COL872
Problem Set 1

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

January 2023

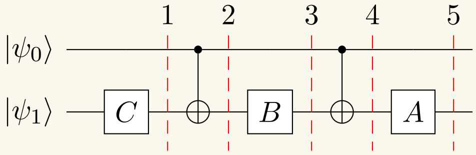
Contents

1 Question 1

Question 1

Question. *Let $U = A \cdot X \cdot B \cdot X \cdot C$ where $I = A \cdot B \cdot C$. Use this representation to construct a 'controlled U' gate using CNOT, and gates implementing the unitaries A, B, C.*

Proof. One implementation of controlled U gate using CNOT and the gates A, B and C is as follows:



To show that this works as Controlled U, We will show the Output in Second Register for Values 0 and 1 of $|\psi_0\rangle$.
When ψ_0 has a value of 0, at line 1, lower register has a value of $C\,|\psi_1\rangle$, After the CNOT, as the control is 0, the value remains unchanged at 2, At 3, the value of register becomes $B \cdot C\,|\psi_1\rangle$ which remains unchanged at 4 and finally at 5, the value becomes $A \cdot B \cdot C\,|\psi_1\rangle$. As $A \cdot B \cdot C = I$, the value becomes $I \cdot |\psi_1\rangle = |\psi_1\rangle$.

When ψ_0 has a value of 1, at line 1, lower register has a value of $C\,|\psi_1\rangle$, After the CNOT, as the control is 1, the value will change to $X \cdot C\,|\psi_1\rangle$ at point 2, At 3, the value of register becomes $B \cdot X \cdot C\,|\psi_1\rangle$ which changes to $X \cdot B \cdot X \cdot C\,|\psi_1\rangle$ at 4 via CNOT and finally at 5, the value becomes $A \cdot X \cdot B \cdot X \cdot C\,|\psi_1\rangle$. As $A \cdot X \cdot B \cdot X \cdot C = U$, the value becomes $U \cdot |\psi_1\rangle$.

Via this, we can say that the implementation of Controlled U gate above is indeed correct. □

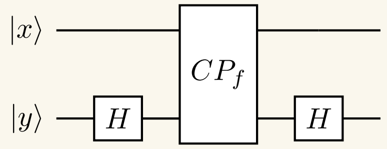
2 Question 2

2.1 Question 2.1

Question 2.1

Question. *Show that, for any* $f : \{0,1\}^n \to \{0,1\}$, U_f *can be implemented using* CP_f.

Proof. the implementation of U_f using CP_f is ans follows:



If the initial value of y is 0, after Hadamard, the qubit becomes $|+\rangle$. Applying CP_f on $|x\rangle|+\rangle$,

$$\begin{aligned} CP_f(|x\rangle|+\rangle) &= \frac{1}{\sqrt{2}}(CP_f|x\rangle|0\rangle + CP_f|x\rangle|1\rangle) \\ &= \begin{cases} |x\rangle|+\rangle & \text{if } f(x)=0 \\ |x\rangle|-\rangle & \text{if } f(x)=1 \end{cases} \end{aligned}$$

After applying Hadamard again, we get $\begin{cases} |x\rangle|0\rangle & \text{if } f(x)=0 \\ |x\rangle|1\rangle & \text{if } f(x)=1 \end{cases}$ which is equal to $|x\rangle|0 \oplus f(x)\rangle$ which is $U_f|x\rangle|0\rangle$.

If the initial value of y is 1, after Hadamard, the qubit becomes $|-\rangle$. Applying CP_f on $|x\rangle|-\rangle$,

$$\begin{aligned} CP_f(|x\rangle|-\rangle) &= \frac{1}{\sqrt{2}}(CP_f|x\rangle|0\rangle - CP_f|x\rangle|1\rangle) \\ &= \begin{cases} |x\rangle|-\rangle & \text{if } f(x)=0 \\ |x\rangle|+\rangle & \text{if } f(x)=1 \end{cases} \end{aligned}$$

