 1. Thus, after applying $\mathbf{\Delta}$ we will either get $|\psi'\rangle = |\mathbf{0}\rangle |\psi\rangle$ or $|\psi'^{\perp}\rangle$ irrespective of which sub-space we are in. And since p_ψ is lower-bounded by $1/2 - \mu$, the probability of getting state $|0\rangle |\psi_0\rangle$ on applying $\mathbf{\Pi} \cdot \mathbf{\Delta}$ is at least $1/2 - \mu$ for any of the sub-spaces. On applying $\mathbf{\Delta} \cdot \mathbf{\Pi} \cdot \mathbf{\Delta}$ (assuming that we don't get a 0 on applying $\mathbf{\Pi}$), we will get $|\psi'\rangle$ with probability at least $(1/2 - \mu) \cdot (1/2 - \mu) = (1/2 - \mu)^2$ (again assuming the lower bound). Therefore, we can consider the transition probabilities to all be $1/2 - \mu$ (since it is the lower bound for all transitions). Note that in the above analysis, we treat each sub-space independently and show a bound on the transition probability. Thus, the probability of success after n rounds can be given by p_n, we get the following recurrence,

$$\begin{aligned} p_1 &\geq \frac{1}{2} - \mu \\ p_n &\geq p_{n-1} + (1 - p_{n-1}) \cdot \left(\frac{1}{2} - \mu\right) \\ &= \frac{p_{n-1}}{2} + \frac{1}{2} - \mu(1 - p_{n-1}) \\ &\geq \frac{p_{n-1} + (1 - 2\mu)}{2} \end{aligned} \tag{19}$$

On solving the recurrence, we get

$$\begin{aligned} p_n &\geq (1 - 2\mu) \cdot \left(1 - \frac{1}{2^{n-1}}\right) \\ &= 1 - \mu' \end{aligned}$$

□

Therefore, after a polynomial number of rounds, the simulator will succeed with probability close to 1.