Homework 06

Due Date: 111/03/30

Instruction. Do not submit part B.

A Homework Problems

1. Let
$$A = \begin{bmatrix} 2 & 3-3i \\ 3+3i & 5 \end{bmatrix}.$$
Find $U \in M_2(\mathbb{C})$ such that U^*AU is a diagonal matrix.

Definition A.1. Let $A \in M_n(\mathbb{C})$. A **square root** of A is a matrix $P \in M_n(\mathbb{C})$ such that $P^2 = A$.

2. Let $A, B \in M_n(\mathbb{C})$ be positive definite.
   (a) Prove that A has a positive definite square root.
   (b) For $A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$, find a positive definite square root for A.
   (c) Find an example that AB is not positive definite.
   (d) Show that $\operatorname{tr}(AB) \geq 0$. (*Hint*. Use (2a) to get a square root of A, say $\sqrt{A}$, then observe $\operatorname{tr}(AB) = \operatorname{tr}\left(\sqrt{A}B\sqrt{A}\right)$).

3. Let W be a finite-dimensional subspace of an inner product space V. We know that $V = W \oplus W^\perp$. Define $U : V \to V$ by
$$U(v_1 + v_2) = v_1 - v_2,$$
where $v_1 \in W$ and $v_2 \in W^\perp$. Prove that U is a self-adjoint unitary operator.
Remark. Such U is called the reflection of V about the subspace W.

4. Let T be a linear operator on a finite-dimensional inner product space V. Suppose that T is a projection such that $\|T(x)\| \leq \|x\|$ for all $x \in V$. Prove that T is an orthogonal projection.

B Supplementary Problems

Definition B.1. Let V be a finite dimensional inner product space and $u \in V$ be a unit vector. Define an operator $H_u : V \to V$ by

$$H_u(x) = x - 2\langle x, u\rangle u.$$

Geometrically, H_u is the reflection across the hyperplane $\text{span}\{u\}^{\perp}$. This operator is called **Householder operator**.

5. Let V be a finite dimensional inner product space.
   (a) Let $u \in V$ be a unit vector. Show that H_u is self-adjoint, and $H_u^2 = I$. (Hence H_u is unitary [orthogonal]).
   (b) Let $x, y \in V$ be linearly independent in V and $\|x\| = \|y\|$.
      i. If $F = \mathbb{C}$, prove that there exist a unit vector $u \in V$ and $\theta \in \mathbb{C}$ with $|\theta| = 1$ such that $H_u(x) = \theta y$. (*Hint.* Choose θ so that $\langle x, \theta y\rangle$ is real and set $u = \frac{x-\theta y}{\|x-\theta y\|}$.)
      ii. If $F = \mathbb{R}$, prove that there exist a unit vector $u \in V$ such that $H_u(x) = y$.

6. (**Cayley transform**) Let $A \in M_n(\mathbb{R})$ be skew-symmetric, that is, $A^t = -A$.
   (a) Show that the eigenvalues of A are either zero or purely-imaginary (that is, the real part is 0). (*Hint.* Mimic the proof of "self-adjoint operators have real eigenvalues" given in class.)
   (b) Show that $I + A$ is invertible.
   (c) Prove that $(I - A)$ and $(I + A)^{-1}$ commute.
   (d) Put $Q = (I - A)(I + A)^{-1}$. Show that Q is orthogonal.
   (e) Prove that $I + Q$ is invertible and $A = (I + Q)^{-1}(I - Q)$.

   Remark. This problem gives a bijection between skew-symmetric real matrices and orthogonal matrices without eigenvalue -1.

7. (**QR factorization**) Let $F = \mathbb{R}$ or $\mathbb{C}$, $A \in M_n(F)$ be an invertible matrix and denote the k-th column vector of A by w_k. Since A is invertible, we know that $\{w_1, w_2, ..., w_n\}$ forms a basis for F^n. Suppose $\{v_1, v_2, ..., v_n\}$ is the orthogonal set obtained by performing Gram-Schmidt process to $\{w_1, w_2, ..., w_n\}$ (with respect to the standard inner product), and let $u_k = \frac{v_k}{\|v_k\|}$ be the normalization of v_k for $1 \le k \le n$.
   (a) For $1 \le k \le n$, show that

   $$w_k = \|v_k\| u_k + \sum_{j=1}^{k-1} \langle w_k, u_j\rangle u_j.$$

   Deduce that $A = QR$, where $Q \in M_n(F)$ is the matrix with k-th column equals to u_k, and $R \in M_n(F)$ is defined by

   $$R_{jk} = \begin{cases} \|v_j\|, & j = k \\ \langle w_k, u_j\rangle, & j < k \\ 0, & j > k \end{cases}.$$

This is called the **QR factorization** of A. Note that Q is unitary [orthogonal] and R is upper-triangular.