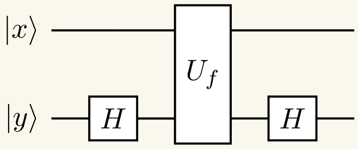
After applying Hadamard again, we get $\begin{cases} |x\rangle|1\rangle & \text{if } f(x)=0 \\ |x\rangle|0\rangle & \text{if } f(x)=1 \end{cases}$ which is equal to $|x\rangle|1 \oplus f(x)\rangle$ which is $U_f|x\rangle|1\rangle$. □

2.2 Question 2.2

Question 2.2

Question. *Show that, for any $f : \{0,1\}^n \to \{0,1\}$, CP_f can be implemented using U_f.*

Proof. the implementation of CP_f using U_f is ans follows:



If the initial value of y is 0, after Hadamard, the qubit becomes $|+\rangle$. Applying U_f on $|x\rangle|+\rangle$,

$$\begin{aligned} U_f(|x\rangle|+\rangle) &= \frac{1}{\sqrt{2}}(U_f|x\rangle|0\rangle + U_f|x\rangle|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle + |x\rangle|1 \oplus f(x)\rangle \\ &= |x\rangle|+\rangle \text{ ,for any value of f(x)} \end{aligned}$$

After applying Hadamard again, we get $|x\rangle|0\rangle$ which is equal to $CP_f|x\rangle|0\rangle$.
If the initial value of y is 1, after Hadamard, the qubit becomes $|1\rangle$. Applying U_f on $|x\rangle|1\rangle$,

$$\begin{aligned} U_f(|x\rangle|1\rangle) &= \frac{1}{\sqrt{2}}(U_f|x\rangle|0\rangle\, 1U_f|x\rangle|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle \\ &= \begin{cases} |x\rangle|-\rangle & \text{if } f(x) = 0 \\ -|x\rangle|-\rangle & \text{if } f(x) = 1 \end{cases} \\ &= CP_f|x\rangle|-\rangle \end{aligned}$$

After applying Hadamard again, we get $CP_f|x\rangle|1\rangle$.
Thus, using above circuit CP_f can be implemented using U_f.

□

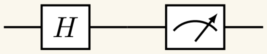
3 Question 3

3.1 Question 3.1

Question 3.1

Question. *Construct a single qubit quantum circuit such that it has identical output on $|0\rangle$ and $|1\rangle$, but different output on $|+\rangle$.*

Proof. Currently we do not know any unitary which gives same output on $|0\rangle$ and $|1\rangle$, so to achieve the objective, we will need to apply measurement. So we can create a circuit like



Now, when we put $|0\rangle$ as input, we get $|+\rangle$ from the Hadamard and we get $|-\rangle$ on inputting $|1\rangle$. As both of them have the same density matrix, we will get the same measurement from both of them.
While if we input $|+\rangle$ in the circuit, Hadamard gives us $|0\rangle$ as output which has a different density matrix from $|+\rangle$ and $|-\rangle$ and thus will give different measurement.
In this way we get the required circuit.

□

3.2 Question 3.2

Question 3.2

Question. *Show that any quantum circuit C operating on n qubits with m intermediate measurement gates can be perfectly simulated using a quantum circuit C' acting on $n+m$ qubits such that all measurements happen at the end of the computation.*

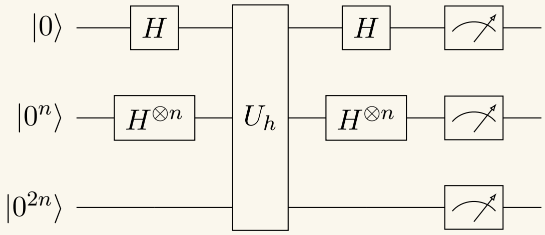
Proof. Circuit C has m measurements. Let's start with the first measurement. Suppose it happens on the qubit #q.
We initialize the $n+1^{th}$ qubit in the state $|0\rangle$. Now, instead of applying the first measurement, we can replace the measurement gate with a CNOT gate which has the control qubit as #q and target qubit as #(n+1) and measure this target qubit. Now we can move the measurement of the $n+1^{th}$ qubit at the end as this qubit collapses after measurement and is not needed in the circuit at any time. This is the correct simulataion of the original circuit at that time.
If there was something to be done with the result of measurement of qubit #q, we can modify the circuit to include a controlled U gate which takes as control the qubit #q with targets as the qubits which were getting affected according to the measurement of qubit #q. In this way we have reduced 1 measurement using 1 additional qubit.
This process can be replaced m times to get a circuit with n+m qubits which does not have any intermediate measurements. □

