Soham Chatterjee
Email: sohamc@cmi.ac.in
Course: Quantum Algorithmic Thinking

Assignment - 1
Roll: BMC202175
Date: October 20, 2023

Problem 1

Find the eigenvectors, eigenvalues, and diagonal representations of the Pauli matrices.

Solution: Pauli matrices are

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix}\quad \sigma_x=\begin{bmatrix}0&1\\1&0\end{bmatrix}\quad \sigma_y=\begin{bmatrix}0&i\\-i&0\end{bmatrix}\quad \sigma_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$$

For I for all vectors v $Iv=v$. S0 every vector is an eigenvector and its eigenvalue is 1. Since I is already in its diagonal representation I's diagonal representation is I itself.

Since $\sigma_x\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}$ and $\sigma_x\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$ we have

$$\sigma_x\left(\begin{bmatrix}1\\0\end{bmatrix}+\begin{bmatrix}0\\1\end{bmatrix}\right)=\begin{bmatrix}0\\1\end{bmatrix}+\begin{bmatrix}1\\0\end{bmatrix}\quad \sigma_x\left(\begin{bmatrix}1\\0\end{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix}\right)=\begin{bmatrix}0\\1\end{bmatrix}-\begin{bmatrix}1\\0\end{bmatrix}=-\left(\begin{bmatrix}1\\0\end{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix}\right)$$

So the for the eignevalue 1 the corresponding eignevector is $\begin{bmatrix}1\\0\end{bmatrix}+\begin{bmatrix}0\\1\end{bmatrix}$ and for the eigenvalue -1 the corresponding eigenvalue is $\begin{bmatrix}1\\0\end{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix}$.

Since $\sigma_y\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\-i\end{bmatrix}$ and $\sigma_y\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}i\\0\end{bmatrix}$ we have

$$\sigma_y\left(\begin{bmatrix}1\\0\end{bmatrix}+i\begin{bmatrix}0\\1\end{bmatrix}\right)=\begin{bmatrix}0\\-i\end{bmatrix}+i\begin{bmatrix}i\\0\end{bmatrix}=-1\left(i\begin{bmatrix}0\\1\end{bmatrix}+\begin{bmatrix}1\\0\end{bmatrix}\right)\quad \sigma_y\left(\begin{bmatrix}1\\0\end{bmatrix}-i\begin{bmatrix}0\\1\end{bmatrix}\right)=\begin{bmatrix}0\\-i\end{bmatrix}-i\begin{bmatrix}i\\0\end{bmatrix}=-i\begin{bmatrix}0\\1\end{bmatrix}+\begin{bmatrix}1\\0\end{bmatrix}$$

So the for the eignevalue 1 the corresponding eignevector is $\begin{bmatrix}1\\0\end{bmatrix}-i\begin{bmatrix}0\\1\end{bmatrix}$ and for the eigenvalue -1 the corresponding eigenvalue is $\begin{bmatrix}1\\0\end{bmatrix}+i\begin{bmatrix}0\\1\end{bmatrix}$.

Since $\sigma_z\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$ and $\sigma_y\begin{bmatrix}0\\1\end{bmatrix}=-\begin{bmatrix}0\\1\end{bmatrix}$. So the for the eignevalue 1 the corresponding eignevector is $\begin{bmatrix}1\\0\end{bmatrix}$ and for the eigenvalue -1 the corresponding eigenvalue is $\begin{bmatrix}0\\1\end{bmatrix}$.

Now $\sigma_x,\sigma_y,\sigma_z$ has eigenvalues 1 and -1. So if we write in their corresponding eigenbasis then we will obtain the same diagonalized matrices where all the eigenvalues are in the diagonal positions i.e. $\begin{bmatrix}1&0\\0&-1\end{bmatrix}$

□

Problem 2

Show that a normal matrix is Hermitian if and only if it has real eigenvalues. Show that a positive operator is necessarily Hermitian.

Solution:

- Let A is normal and it is hermitian. Then $A=A^\dagger$. Let v be an eigenvector of A with eigenvalue λ. Then $v^\dagger Av=v^\dagger\lambda v=\lambda|v|^2$. Also $v^\dagger Av=v^\dagger A^\dagger v=(Av)^\dagger v=\lambda^\dagger v^\dagger v=\lambda^\dagger|v|^2$. So we have $\lambda=\lambda^\dagger$. Which implies λ is real. Hence all eigenvalues of A are real.

  For the opposite direction we need some lemmas.

Lemma 1. *The product of two unitary matrices is unitary*

Proof: Let U, V are two unitary matrices then $(UV)^\dagger = V^\dagger U^\dagger$. Now $(UV)(UV)^\dagger = U(VV^\dagger U^\dagger) = UIU^\dagger = I$. $\square$

Lemma 2. *If A is any square complex matrix then there is an upper triangular complex matrix T and a unitary matrix U so that $A = UTU^\dagger$*