(b) Suppose $A = Q_1R_1 = Q_2R_2$, where Q_1, Q_2 are unitary [orthogonal], R_1, R_2 are upper-triangular. Prove that $R_2R_1^{-1}$ is diagonal.

Remark. This factorization could be used to solve linear systems in numerical analysis. The system $Ax = b$ is equivalent to $Rx = Q^*b$, and since R is upper-triangular, solving this system is more convenient than the original one.

8. **(Hadamard Product of Definite Matrices)** Let A, $B \in M_n(\mathbb{C})$ be two matrices, the **Hadamard product** of A and B is a matrix $A \circ B \in M_n(\mathbb{C})$ defined to be

$$(A \circ B)_{ij} = A_{ij}B_{ij}.$$

(a) Compute the identity of these product, that is, find $J \in M_n(\mathbb{C})$ such that

$$A \circ J = J \circ A = A.$$

(b) Show that if A, B are positive semidefinite, then $A \circ B$ is positive semidefinite. (*Hint*: Consider the spectral decomposition of A and B)

(c) Show that if A, B are positive definite, then $A \circ B$ is positive definite.

9. If all eigenvalues of $A \in M_n(\mathbb{C})$ have absolute value 1 and $\|Ax\| \leq 1$ for all unit vectors $x \in \mathbb{C}^n$, show that A is unitary.

Definition B.2. The following three 2×2 matrices are called the *Pauli matrices*:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

One sees immediately that these matrices are unitary, and their eigenvalues are all ± 1.

10. Show that X, Y, Z form a basis for the set

$$\{A \in M_2(\mathbb{C}) | A^* = -A, \mathrm{tr}(A) = 0\}.$$

This set is called the *Lie algebra* $\mathfrak{su}(2)$.

11. For $\vec{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ and $\theta \in \mathbb{R}$, define the 2×2 complex matrix

$$R_{\vec{n}}(\theta) := \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z).$$

Let U be a 2×2 unitary matrix.

(a) Prove that there exist $\alpha, \theta \in \mathbb{R}$ and $\vec{n} \in \mathbb{R}^3$ such that

$$U = e^{i\alpha} R_{\vec{n}}(\theta).$$

(b) **(ZY decomposition)** Let $\vec{y} = (0, 1, 0), \vec{z} = (0, 0, 1) \in \mathbb{R}^3$. Prove that there exist $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = e^{i\alpha} R_{\vec{z}}(\beta) R_{\vec{y}}(\gamma) R_{\vec{z}}(\delta).$$

(c) Show that there exist unitary matrices A, B, C and $\alpha \in \mathbb{R}$ such that $ABC = I$ and $U = e^{i\alpha} AXBXC$.
(*Hint.* First write U in the form in (b), then choose A, B, C to be suitable matrices constructed by $R_{\vec{y}}$ and $R_{\vec{z}}$.)

(d) Let $\vec{n_1}, \vec{n_2} \in \mathbb{R}^3$ be two orthogonal vectors (with respect to the standard inner product). Prove the result in (b) with $\vec{y}, \vec{z}$ replaced by $\vec{n_1}, \vec{n_2}$. What if $\vec{n_1}, \vec{n_2}$ are not orthogonal?

Remark. 2×2 unitary matrix can be realized as rotations in $\mathbb{R}^3$. Check out "Euler angles" and "3D rotation group" for further information.

Definition B.3. Let $V = \mathbb{C}^n$ equipped with standard inner product and let $m \in \mathbb{N}$. Let $p_1, p_2, ..., p_m$ be m non-negative real numbers and $\sum_k p_k = 1$, and $v_1, v_2, ..., v_m$ be m unit vectors in V. We call the set of pairs $\{(p_k, v_k)\}_k$ an **ensemble of pure states**. For an ensemble of pure states, we define its **density operator** ρ to be the linear transformation $\sum_k p_k \operatorname{Pr}_{v_k}$, where Pr_{v_k} is the orthogonal projection onto the 1-dimensional subspace spanned by v_k, namely $\operatorname{Pr}_{v_k}(v) = \langle v, v_k \rangle v_k$.