4 Question 4

Question 4

Question. *Design an efficient quantum algorithm for the 'Modified Simon's Problem'. Here, the algorithm is given oracle access to two functions $f_1 : \{0,1\}^n \to \{0,1\}^n$, $f_2 : \{0,1\}^n \to \{0,1\}^n$ with the guarantee that there exist a bit-string $s \in \{0,1\}^n$ such that for all $x \in \{0,1\}^n$, $f_1(x) = f_2(x \oplus s)$. The algorithm must output s with non-negligible probability, and can make $poly(n)$ queries to f_1, f_2. Describe the quantum circuit using unitaries U_{f_1},U_{f_2}.*

Proof. The quantum circuit that solves the problem can be described as follows:



Claim 4.1. *There exists an equivalent problem to solve as Simon's problem.*

Proof. Construct a function $h : \{0,1\} \times \{0,1\}^n \to \{0,1\}^{2n}$ such that $h(b,x) = f_{b+1}(x)||f_{2-b}(x)$

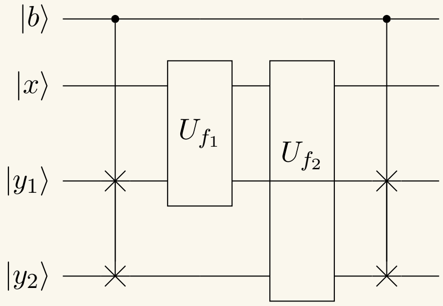
Now, let us look at $h(\bar{b}, x \oplus s)$ where $s \in \{0,1\}^n$ is a bit string s.t. for all $x \in \{0,1\}^n$, $f_1(x) = f_2(x \oplus s)$.

$$\begin{aligned} h(\bar{b}, x \oplus s) &= f_{(1-b)+1}(x \oplus s)||f_{2-(1-b)}(x \oplus s) \\ &= f_{2-b}(x)||f_{b+1}(x) \\ &= h(b,x) \end{aligned} \tag{1}$$

Here, $h(\bar{b}, x \oplus s)$ will be equal to $h(b,x)$ only when $f_1(x) = f_2(x \oplus s)$ holds for all x. Hence Modified Simon's Problem can be reduced to Simon's problem (note that if we have two x, x' such that $f_1(x) = f_1(x') \wedge f_2(x) = f_2(x')$ it won't be an issue similar to the case in Even-Mansour Cipher).

□

We now show a circuit using U_{f_1} and U_{f_2} that performs the working of U_h:



Claim 4.1 and the above oracle unitary clearly show the efficient algorithm for finding a solution to the modified Simon's problem by successfully reducing it to Simon's Problem. □

5 Question 5

5.1 Question 5.1

Question 5.1

Question. *Consider an operator that maps a matrix* $\mathbf{M} \in \mathbb{C}^{2\times 2}$ *to* $\frac{1}{4}(\mathbf{M} + \mathbf{X}\cdot\mathbf{M}\cdot\mathbf{X} + \mathbf{Z}\cdot\mathbf{M}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{M}\cdot\mathbf{Z}\cdot\mathbf{X}$.
What is the output when this operator is applied to $\mathbf{M} \in \{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X}\cdot\mathbf{Z}\}$*?*

Proof. The outputs for different values for M are as follows:

1. $\mathbf{M} = \mathbf{I}$

$$\begin{aligned} f(\mathbf{I}) &= \frac{1}{4}(\mathbf{I} + \mathbf{X}\cdot\mathbf{I}\cdot\mathbf{X} + \mathbf{Z}\cdot\mathbf{I}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{I}\cdot\mathbf{Z}\cdot\mathbf{X}) \\ &= \frac{1}{4}(\mathbf{I} + \mathbf{I} + \mathbf{I} + \mathbf{I}) \\ &= \mathbf{I} \end{aligned} \tag{2}$$

