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 $\mathcal{S} = (S_1, \dots, S_s)$ 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. □

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:

$$
\begin{aligned}
\mathbf{Q}_j \mathbf{P}_i &= \sum_{l \in T_j} |u_l\rangle \langle u_l| \sum_{k \in S_i} |v_k\rangle \langle v_k| \\
&= \left(\sum_{l \in T_j} \sum_{p} \alpha_{lp}^2 |v_p\rangle \langle v_p| \right) \left(\sum_{k \in S_i} |v_k\rangle \langle v_k| \right) \\
&= \sum_{l \in T_j} \sum_{k \in S_i} \left(\left(\sum_{p} \alpha_{lp}^2 |v_p\rangle \langle v_p| \right) |v_k\rangle \langle v_k| \right) \\
&= \sum_{l \in T_j} \sum_{k \in S_i} \alpha_{lk}^2 |v_k\rangle \langle v_k| \quad (\because \langle v_p | v_k\rangle = 0 \texttt{ if } p \neq k \texttt{ since orthogonal})
\end{aligned} \tag{6}
$$

Similarly, let $\mathbf{P}_i$ be represented in $\{|\mathbf{u}_i\rangle\}_i$ basis instead. Then, $\mathbf{P}_i\mathbf{Q}_j$ can be written as:

$$\begin{aligned}\mathbf{P}_i\mathbf{Q}_j &= \sum_{k\in S_i} |u_k\rangle\langle u_k| \sum_{l\in T_j} |v_l\rangle\langle v_l| \\ &= \sum_{l\in T_j}\sum_{k\in S_i} \alpha_{kl}^2 |v_l\rangle\langle v_l|\end{aligned} \tag{7}$$

In the case $\mathbf{Q}_j\mathbf{P}_i = \mathbf{P}_i\mathbf{Q}_j$, following can be noted:

$$\forall x \in S_i \cap T_j : \sum_{l\in T_j} \alpha_{lx}^2 = \sum_{k\in S_i} \alpha_{kx}^2 \tag{8}$$

And,

$$\begin{aligned}&\forall x \in S_i \cup T_j \setminus S_i \cap T_j : \sum_{l\in T_j} \alpha_{lx}^2 = 0 = \sum_{k\in S_i} \alpha_{kx}^2 \\ &\implies \forall l \in T_j, k \in S_i : \alpha_{lx} = 0 = \alpha_{kx}\end{aligned} \tag{9}$$

I forgot aage ka logic □

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} + $ **(I-P)**φ**(I-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

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

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,

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

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 $|w|^2|x|^2 \geq |w \cdot x|^2$ □

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 hast function family $\mathcal{H}'$ as

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

□

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 3.2

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

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

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,

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

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. *question*

Proof. proof □

4 Question 4

4.1 Question 4

Question x: description

Question. *question*

Proof. proof □

5 Question 5

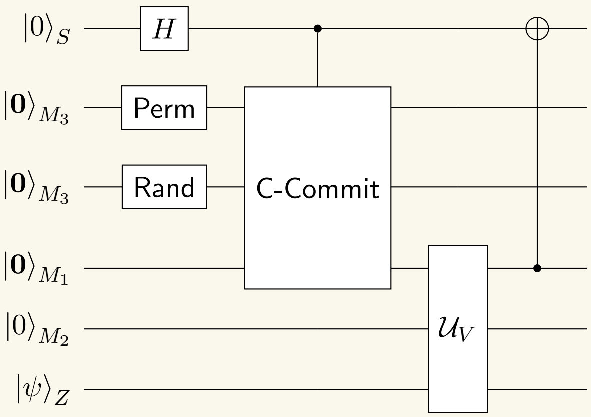
5.1 Question 5.1

Question 5.1

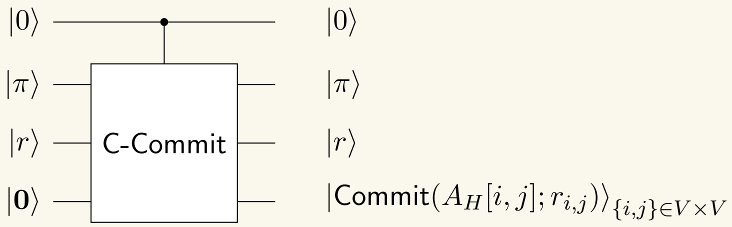
Question. *Similar to the graph-isomorphism protocol, construct a unitary* $\mathbf{Q}$ *for Blum's protocol such that,*

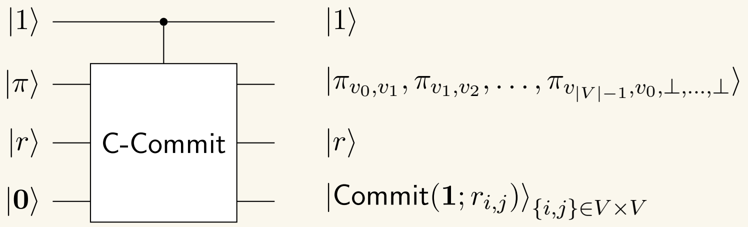
$$\mathbf{Q}\left|\mathbf{0}\right\rangle\left|\psi\right\rangle = \sqrt{p_\psi}\left|0\right\rangle\left|\psi_0\right\rangle + \sqrt{1-p_\psi}\left|1\right\rangle\left|\psi_1\right\rangle \tag{15}$$

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,





$|1\rangle$
$|\pi\rangle$
$|r\rangle$
$|\mathbf{0}\rangle$
C-Commit
$|1\rangle$
$|\pi_{v_0,v_1}, \pi_{v_1,v_2}, \ldots, \pi_{v_{|V|-1},v_0,\perp,\ldots,\perp}\rangle$
$|r\rangle$
$|\mathsf{Commit}(\mathbf{1};r_{i,j})\rangle_{\{i,j\}\in V\times V}$

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:

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

□

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 1: 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. *question*

Proof. proof □