12. Using the notations in the previous definition, do the followings.

(a) Prove that if ρ is the density operator of an ensemble $\{(p_k, v_k)\}_k$, then $\operatorname{tr}(\rho) = 1$ and ρ is positive semidefinite.

(b) Conversely, prove that if ρ is any positive semidefinite linear transformation satisfying $\operatorname{tr}(\rho) = 1$ then ρ is the density operator of some ensemble of pure states $\{(p_k, v_k)\}_k$.(*Hint.* Spectral decomposition theorem.)
Hence from now on, we say ρ is a density operator if it meets these two conditions. We will denote the set of all density operators on V by $D(V)$.

(c) If ρ is a density operator, prove that $\operatorname{tr}(\rho^2) \leq 1$. When does the equality holds? We call ρ *pure* when the equality holds.

(d) Let $m \in \mathbb{N}$ and let $\{(p_i, v_i)\}_{i=1}^m$ and $\{(q_j, w_j)\}_{j=1}^m$ be two ensembles consisting of m pairs. Prove that they have the same density operator if and only if there is an unitary matrix U of size m such that $v_i = \sum_j U_{ij} w_j$ for all i. What if the two ensembles have different numbers of pairs?

13. Let ρ, σ be density operators on $V = \mathbb{C}^n$. Their *fidelity* is defined to be

$$F(\rho, \sigma) := \left(\operatorname{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)\right)^2.$$

(a) Prove that $F(\rho, \sigma) \in [0, 1]$ and $F(\rho, \sigma) = F(\sigma, \rho)$.

(b) Prove that $F(\rho, \sigma) = 1$ if and only if $\rho = \sigma$, and $F(\rho, \sigma) = 0$ if and only if $\rho \perp \sigma$ (with respect to the Frobenius inner product)

(c) Prove that $F(U\rho U^*, U\sigma U^*) = F(\rho, \sigma)$ for any unitary U.

Definition B.4. For $V = \mathbb{C}^n$, A **Quantum operation** on V is a map $\mathcal{E} : D(V) \to D(V)$ taking the form

$$\mathcal{E}(\rho) = \sum_{k=1}^{r} E_k \rho E_k^*,$$

where $\{E_k\}_{k=1}^r$ is a set of linear transformations $V \to V$ satisfying $\sum_k (E_k^* E_k) = I$, and $r \geq 1$ is a positive integer. The E_k's are called the **Kraus operators** of $\mathcal{E}$.

14. Let $V = \mathbb{C}^n$.

 (a) Show that a quantum operation $\mathcal{E}$ on V is trace-preserving, namely $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\rho) = 1$. Also prove that it is convex-linear: $\mathcal{E}(\sum_i p_i \rho_i) = \sum_i p_i \mathcal{E}(\rho_i)$ where $\{p_i\}$ is a finite set of non-negative real numbers summing to 1, and $\{\rho_i\}$ is a collection of density operators on V.

 (b) Show that if $\mathcal{E}$ and $\mathcal{F}$ are two quantum operations on V, then $\mathcal{F} \circ \mathcal{E}$ is still a quantum operation on V.

 (c) Let $\mathcal{E}$ and $\mathcal{F}$ be two quantum operations on V and $\{E_i\}_{i=1}^m$, $\{F_j\}_{j=1}^k$ be their Kraus operators respectively. By appending zero operators to the smaller set, we may assume $m = k$. Show that $\mathcal{E} = \mathcal{F}$ if and only if there exist an unitary $U \in M_m(\mathbb{C})$ such that $E_i = \sum_j U_{ij} F_j$ for all i.

 (d) Let $\mathcal{E}$ be a quantum operation on $V = \mathbb{C}^n$ given by $\{E_i\}_{i=1}^m$. Prove that there exists another set of operation elements $\left\{\widetilde{E_j}\right\}$ consisting of **at most** n^2 **elements** such that $\left\{\widetilde{E_j}\right\}$ defines the same quantum operation $\mathcal{E}$. That is to say,

$$\sum_{i=1}^{m} E_i \rho E_i^* = \sum_{j=1}^{n^2} \widetilde{E_j} \rho \widetilde{E_j}^*$$

 for all $\rho \in D(V)$.