2. $\mathbf{M} = \mathbf{X}$

$$\begin{aligned} f(\mathbf{X}) &= \frac{1}{4}(\mathbf{X} + \mathbf{X}\cdot\mathbf{X}\cdot\mathbf{X} + \mathbf{Z}\cdot\mathbf{X}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{X}) \\ &= \frac{1}{4}(\mathbf{X} + \mathbf{X} - \mathbf{X} - \mathbf{X}) \\ &= \mathbf{0} \end{aligned} \tag{3}$$

3. $\mathbf{M} = \mathbf{Z}$

$$\begin{aligned} f(\mathbf{Z}) &= \frac{1}{4}(\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{X} + \mathbf{Z}\cdot\mathbf{Z}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{Z}\cdot\mathbf{Z}\cdot\mathbf{X}) \\ &= \frac{1}{4}(\mathbf{Z} - \mathbf{Z} + \mathbf{Z} - \mathbf{Z}) \\ &= \mathbf{0} \end{aligned} \tag{4}$$

4. $\mathbf{M} = \mathbf{X}\cdot\mathbf{Z}$

$$\begin{aligned} f(\mathbf{X}\cdot\mathbf{Z}) &= \frac{1}{4}(\mathbf{X}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{X} + \mathbf{Z}\cdot\mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{Z} + \mathbf{X}\cdot(\mathbf{Z}\cdot\mathbf{X}\cdot\mathbf{Z})\cdot\mathbf{Z}\cdot\mathbf{X}) \\ &= \frac{1}{4}(\mathbf{X}\cdot\mathbf{Z} + \mathbf{X}\cdot(-\mathbf{Z}) + (-\mathbf{X})\cdot\mathbf{Z} + \mathbf{X}\cdot(-\mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{X})) \\ &= \frac{1}{4}(\mathbf{X}\cdot\mathbf{Z} - \mathbf{X}\cdot\mathbf{Z} - \mathbf{X}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}) \\ &= \mathbf{0} \end{aligned} \tag{5}$$

□

5.2 Question 5.2

Question 5.2

Question. *Show that any density matrix $\rho \in \mathbb{C}^{2\times 2}$ can be expressed as a linear combination of $\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X}\cdot\mathbf{Z}$.*

Proof. The matrix representations of $\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X}\cdot\mathbf{Z}$ are as follows:

1. $\mathbf{I}: \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
2. $\mathbf{X}: \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
3. $\mathbf{Z}: \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
4. $\mathbf{X}\cdot\mathbf{Z}: \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

It can be clearly seen that $\{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X}\cdot\mathbf{Z}\}$ spans the entire $\mathbb{C}^{2\times 2}$ matrix space (We can obtain $e_{00}, e_{01}, e_{10}, e_{11}$ by simple addition, subtraction). Hence any density matrix $\rho \in C^{2\times 2}$ can be expressed as a linear combination of $\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X}\cdot\mathbf{Z}$ □

5.3 Question 5.3

Question 5.3

Question. *Suppose we encrypt a quantum state $|\psi\rangle$ using a random 2-bit key (a, b). The resulting density matrix is*
$\rho = \frac{1}{4}|\psi\rangle\langle\psi| + \mathbf{X}|\psi\rangle\langle\psi|\mathbf{X} + \mathbf{Z}|\psi\rangle\langle\psi|\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}|\psi\rangle\langle\psi|\mathbf{Z}\cdot\mathbf{X}$ *Using the above two parts, what can we conclude about ρ?*

Proof. Consider the density matrix of $|\psi\rangle$. It can be written as a linear combination of matrices in $\mathcal{M}$,

$$\begin{aligned} |\psi\rangle\langle\psi| &= \alpha_1\mathbf{I} + \alpha_2\mathbf{X} + \alpha_3\mathbf{Z} + \alpha_4\mathbf{X}\cdot\mathbf{Z} \\ &= \begin{bmatrix} \alpha_1+\alpha_3 & \alpha_2-\alpha_4 \\ \alpha_2+\alpha_4 & \alpha_1-\alpha_3 \end{bmatrix} \end{aligned} \tag{6}$$