Proof: Let A is a $n \times n$ matrix. Let v_1 be a eigenvector of A with the corresponding eigenvalue λ_1. We can take x_1 to be of unit length. Now by Gram-Schmidt process we can extend x_1 to an orthonormal basis $\{x_1, v_2, \dots, v_n\}$; Let $S_0 = \begin{bmatrix} x_1 & v_2 & \cdots & v_n \end{bmatrix}$ then S_0 is unitary and

$$S_0^\dagger A S_0 = \begin{bmatrix} \lambda_1 & * \\ 0 & A_1 \end{bmatrix}$$

where A_1 is an $(n-1) \times (n-1)$ matrix. Again suppose x_2 is an eigenvector of A_1 and the corresponding eigenvalue is λ_2. Then again for A_1 we extend x_2 to an orthonormal basis $\{x_2, \tilde{v}_2, \dots, \tilde{v}_{n-1}\}$ and take $\hat{S}_1 = \begin{bmatrix} x_2, \tilde{v}_2, \cdots, \tilde{v}_{n-1} \end{bmatrix}$ then S_1 is also unitary and we have $\hat{S}_1^\dagger A_1 \hat{S}_1 = \begin{bmatrix} \lambda_2 & * \\ 0 & A_2 \end{bmatrix}$ where A_2 is a $(n-2) \times (n-2)$ matrix. So we take $S_1 = S_0 \begin{bmatrix} 1 & 0 \\ 0 & \hat{S}_1 \end{bmatrix}$. Then

$$S_1^\dagger A S_1 = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \lambda_2 & * \\ 0 & 0 & A_2 \end{bmatrix}$$

We continue like this letting $S_k = S_{k-1} \begin{bmatrix} I_k & 0 \\ 0 & \hat{S}_k \end{bmatrix}$ thus at the end we obtain $U := S_n$ such that $U^\dagger A U = T$ which is an upper triangular matrix. Hence we have $A = UTU^\dagger$ $\square$

Lemma 3. *A matrix A is diagonalizable with a unitary matrix if and only if A is normal*

Proof: Let A is normal. Then by Lemma 2 there is a unitary matrix U and a upper traingular matrix T such that $A = UTU^\dagger$. Then

$$\begin{aligned} TT^\dagger &= U^\dagger A U (U^\dagger A U)^\dagger = U^\dagger A U U^\dagger A^\dagger U = U^\dagger A A^\dagger U \\ &= U^\dagger A^\dagger A U = U^\dagger A^\dagger U U^\dagger A U = (U^\dagger A U)^\dagger U^\dagger A U = T^\dagger T \end{aligned}$$

Now let $T = (t_{i,j})_{1 \le i,j \le n}$. Then the first diagonal entry of $TT^\dagger$ is

$$\sum_{i=1}^{n} t_{1,i} \overline{t_{1,i}} = \sum_{i=1}^{n} |t_{1,i}|^2$$

Now the first diagonal entry of $T^\dagger T$ is $t_{1,1}\overline{t_{1,1}} = |t_{1,1}|^2$. These two are equal. Hence for all $2 \le i \le n$ we have $t_{1,i} = 0$. Similarly comparing the second diagonal entry of $TT^\dagger$ and $T^\dagger T$ we have that all the nondiagonal entries of second row of T is 0. Continuing like this we have that T is diagonal. $\square$

- Suppose that A is any matrix such that there exists an unitary matrix U such that $U^\dagger AU = D$ where D is diagonal. Then

$$AA^\dagger = UDU^\dagger(UDU^\dagger)^\dagger = UDU^\dagger UD^\dagger U^\dagger = UDD^\dagger U^\dagger$$
$$= UD^\dagger DU^\dagger = UD^\dagger U^\dagger UDU^\dagger = (UDU^\dagger)^\dagger UDU^\dagger = A^\dagger A$$

So A is normal.

Now coming back to the original question we have that the eigenvalues of A are real. A is normal. Then there exists an unitary matrix U such that $U^\dagger AU = D$ where D is diagonal. Since all eigenvalues of A are real $D^\dagger = D$. Then we have

$$A^\dagger = (U^\dagger DU)^\dagger = U^\dagger D^\dagger U = U^\dagger DU = A$$

So A is hermitian

Now suppose A is positive operator. Then for all $v \in V$ we have

$$v^\dagger Av \geq 0 \implies v^\dagger Av = (v^\dagger Av)^\dagger = v^\dagger A^\dagger v \geq 0 \implies v^\dagger(A - A^\dagger)v = 0$$

Now also we have

$$(A - A^\dagger)(A - A^\dagger)^\dagger = (A - A^\dagger)(A^\dagger - A) = AA^\dagger - A^\dagger A^\dagger - AA + A^\dagger A$$
$$= (A^\dagger - A)(A - A^\dagger) = (A - A^\dagger)^\dagger(A - A^\dagger)$$

So $A - A^\dagger$ is a normal operator. Hence by Lemma 3 there exists an unitary matrix U such that $U^\dagger(A - A^\dagger)U = D$ where D is a diagonal matrix. Now for standard basis for any e_i

$$e_i^\dagger De_i = e^\dagger U^\dagger(A - A^\dagger)Ue_i = (Ue_i)^\dagger(A - A^\dagger)(Ue_i) = 0$$

Now $e_i^\dagger De_i$ is the i-th diagonal element of D which we got is 0. Since this is true for all $i \in [n]$ we have D is a null matrix. So

$$U^\dagger(A - A^\dagger)U = 0 \iff A - A^\dagger = U0U^\dagger = 0 \iff A = A^\dagger$$

Hence A is hermitian.

□

Problem 3

Suppose that A and B are Hermitian operators. Then show that the commutator $[A, B] = 0$ if and only if there exists an orthonormal basis such that both A and B are diagonal with respect to that basis.

Solution: If there exists an orthonormal basis such that both A and B are diagonal with respect to that basis then let we have $P^\dagger AP = D_A$ and $P^\dagger P - D_B$. Then

$$AB - BA = PD_AP^\dagger PD_BP^\dagger - PD_BP^\dagger PD_AP^\dagger = PD_AD_BP^\dagger - PD_BD_AP^\dagger = P(D_AD_B - D_BD_A)P^\dagger = 0$$

The last equality comes because D_A and D_B are diagonal matrices so $D_AD_B = D_BD_A$.

For the opposite direction suppose v be an eigenvector with corresponding eigenvector λ of A then $Av = \lambda v$. Now

$$A(Bv) = BAv = B\lambda v = \lambda Bv$$

Hence for any eigenvector v of A Bv is also an eigenvector and if Bv is zero then still it is an eigenvector of A for same eigenvalue.

Let $\lambda_1,\dots,\lambda_k$ be the eigenvalues of A. Then the corresponding eigenspaces of A are V_{λ_i} for $i\in[k]$. Then we have $B(V_{\lambda_i})\subseteq V_{\lambda_i}$ for all $i\in[k]$. Now let β be an eigenvalue of B with corresponding eigenvector is y. Then for any $i\in[k]$ we can think $y=y_1+y_2$ where $y_1\in V_{\lambda_i}$ and and $y_2\in\bigoplus_{j\neq i}V_{\lambda_j}$. Then $By=\beta y=\beta y_1+\beta y_2$. also we have $By=By_2+By_2$. Since $B(V_{\lambda_i})\subseteq V_{\lambda_i}$ and $B\left(\bigoplus_{j\neq i}V_{\lambda_j}\right)\subseteq\bigoplus_{j\neq i}V_{\lambda_j}$ we can say $By_1=\beta y_1$ and $By_2=\beta y_2$. Now if the V_β is the corresponding eigenspace fo the eigenvalue β then

$$V_\beta=\left[V_\beta\cap V_{\lambda_i}\right]\oplus\left[V_\beta\cap\bigoplus_{j\neq i}V_{\lambda_j}\right]=\bigoplus_{i=1}^{k}V_{\lambda_i}\cap V_\beta$$

Now if $\beta_1,\dots,\beta_l$ are the eigenvalues of B then we have

$$\bigoplus_{i=1}^{l}V_{\beta_i}=\bigoplus_{i=1}^{l}\left(\bigoplus_{j=1}^{k}V_{\lambda_j}\cap V_{\beta_i}\right)=\bigoplus_{\substack{1\le i\le l\\1\le j\le k}}V_{\beta_i}\cap V_{\lambda_j}$$

Let us denote $V_{i,j}=V_{\beta_i}\cap V_{\lambda_j}$ then for each $V_{i,j}$ we take an orthogonal basis for all i,j. Then taking union of all of them we have an orthogoanl basis for both A and B such that both A and B are diagonal. Now for each vector in the basis after normalizing we get an orthonormal basis such that both A and B are diagonal with respect to that basis.

$\square$

Problem 4

Prove that a state $|\psi\rangle$ of a composite system AB is a product state if and only if it has Schmidt number 1. Prove that $|\psi\rangle$ is a product state if and only if the reduced density matrices ρ_A and ρ_B are pure states.

Solution:

- Let the $|\psi\rangle$ is a product state. Then $\exists\ |\psi_1\rangle\in A,|\psi_2\rangle\in B$ such that $|\psi\rangle=|\psi_1\rangle|\psi_2\rangle$. Now by Schmidt Decomposition there exists an orthonormal basis $\{|i_A\rangle\}$ for system A and orthonormal basis $\{|i_B\rangle\}$ for system B such that

$$|\psi\rangle=\sum_{i=1}^{n}\lambda_i|i_A\rangle|i_B\rangle$$

where $\lambda_i\in\mathbb{R}$ such that $\sum_{i=1}^{n}\lambda_i^2=1$. We have there exists at least one $\lambda_i\neq0$. WLOG $\lambda_1\neq0$ Now we also have

$$|\psi_1\rangle=\sum_{i=1}^{n}\lambda_{i,A}|i_A\rangle\qquad|\psi_2\rangle=\sum_{i=1}^{n}\lambda_{i,B}|i_B\rangle$$

then we have

$$\sum_{i=1}^{n}\lambda_i|i_A\rangle|i_B\rangle=|\psi\rangle=\left(\sum_{i=1}^{n}\lambda_{i,A}|i_A\rangle\right)\left(\sum_{i=1}^{n}\lambda_{i,B}|i_B\rangle\right)=\sum_{1\le i,j\le n}\lambda_{i,A}\lambda_{j,B}|i_A\rangle|j_B\rangle$$

Comparing the coefficients we have $\lambda_i=\lambda_{i,A}\lambda_{i,B}$ and for all $\lambda_{i,A}\lambda_{j,B}=0$ where $i\neq j$. Since $\lambda_1\neq0$ we have $\lambda_{1,A},\lambda_{1,B}\neq0$. Since for all $j\neq1$, $\lambda_{1,A}\lambda_{j,B}=0$ we have $\lambda_{j,B}=0$ for all $2\le j\le n$. Similarly since for all $i\neq1$, $\lambda_{i,A}\lambda_{1,B}=0$ we have $\lambda_{i,A}=0$ for all $2\le i\le n$. So we have $\lambda_i=0$ for all $2\le i\le n$. So $|\psi\rangle=\lambda_1|i_A\rangle|i_B\rangle$. Hence $|\psi\rangle$ has Schmidt Number 1.

For the opposite direction $|\psi\rangle$ has Schmidt Number 1. So $|\psi\rangle=|i_A\rangle|i_B\rangle$ Here are $|i_A\rangle$ is a state of system A and $|i_B\rangle$ is a state of system B. Hence $|\psi\rangle$ is already in a product state. Hence $|\psi\rangle$ is a product state of the composite system AB.