From the fact that the density matrices have a trace $= 1$, we get that $\alpha_1 = 1/2$. Now consider the resultant density matrix after encrypting $|\psi\rangle$,

$$\begin{aligned}\rho &= \frac{1}{4} |\psi\rangle \langle\psi| + \mathbf{X} |\psi\rangle \langle\psi| \mathbf{X} + \mathbf{Z} |\psi\rangle \langle\psi| \mathbf{Z} + \mathbf{X} \cdot \mathbf{Z} |\psi\rangle \langle\psi| \mathbf{Z} \cdot \mathbf{X} \\ &= f(|\psi\rangle) \\ &= f(\alpha_1 \mathbf{I} + \alpha_2 \mathbf{X} + \alpha_3 \mathbf{Z} + \alpha_4 \mathbf{X} \cdot \mathbf{Z}) \\ &= \alpha_1 f(\mathbf{I}) + \alpha_2 f(\mathbf{X}) + \alpha_3 f(\mathbf{Z}) + \alpha_4 f(\mathbf{X} \cdot \mathbf{Z}) \text{ (since } f \text{ is a linear operator)} \\ &= \alpha_1 f(\mathbf{I}) = \frac{1}{2}\mathbf{I}\end{aligned} \tag{7}$$

Therefore, we get that the resultant density matrix is independent of $|\psi\rangle$ and therefore the proposed encryption scheme perfectly hides the qubit. □

5.4 Question 5.4

Question 5.4

Question. *The above encryption scheme can be extended to encrypt any m qubit state using $2m$ classical bits. Propose a public key encryption scheme that can encrypt any quantum state $|\psi\rangle$ (over m qubits, where m is unbounded). As in the classical setting, we will have only computational security, and the security depends on the key length. You don't need to prove security here.*

Proof. Consider the following quantum public-key encryption $\mathcal{E}_q$ (assuming that we there exists a classical public-key encryption scheme $\mathcal{E} = (\mathsf{KeyGen}_{\mathcal{E}}, \mathsf{Enc}_{\mathcal{E}}, \mathsf{Dec}_{\mathcal{E}})$,

$$\begin{aligned}\mathsf{KeyGen}_{\mathcal{E}_q}(1^m) &= \mathsf{KeyGen}_{\mathcal{E}}(1^{2m}) \\ \mathsf{Enc}_{\mathcal{E}_q}(pk, |\psi_1\rangle |\psi_2\rangle \cdots |\psi_m\rangle) &= (\mathsf{Enc}_{\mathcal{E}}(pk, r_1 || r_2 || \cdots || r_m), \\ &\quad \mathsf{Enc}(r_1, |\psi_1\rangle) \otimes \mathsf{Enc}(r_2, |\psi_2\rangle) \otimes \cdots \otimes \mathsf{Enc}(r_m, |\psi_m\rangle)) \\ &\quad (\forall i \in [m] : r_i \leftarrow \{0,1\}^2)\end{aligned} \tag{8}$$

We encrypt the random key using classical public-key encryption and then use this key to encrypt the qubits via the symmetric key encryption proposed in the question. □

6 Question 6

6.1 Question 6.1

Question 6.1

Question. *Let ρ be the density matrix for a mixed state over n qubits. In class, we saw that there exists a pure state $|\psi\rangle$ over $2n$ qubits such that measuring the last n qubits results in the density matrix ρ. Using Schmidt decomposition, prove that if $|\psi_1\rangle$ and $|\psi_2\rangle$ are two purifications of ρ, then there exists a unitary matrix $\mathbf{U}$ acting over n qubits such that $|\psi_2\rangle = (\mathbf{I}_n \otimes \mathbf{U})|\psi_1\rangle$. Here $\mathbf{I}_n$ is the identity operation over the first n qubits.*

Proof. Let,

$$\begin{aligned} |\psi_1\rangle &= \sum_i \lambda_{1i} |u_{1i}\rangle |v_{1i}\rangle \\ |\psi_2\rangle &= \sum_i \lambda_{2i} |u_{2i}\rangle |v_{2i}\rangle \end{aligned} \tag{9}$$