- $|\psi\rangle$ is a product state. Hence it has Schmidt Number 1. So there exists an orthonormal basis $\{|i_A\rangle\}$ for system A and orthonormal basis $\{|i_B\rangle\}$ for system B such that $|\psi\rangle = |i_A\rangle|i_B\rangle$. Then

$$\rho_{AB} = |\psi\rangle\langle\psi| = (|i_A\rangle|i_B\rangle)(\langle i_A|\langle i_B|) = |i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|$$

Now

$$\rho_A = tr_B(\rho_{AB}) = tr_B(|i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|) = |i_A\rangle\langle i_A| \, tr(|i_B\rangle\langle i_B|) = |i_A\rangle\langle i_A|$$

and similarly

$$\rho_B = tr_A(\rho_{AB}) = tr_A(|i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|) = tr(|i_A\rangle\langle i_A|)\,|i_A\rangle\langle i_B| = |i_B\rangle\langle i_B|$$

So ρ_A and ρ_B are pure states.

Let ρ_A and ρ_B are pure states. Let $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$ Then

$$|\psi\rangle\langle\psi| = \left(\sum_{i=1}^{n} \lambda_i |i_A\rangle|i_B\rangle\right)\left(\sum_{j=1}^{n} \lambda_j \langle j_A|\langle j_B|\right) = \sum_{i=1}^{n} \lambda_i^2 |i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|$$

There exists at least one $\lambda_i \neq 0$. WLOG $\lambda_1 =\neq 0$. Now

$$\rho_A = \mathrm{tr}_B\left(\sum_{i=1}^{n} \lambda_i^2 |i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|\right) = \sum_{i=1}^{n} \lambda_i^2 |i_A\rangle\langle i_A| \, tr(|i_B\rangle\langle i_B|) = \sum_{i=1}^{n} \lambda_i^2 |i_A\rangle\langle i_A|$$

and

$$\rho_B = \mathrm{tr}_A\left(\sum_{i=1}^{n} \lambda_i^2 |i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|\right) = \sum_{i=1}^{n} \lambda_i^2 tr(|i_A\rangle\langle i_A|)\,|i_B\rangle\langle i_B| = \sum_{i=1}^{n} \lambda_i^2 |i_B\rangle\langle i_B|$$

Since ρ_A and ρ_B are pure states there exists $k, l \in [n]$ such that $\rho_A = \lambda_k |k_A\rangle\langle k_A|$ and $\rho_B = \lambda_l |l_B\rangle\langle l_B|$ since we already know that $\lambda_1 \neq 0$ we have $k = l = 1$ for all $2 \leq i \leq n$ $\lambda_i = 0$. So $\rho_A = |1_A\rangle\langle 1_A|$ and $\rho_B = |1_A\rangle\langle 1_B|$. Hence $|\psi\rangle = \lambda_1 |1_A\rangle|1_B\rangle$. So $|\psi\rangle$ has Schmidt Number 1. So $|\psi\rangle$ is a product state of the composite system AB.

□

Problem 5

Write a self-contained proof that single qubit gates and $CNOT$ gates are universal.

Solution:

Lemma 4. *Let U be an unitary matrix acting on $\mathbb{C}^d$. Then there are $N \leq \frac{d(d-1)}{2}$, 2-level unitary matrices i.e. unitary matrices which act on 2 or less dimensional subspaces $U_1, \ldots, U_n$ such that*

$$U_N U_{N-1} \cdots U_2 U_1 U = I$$

.

Proof: We will prove this by induction. Let $d = 3$. Then suppose $U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$. Then first take

$$U_1 = \begin{bmatrix} \frac{a^*}{|a|^2+|b|^2} & \frac{b^*}{|a|^2+|b|^2} & 0 \\ \frac{b}{|a|^2+|b|^2} & \frac{-a}{|a|^2+|b|^2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \implies U_1 U = \begin{bmatrix} 1 & d' & g' \\ 0 & e' & h' \\ c' & f' & i' \end{bmatrix} = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & i' \end{bmatrix}$$

Now we take

$$U_2 = \begin{bmatrix} \frac{a'^*}{|a'|^2+|c'|^2} & 0 & \frac{c'^*}{|a'|^2+|c'|^2} \\ 0 & 1 & 0 \\ \frac{c'}{|a'|^2+|c'|^2} & 0 & \frac{-a'}{|a'|^2+|c'|^2} \end{bmatrix} \implies U_2 U_1 U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & i'' \end{bmatrix}$$

Clearly U_1 and U_2 are unitary matrix. Hence U_2U_1U is unitary matrix. Since U_2U_1U is a unitary matrix and $(U_2U_1U)^\dagger = U_2U_1U$ we have $d'' = g'' = 0$. Hence

$$U_2U_1U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & i'' \end{bmatrix}$$

So we will take

$$U_3 = (U_2U_1U)^\dagger = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & h''^* \\ 0 & f''^* & i''^* \end{bmatrix}$$

Hence $U_3U_2U_1U = I \implies U = U_1^\dagger U_2^\dagger U_3^\dagger$.

Now suppose this statement is true for $d-1$. For d like the above process we need $d-1$ unitary matrices to make the first entry of the first column 1 and the rest entries of the first column to be 0. Let the unitary matrices are $U_1, \ldots, U_{d-1}$. So $U_{d-1}\cdots U_1U = \begin{bmatrix} 1 & 0 \\ 0 & U' \end{bmatrix}$ where U' is a $(d-1)\times(d-1)$ matrix. Since U is unitary we have U' is unitary. By induction hypothesis there exists $k \le \frac{(d-1)(d-2)}{2}$ matrices $U_1', \ldots, U_k'$ such that $U_k'\cdots U_1'U' = I_{d-1}$. Now $\forall\ i \in [k]$ we take the matrices

$$\tilde{U}_i = \begin{bmatrix} 1 & 0 \\ 0 & U_i' \end{bmatrix}$$

Then we have

$$\left(\tilde{U}_k \cdots \tilde{U}_1\right)\left(U_{d-1}\cdots U_1\right)U = I_d$$

Now

$$k + d - 1 \le \frac{(d-1)(d-2)}{2} + d - 1 = \frac{d-1}{2}(d-2+2) = \frac{d(d-1)}{2}$$

Hence there exists $N \le \frac{d(d-1)}{2}$ unitary matrices $U_1, \ldots, U_N$ such that ${}_N \cdots U_1U = I$. □

Now if U is an unitary matrix acting on a $n-$qubit system then we can decompose U into product of 2-level unitary matrices using the previous lemma. So it is enought to see 2-level unitary matrices. Now denote U to be a 2-level matrix on an n-qubit system. Suppose U acts non-trivially on the space spanned by the computational basis $\{|x\rangle, |y\rangle\}$. where $bin(x) = x_{n-1}\cdots x_0$ and $bin(y) = y_{n-1}\cdots y_0$ are the binar expressions for x, y where $\forall\ i, j \in [n]$ we have $x_i, y_j \in \{0, 1\}$. Let $U|x\rangle = a|x\rangle + b|y\rangle$ and $U|y\rangle = c|x\rangle + d|y\rangle$. Therefore U is an $2^n \times 2^n$ matrix where U has 1 in all diagonal positions and 0 in all off diagonal positions except $U_{xx} = a, U_{xy} = c, U_{yx} = b, U_{yy} = d$. Take $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$. Now we will try to reduce U to $\tilde{U}$ using single qubit gates and $CNOT$ gate. $\tilde{U}$ can be thought of as a unitary matrix acting on a single qubit.

To reduce U to $\tilde{U}$ we first take s sequence of binary numbers $\{a_1, \ldots, a_m\}$ such that $a_1 = x$ and $a_m = y$ and for any $i \in [m-1]$, a_i, a_{i+1} differ in exactly one bit. Clearly $m \le n+1$ since there are n bits. Our main strategy is to find gates providing the sequence of state changes

$$|x\rangle = |x_1\rangle \to |x_2\rangle \to \cdots \to |x_{m-1}\rangle$$

then $|x_{m-1}\rangle$ and $|x_m\rangle = |y\rangle$ differs in only one position and then apply $\tilde{U}$ on that specific bit position and then undo the sequence so that

$$|x\rangle = |x_1\rangle \leftarrow |x_2\rangle \leftarrow \cdots \leftarrow |x_{m-1}\rangle$$

Now to change the state $|x_i\rangle \to |x_{i+1}\rangle$ let $x_i = x_{i,n-1}\cdots x_{i,0}$ and the difference of x_i and x_{i+1} is at jth position. Then

$$x_{i+1} = x_{i,n-1}\cdots x_{i,j+1}\overline{x_{i,j}}x_{i,j-1}\cdots x_{i,0}$$

Then we apply $C^{n-1}(X)$ on jth bit along with sandwitching by X gate at lth bit, $l \ne j$ if $x_{i,l} = 0$. Thus jth bit is changed only if the other bits are equal to $|x_i\rangle$ state's bits in their respective positions. Lets denote the gate $C_i^n(X)$ for the change of state $|x_i\rangle \to |x_{i+1}\rangle$. We apply this this for all $i \in [m-2]$ to finaly get $|x_{m-1}\rangle$

Now let x_{m-1} and $x_m = y$ differs in kth position. Let $x_{m-1} = x_{m-1,n-1} \cdots x_{m-1,0}$ then

$$x_m = x_{m-1,n-1} \cdots x_{m-1,k+1}\overline{x_{m-1,k}}x_{m-1,k-1} \cdots x_{m-1,0}$$

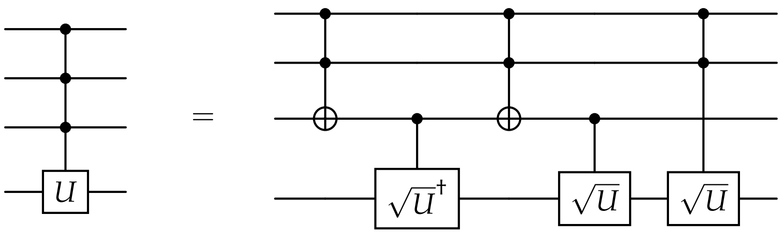
Then we apply $C^{n-1}(\tilde{U})$ where $\tilde{U}$ is applied in k-th position along with sandwitching by X gates if at lth bit, $l \neq k$ if $x_{m-1,l} = 0$. Thus $\tilde{U}$ is applied to kth bit only if the rest of the bits are equal to $x_{m-1,n-1}, \ldots, x_{m-1,k+1}$, $x_{m-1,k-1}, \ldots, x_{m-1,0}$ respectively.