On measuring the last n qubits, we are left with,

$$\begin{aligned} \rho = \rho_1 &= \sum_i \lambda_{1i}^2 |u_{1i}\rangle \langle u_{1i}| \\ = \rho_2 &= \sum_i \lambda_{2i}^2 |u_{2i}\rangle \langle u_{2i}| \end{aligned} \tag{10}$$

Since $\{|u_{1i}\rangle\}_i$ and $\{|u_{2i}\rangle\}_i$ are orthonormal vectors, the two multi-sets $\{\lambda_{1i}\}_i$ and $\{\lambda_{2i}\}_i$ should be the same and they form the eigenvalues of ρ. Therefore, we can assume the ordering of $\{|u_{1i}\rangle\}_i$ and $\{|u_{2i}\rangle\}_i$ such that $\lambda_{1i} = \lambda_{2i} = \lambda_i$ (direct equality holds since λ_{bi} are guaranteed to be positive by Schmidt decomposition).
Now, we represent $|\psi_2\rangle$ such that the first n qubits have the same orthonormal vectors as $|\psi_1\rangle$. It is guaranteed that $|u_{1i}\rangle = |u_{2i}\rangle$ if the multiplicity of λ_i^2 is 1. Consider λ_p^2 such that it has a multiplicity $k > 1$. The two sets of eigenvectors corresponding to this eigenvalue are $S_1 = \{|u_{1i}\rangle \,|\lambda_i = \lambda_p\}$ and $S_2 = \{|u_{2i}\rangle \,|\lambda_i = \lambda_p\}$. Now, these two sets span the same subspace of n qubits. Therefore, we can write $\sum_{|u_{2i}\rangle \in S_2} |u_{2i}\rangle |v_{2i}\rangle$ as,

$$\begin{aligned} \sum_{|u_{2i}\rangle \in S_2} |u_{2i}\rangle |v_{2i}\rangle &= \sum_{|u_{2i}\rangle \in S_2} \left(\sum_{|u_{1j}\rangle \in S_1} \alpha_{ij} |u_{1j}\rangle \right) |v_{2i}\rangle \\ &= \sum_{|u_{2i}\rangle \in S_2} \left(\sum_{|u_{1j}\rangle \in S_1} |u_{1j}\rangle \alpha_{ij} |v_{2i}\rangle \right) \\ &= \sum_{|u_{1j}\rangle \in S_1} |u_{1j}\rangle \left(\sum_{|u_{2i}\rangle \in S_2} \alpha_{ij} |v_{2i}\rangle \right) \\ &= \sum_{|u_{1j}\rangle \in S_1} |u_{1j}\rangle |v'_{2j}\rangle \end{aligned} \tag{11}$$

Note that $\{|v'_{2j}\rangle \,|\lambda_j = \lambda_p\}$ is an orthonormal set since S_2 is also an orthonormal set. Therefore, $|\psi_2\rangle$ can be written as,

$$|\psi_2\rangle = \sum_i \lambda_i |u_{1i}\rangle |v'_{2i}\rangle = \sum_i \lambda_i |u_i\rangle |v'_{2i}\rangle \tag{12}$$

Now, since $\{|v_{1i}\rangle\}_i$ and $\{|v'_{2i}\rangle\}_i$ are both orthonormal sets, there exists a change of basis matrix (assuming that both sets span the entire set of n qubits, else, we can extend them to span the entire set), say $\mathbf{U}$. Therefore, we can write $|\psi_2\rangle$ in terms of $|\psi_1\rangle$ as,

$$|\psi_2\rangle = (\mathbf{I}_n \otimes \mathbf{U}) |\psi_1\rangle \tag{13}$$

This completes the proof. □

6.2 Question 6.2

Question 6.2

Question. *Let ρ_1, ρ_2 be two density matrices, corresponding to mixed states over n qubits. Show that the following two statements are equivalent:*

- *ρ_1 and ρ_2 have the same set of eigenvalues (counting multiplicities).*
- *There exists a pure state $|\psi\rangle$ over $2n$ qubits such that when the first n qubits are measured, the state of the remaining qubits is described by density matrix ρ_2. Similarly, when the last n qubits are measured, the state of the first n qubits is ρ_1.*