Lemma 5. *For any unitary matrix U there is an unitary matrix V such that $V^2 = U$.*

Proof: Since $UU^\dagger = I$ we also have $U^\dagger U = (UU^\dagger)^\dagger = I^\dagger = I$. Hence unitary matrix is normal. Now by Lemma 3 we know normal matrices are diagonalizable. So there is a unitary matrix V such that $V^\dagger UV = D$ where D is diagonal. Since all elements of D are complex number for all diagonal element of D there is a square root of that element. Hence we construct a new diagonal matrix $\tilde{D}$ such that square of any diagonal element of $\tilde{D}$ is the same element of D of smae diagonal position. SO $\tilde{D}\tilde{D} = D$. Hence we take $\sqrt{U} = V\tilde{D}V^\dagger$. Then $\sqrt{U}\sqrt{U} = V\tilde{D}V^\dagger V\tilde{D}V^\dagger = V\tilde{D}\tilde{D}V^\dagger = VDV^\dagger = U$. Hence such matrix exists □

Lemma 6. *For any unitary gate U acting on a single qubit system $C^n(U)$ gate on a n qubit system can be constructed by 3 $C^{n-1}(V)$ and 3 $C(W)$ gates where V, W are unitary matrices. [I took this idea from algoassert.com]*

Proof: We will prove drawing the circuit for $n = 3$.



There are 4 cases arise:

1. **OFF, OFF**: If any of the first 2 states is $|0\rangle$ and the 3rd state is $|0\rangle$ then no gate is applied on the 4th state.
2. **ON, OFF**: If first 2 states are $|1\rangle$ and the 3rd state is $|0\rangle$ then after the first $C^2(X)$ gate the 3rd state becomes $|1\rangle$ so the $\sqrt{U}^\dagger$ is applied on 4th state and after the second $C^2(X)$ the 3rd state becomes $|0\rangle$ so only the last $\sqrt{U}$ is applied on 4th state. But we know $\sqrt{U}^\dagger\sqrt{U} = I$ so in the end nothing changes
3. **ON, ON**: If first 2 states are $|1\rangle$ and 3rd state is $|1\rangle$ then after the first $C^2(X)$ gate the 3rd state becomes $|0\rangle$ so the $\sqrt{U}^\dagger$ is not applied on 4th state and after the second $C^2(X)$ the 3rd state becomes $|1\rangle$ so both the last two $\sqrt{U}$ gate are applied on 4th state. Since $\sqrt{U}\sqrt{U} = U$ we can say when all the first 3 states are $|1\rangle$ U is applied to the 4th state.
4. **OFF, ON**: If any of the first 2 states is $|0\rangle$ and the 3rd state is $|1\rangle$ then after the first $C^2(X)$ gate the 3rd state doesn't change so it remains $|1\rangle$ so the $\sqrt{U}^\dagger$ is applied on 4th state and after the second $C^2(X)$ the 3rd state still remains $|1\rangle$ so the first $\sqrt{U}$ gate is applied but the last $\sqrt{U}$ iis not applied since at least one of the first 2 states is $|0\rangle$

We will implement the same for any n. Here we are using 2 $C^{n-1}(X)$ gate one $C^{n-1}(\sqrt{U})$ gate and one $C(\sqrt{U})$ and one $C(\sqrt{U}^\dagger)$ gate. So the lemma is true. □

With this lemma we can constuct a $C^n(U)$ gate using 2 $C^{n-1}(X)$ gate one $C^{n-1}(\sqrt{U})$ gate and one $C(\sqrt{U})$ and one $C(\sqrt{U}^\dagger)$ gate. So applying this procedure again and again we can finally reach where we are using only $C(V)$ gates where V is an unitary gate acting on a single qubit.

Let $SU(n)$ define the set of all $n \times n$ unitary matrices with determinant 1.

Lemma 7. *$\forall\, U \in SU(2)$ there exists $a, b \in \mathbb{C}$ and $\theta \in \mathbb{R}$ with $|a|^2 + |b|^2 = 1$ such that*

$$U = \begin{bmatrix} a & b \\ -b^* e^{i\theta} & a^* e^{i\theta} \end{bmatrix}$$

Proof: Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. We know $U^\dagger = U^{-1}$. Now

$$U^{-1} = \frac{1}{\det U} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \qquad U^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$$

So we have

$$d = a^* \det U, a = d^* \det U, \text{ and } -b = c^* \det U$$

So we have $d = d(\det U)^* \det U = d|\det U|$. So if $d \neq 0$ we have $|\det U| = 1 = (\det\{U\})^* \det U = \det U^\dagger \det U = \det(UU^\dagger)$. So we can think $\det U = e^{i\theta}$ So we have

$$d = a^* e^{i\theta} \qquad c = -b^* e^{i\theta}$$

Hence $U = \begin{bmatrix} a & b \\ -b^* e^{i\theta} & a^* e^{i\theta} \end{bmatrix}$. Now

$$\det U = aa^* e^{i\theta} + bb^* e^{i\theta} = e^{i\theta}(|a|^2 + |b|^2) \implies |\det U| = 1 = |e^{i\theta}|(|a|^2 + |b|^2) = |a|^2 + |b|^2$$

□

Now since $|a|^2 + |b|^2 = 1$ so we can think $|a| = \sin\theta$ and $|b| = \cos\theta$. So $a = e^{i\lambda}\sin\theta$ and $b = e^{i\mu}\cos\theta$. So

$$U = \begin{bmatrix} e^{i\lambda}\sin\theta & e^{i\mu}\cos\theta \\ -e^{i(\theta-\mu)}\cos\theta & e^{i(\theta-\lambda)} \end{bmatrix} = e^{i\frac{\theta}{2}} \begin{bmatrix} e^{i(\lambda-\frac{\theta}{2})}\sin\theta & e^{i(\mu-\frac{\theta}{2})}\cos\theta \\ -e^{-i(\mu-\frac{\theta}{2})}\cos\theta & e^{-i(\lambda-\frac{\theta}{2})}\sin\theta \end{bmatrix}$$

So we take $\alpha = \lambda - \frac{\theta}{2}$ and $\beta = \mu - \frac{\theta}{2}$. Now introduce $\alpha = \phi + \psi$ and $\beta = \phi - \psi$. Then we have

$$U = e^{i\frac{\theta}{2}} \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix} \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{bmatrix} \begin{bmatrix} e^{i\psi} & 0 \\ 0 & e^{-i\psi} \end{bmatrix}$$

Now for any 2×2 matrix A and for any element x we have $xA = (xI)A$. So here we can take the multiplication of $e^{i\frac{\theta}{2}}$ as multiplication of the matrix $e^{i\frac{\theta}{2}} I = \Phi(\frac{\theta}{2})$. To write in short we will take $\frac{\theta}{2} = \omega$. So $\Phi(\frac{\theta}{2}) = \Phi(\omega)$. Now for any angle γ we know

$$R_z(\gamma) = \begin{bmatrix} e^{i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{bmatrix} \qquad R_y(\gamma) = \begin{bmatrix} \cos\frac{\gamma}{2} & \sin\frac{\gamma}{2} \\ -\sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}$$

Since $\cos\gamma = \sin\left(\frac{\pi}{2} - \gamma\right)$ we have

$$R_z(2\phi) = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix} \quad R_y(\pi - 2\theta) = \begin{bmatrix} \cos\frac{\pi-2\theta}{2} & \sin\frac{\pi-2\theta}{2} \\ -\sin\frac{\pi-2\theta}{2} & \cos\frac{\pi-2\theta}{2} \end{bmatrix} = \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{bmatrix} \quad R_z(2\psi) = \begin{bmatrix} e^{i\psi} & 0 \\ 0 & e^{-i\psi} \end{bmatrix}$$

Hence $U = \Phi(\omega) R_z(2\phi) R_y(\pi - 2\theta) R_z(2\psi)$. Now we need to break $C(U)$ into single qubit gates and $CNOT$ gate.

Lemma 8. *Let $U \in SU(2)$ then there exists $A, B, C \in SU(2)$ such that $U = \Phi(\delta) AXBXC$ where $ABC = I$ and $X = \sigma_x$ for some $\delta \in \mathbb{R}$*

Proof: By the previous construction there exists $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that $U = \Phi(\delta)R_z(\alpha)R_y(\beta)R_z(\gamma)$. Now take

$$A = R_z(\alpha)R_y\left(\frac{\beta}{2}\right), \quad B = R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right), \quad C = R_z\left(-\frac{\alpha-\gamma}{2}\right)$$

Then

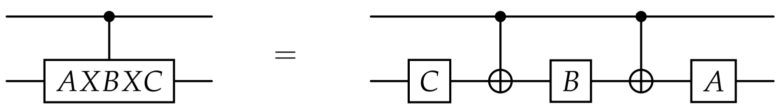
$$\begin{aligned}
AXBXC &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)XR_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)XR_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)\left[XR_y\left(-\frac{\beta}{2}\right)X\right]\left[XR_z\left(-\frac{\alpha+\gamma}{2}\right)X\right]R_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(\frac{\beta}{2}\right)R_z\left(\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y(\beta)R_z(\gamma)
\end{aligned}$$

We also need to verify that $ABC = I$. For that

$$ABC = R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) = R_z(\alpha)R_y(0)R_z(-\alpha) = R_z(\alpha)R_z(-\alpha) = I$$

$\square$

We know if U_1 and U_2 are two unitary gates acting on a single qubit then $C(U_1U_2) = C(U_1)C(U_2)$. Hence $C(U) = C(\Phi(\delta))C(AXBXC)$. Now we can impliment $C(AXBXC)$ where $ABC = I$ like this



So if the control state is $|0\rangle$ then $ABC = I$ is applied on the 2nd state but nothing changes. If the control state is $|1\rangle$ then $AXBXC$ is applied on the 2nd state. Now we will try to simulate $C(\Phi(\delta))$.

Lemma 9. *For any $\Phi(\delta)$ gate where $\delta \in \mathbb{R}$) Take*

$$D = R_z(-\delta)\Phi\left(\frac{\delta}{2}\right)$$

then $C(\Phi(\delta)) = D \otimes I$

Proof: First simplify D.

$$D = R_z(-\delta)\Phi\left(\frac{\delta}{2}\right) = \begin{bmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{bmatrix}\begin{bmatrix} e^{i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

Now we know

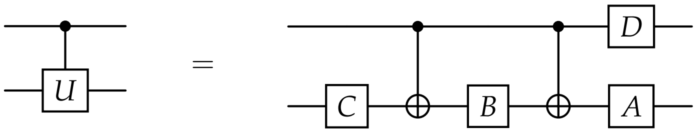
$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \Phi(\delta) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\delta}I = |0\rangle\langle 0| \otimes I + e^{i\delta}|1\rangle\langle 1| \otimes I$$

Also

$$D \otimes I = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix} \otimes I = \Big[|0\rangle\langle 0| + e^{i\delta}|1\rangle\langle 1|\Big] \otimes I = |0\rangle\langle 0| \otimes I + e^{i\delta}|1\rangle\langle 1| \otimes I$$