Proof. ($\implies$) Let the eigenvalues of ρ_1 and ρ_2 be $\{\lambda_i^2\}_i$ and the eigenvectors be $\{|u_i\rangle\}_i$ and $\{|v_i\rangle\}_i$ respectively. Now, consider the pure state,

$$|\psi\rangle = \sum_i \lambda_i |u_i\rangle |v_i\rangle \tag{14}$$

Therefore, on measuring the first n qubits, we get $\rho_2 = \sum_i \lambda_i^2 |v_i\rangle \langle v_i|$ and on measuring the last n qubits, we get $\rho_1 = \sum_i \lambda_i^2 |u_i\rangle \langle u_i|$. Therefore, we have shown the existence of a pure state $|\psi\rangle$ over $2n$ qubits which yields ρ_1 on measuring the last n qubits and ρ_2 on measuring the first n qubits.
($\impliedby$) Using Schmidt decomposition, we can represent $|\psi\rangle$ as $\sum_i \lambda_i |u_i\rangle \langle v_i|$. Now, on measuring the last n qubits, we get the density matrix $\rho_1 = \sum_i \lambda_i^2 |u_i\rangle \langle u_i|$ and on measuring the first n qubits, we get the density matrix as $\rho_2 = \sum_i \lambda_i |v_i\rangle \langle v_i|$. Now, since $\{|u_i\rangle\}_i$ and $\{|v_i\rangle\}_i$ are both orthonormal sets, the eigenvalues of ρ_1 and ρ_2 are both $\{\lambda_i\}_i$ (multi-set). Thus, ρ_1 and ρ_2 have the same set of eigenvalues. □

7 Question 7

7.1 Question 7.1

Question 7.1

Question. *Consider the partial measurement of the first qubit in an n qubit system. Express this partial measurement is as projective measurement.*

Proof. Consider the projective measurement,

$$\begin{aligned}\mathbf{P}_0 &= (|0\rangle\langle 0|) \otimes \mathbf{I}_{n-1} \\ \mathbf{P}_1 &= (|1\rangle\langle 1|) \otimes \mathbf{I}_{n-1}\end{aligned} \tag{15}$$

This $\{\mathbf{P}_i\}_{i\in[2]}$ is the projective measurement that is equivalent to the partial measurement of the first qubit in an n qubit system. Clearly, it satisfies the idempotence property and $\mathbf{P}_0 + \mathbf{P}_1 = \mathbf{I}_n$. Consider any pure state $|\psi\rangle = \alpha_0 |0\rangle |\phi_0\rangle + \alpha_1 |1\rangle |\phi_1\rangle$. Now, applying $\mathbf{P}_b$ on $|\psi\rangle$ gives,

$$\begin{aligned}\Pr[\text{first qubit} = b] &= \langle\psi|\mathbf{P}_b|\psi\rangle \\ &= \alpha_0^2 \langle\phi_0| \langle 0|\mathbf{P}_b|0\rangle |\phi_0\rangle + \alpha_1^2 \langle\phi_1| \langle 1|\mathbf{P}_b|1\rangle |\phi_1\rangle \\ &= \alpha_b^2 \langle\phi_b|\phi_b\rangle \\ &= \alpha_b^2\end{aligned} \tag{16}$$

The collapsed states are,

$$\begin{aligned}|\psi_b'\rangle &= \frac{\mathbf{P}_b |\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_b|\psi\rangle}} \\ &= \frac{((|b\rangle\langle b|) \otimes \mathbf{I}_{n-1}) (\alpha_0 |0\rangle \otimes |\psi_0\rangle + \alpha_1 |1\rangle \otimes |\psi_1\rangle)}{\alpha_b} \\ &= \frac{1}{\alpha_b} \cdot ((\alpha_0 |b\rangle\langle b| |0\rangle) \otimes |\psi_0\rangle + (\alpha_1 |b\rangle\langle b| |1\rangle) \otimes |\psi_1\rangle) \\ &= \frac{1}{\alpha_b} \cdot \alpha_b |b\rangle |\phi_b\rangle \\ &= |b\rangle |\phi_b\rangle\end{aligned} \tag{17}$$