Hence we have $C(\delta) = D \otimes I$. $\square$

Therefore for $C(\Phi(\delta))$ it is enought to apply the D gate to the control state. Hence for any $C(U)$ where $U \in SU(2)$ there exists $\delta \in \mathbb{R}$ and $A, B, C \in SU(2)$ such that $U = \Phi(\delta)AXBXC$ where $ABC = I$. Then let D be the gate $D = R_z(-\delta)\Phi\left(\frac{\delta}{2}\right)$. Then we impliment $C(U)$ like this:



Now we have broken down $C(U)$ into single qubit gates and $CNOT$ gates. Therefore combining this full process we finally obtained that for any unitary gate operating on n qubits can be broken down into single qubit gates and $CNOT$ gates. Hence single qubit gates and $CNOT$ gates are universal.

$\square$

Problem 6

Let S be a subspace of $\mathbb{Z}_2^n$. Define $S^\perp = \{t \in \mathbb{Z}_2^n \mid t \cdot s = 0 \text{ for all } s \in S\}$. Let $|S\rangle$ be the quantum stae that represents the uniform superposition over S. Compute the values of $H^{\otimes n}|S\rangle$ and $H^{\otimes n}|y+S\rangle$ for any $y \in \{0,1\}^n$.

Solution: We have $|S\rangle = \frac{1}{\sqrt{|S|}}\sum\limits_{x\in S}|x\rangle$. Now since S is a subspace of $\mathbb{Z}_2^n$ it has a basis. Let $\{x_1,\dots,x_k\}$ is a basis of S. Then $\forall\ x \in S\ \exists\ a_i^x \in \{0,1\}$.for all $i \in [k]$ such that $\sum\limits_{i=1}^{k} a_i^x x_i = x$. So $|S| = 2^k$. Now let $y \in \mathbb{Z}_2^n$. Then $|S+y\rangle = \frac{1}{\sqrt{|S|}}\sum\limits_{x\in S}|x+y\rangle$. So now

$$\begin{aligned}
H^{\otimes n}|S+y\rangle &= \frac{1}{\sqrt{|S|}}\sum_{x\in S} H^{\otimes n}|x+y\rangle = \frac{1}{\sqrt{|S|}}\sum_{x\in S}\left[\sum_{i=0}^{2^n-1}(-1)^{\langle x+y,i\rangle}|i\rangle\right] \\
&= \frac{1}{\sqrt{|S|}}\sum_{x\in S}\left[\sum_{i=0}^{2^n-1}(-1)^{\langle y,i\rangle}(-1)^{\langle x,i\rangle}|i\rangle\right] \\
&= \frac{1}{\sqrt{|S|}}\sum_{x\in S}\left[\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{\langle y,i\rangle}(-1)^{\sum\limits_{j=1}^{k}a_j^x\langle x_j,i\rangle}|i\rangle\right] \\
&= \frac{1}{\sqrt{2^n|S|}}\sum_{i=0}^{2^n-1}(-1)^{\langle y,i\rangle}\left[\sum_{x\in S}\prod_{j=1}^{k}(-1)^{a_j^x\langle x_j,i\rangle}\right]|i\rangle \\
&= \frac{1}{\sqrt{2^n|S|}}\sum_{i=0}^{2^n-1}(-1)^{\langle y,i\rangle}\left[\sum_{a_1=0}^{1}\sum_{a_2=0}^{1}\cdots\sum_{a_k=0}^{1}\left(\prod_{j=1}^{k}(-1)^{a_j\langle x_j,i\rangle}\right)\right]|i\rangle \\
&= \frac{1}{\sqrt{2^n|S|}}\sum_{i=0}^{2^n-1}(-1)^{\langle y,i\rangle}\left[\prod_{j=1}^{k}\left((-1)^{0\times\langle x_j,i\rangle}+(-1)^{1\times\langle x_j,i\rangle}\right)\right]|i\rangle \\
&= \frac{1}{\sqrt{2^n|S|}}\sum_{i=0}^{2^n-1}(-1)^{\langle y,i\rangle}\left[\prod_{j=1}^{k}\left(1+(-1)^{\langle x_j,i\rangle}\right)\right]|i\rangle \\
&= \frac{1}{\sqrt{2^n|S|}}\sum_{x\in S^\perp}(-1)^{\langle y,i\rangle}\left[\prod_{j=1}^{k}(1+(-1)^0)\right]|x\rangle \\
&= \frac{1}{\sqrt{2^n|S|}}\sum_{x\in S^\perp}(-1)^{\langle y,x\rangle}2^k|x\rangle = \frac{2^k}{\sqrt{2^n\times 2^k}}\sum_{x\in S^\perp}(-1)^{\langle y,x\rangle}|x\rangle = \frac{1}{\sqrt{2^{n-k}}}\sum_{x\in S^\perp}(-1)^{\langle y,x\rangle}|x\rangle
\end{aligned}$$

Since for $H^{\otimes n}|S\rangle$ we have $y = \underbrace{(0,0,\dots,0)}_{n \text{ times}} = \bar{0}$ we have

$$H^{\otimes n}|S\rangle = H^{\otimes n}|S+\bar{0}\rangle = \frac{1}{\sqrt{2^{n-k}}}\sum_{x\in S^\perp}(-1)^{\langle\bar{0},x\rangle}|x\rangle = \frac{1}{\sqrt{2^{n-k}}}\sum_{x\in S^\perp}|x\rangle = \left|S^\perp\right\rangle$$

$\square$