These are exactly the same as the partial measurements. Therefore, the proposed $\{\mathbf{P}_i\}_{i\in[2]}$ is the projective measurement that corresponds to the partial measurement of the first qubit in an n qubit system. □

7.2 Question 7.2

Question 7.2

Question. *The measurements discussed in class have the following (collapsing) property: once the measurement is applied to an n-qubit system, the state collapses to one of $\{|x\rangle\}_{x\in\{0,1\}^n}$, and any further measurements produce the same measurement. Does this property hold true for projective measurements?*

Proof. From the idempotence property of $\mathcal{P}$, we get that any further measurements will produce the same measurement. However, it need not be the case that the state will collapse to one of $\{|x\rangle\}_{x\in\{0,1\}^n}$. For instance, consider the following projective measurement on 1 qubit system,

$$\mathbf{P}_0 = |+\rangle\langle+|\,, \mathbf{P}_1 = |-\rangle\langle-| \tag{18}$$

This satisfies the idempotence property and the sum of the two projections is equal to $\mathbf{I}_1$. However, consider the collapsed state on input $|0\rangle$ with $\mathbf{P}_0$,

$$\frac{\mathbf{P}_0|0\rangle}{\sqrt{\langle 0|\mathbf{P}_0|0\rangle}} = \frac{\frac{1}{\sqrt{2}}\cdot|+\rangle}{\frac{1}{\sqrt{2}}} = |+\rangle \tag{19}$$

This is neither $|0\rangle$ nor $|1\rangle$. Therefore, the state does not necessarily collapse to one of the possible bit-strings in case of a projective measurement. □

7.3 Question 7.3

Question 7.3

Question. *Let $\mathcal{M} = \{\mathbf{M}_i\}_{i\in[t]}$ be a POVM applied to an n qubit pure state $|\psi\rangle$. Show that there exists a projective measurement $\mathcal{P} = \{\mathbf{P}_i\}_{i\in[t]}$ on a larger system over $n + \log t$ qubits, and a pure state $|\psi'\rangle$ on $n + \log t$ qubits such that $\langle\psi|\mathbf{M}_i|\psi\rangle = \langle\psi'|\mathbf{P}_i|\psi'\rangle$ for all $i \in [t]$.*

Proof. We first show that each $\mathbf{M}_i$ can be represented as a matrix of the form $|\alpha_i|^2\mathbf{V}_i^\dagger\cdot\mathbf{V}_i$ for some matrix $\mathbf{V}_i$. Since all $\mathbf{M}_i$ are Hermitian and psd, we can represent them as $|\alpha_i|^2\sum_j\lambda_j|u_j\rangle\langle u_j|$ such that all $|u_j\rangle$ are orthonormal vectors and thus the previous representation follows (where $|\alpha_i|^2 = \mathsf{Tr}(\mathbf{M}_i)$). Now consider the following state $|\psi'\rangle$,

$$|\psi'\rangle = \sum_{i\in[t]}\alpha_i\mathbf{V}_i|\psi\rangle|i\rangle \tag{20}$$

□

Now, consider the following projective measurement $\mathcal{P}$,

$$\mathbf{P}_i = \mathbf{I}_n\otimes(|i\rangle\langle i|) \tag{21}$$

Consider the probability of getting output i,

$$\begin{aligned}\langle \psi' | \mathbf{P}_i | \psi' \rangle &= \sum_{j \in [t]} \langle \psi | \mathbf{V}_j^\dagger \alpha_j^* | \mathbf{I}_n | \alpha_j \mathbf{V}_j | \psi \rangle \cdot \langle j | (|i\rangle \langle i|) | j \rangle \\ &= \langle \psi | \mathbf{V}_i^\dagger \alpha_i^* | \mathbf{I}_n | \alpha_i \mathbf{V}_i | \psi \rangle \\ &= \langle \psi | |\alpha_i|^2 \mathbf{V}_i^\dagger \mathbf{V}_i | \psi \rangle \\ &= \langle \psi | \mathbf{M}_i | \psi \rangle \end{aligned} \tag{22}$$

Therefore, the probability of getting output i via the projective and the POVM is the same. Additionally, we require $\log t$ registers to store the values of i. Therefore, a POVM is a projective measurement on a larger space.