Quantum Information and Computation
Homework 0: Reviews on Linear Algebra

(Report Due: N/A)

1 Overview

Homework 0 gives a very basic review of the mathematical preliminaries — mainly linear algebra — for the course *Quantum Information and Computation*. It is highly recommended that your are familiar with the homework problems before diving into the main course. We will use the concepts, notation, facts, and some statements of this homework problems in the course without proofs.

2 Homework Problems

1. **Complex inner product space:**

   Definition 1 (Complex vector space)**.** *A set $\mathbb{C}^d$ forms a vector space of dimension d over the complex numbers when addition and scalar multiplication are defined as follows:*

   - (*Addition*) *For vectors $u, v \in \mathbb{C}^d$, the vector $u+v \in \mathbb{C}^d$ is defined by the equation $(u+v)_i := u_i + v_i$ for $i = 1, 2, \ldots, d$. Here, u_i denotes the i-th entry of the vector u.*
   - (*Scalar multiplication*) *For a vector $u \in \mathbb{C}^d$ and a scalar $c \in \mathbb{C}$, the vector $cu \in \mathbb{C}^d$ is defined by the equation $(cu)_i := cu_i$ for all $i \in \{1, 2, \ldots, d\}$.*

   The vector whose entries are all zero is simply denoted as 0.

   Remark. In Definition 1, the entry of vectors in $\mathbb{C}^d$ is indexed by the set $\{1, 2, \ldots, d\}$. Generally, such set could be an arbitrary alphabet or even an uncountable set. Indeed, every d-dimensional complex vector space (or called the complex Euclidean space) is *isomorphic*[1] to $\mathbb{C}^d$ described above. Hence, we often only consider the linear space $\mathbb{C}^d$ of all d-tuples of complex numbers in this course.

   More generally, a *vector space* (or called *linear space*) $\mathcal{V}$ over field[2] F is a set on which *addition* and *scalar multiplication* are defined, i.e. for any $u, v \in \mathcal{V}$ and $a, b \in F$, one has $ax, by \in \mathcal{V}$ and the *linear combination* $ax + by = by + ax \in \mathcal{V}$.

   Definition 2 (Inner product)**.** *Let $\mathbb{C}^d$ be a complex vector space. A complex-valued function $\langle \cdot | \cdot \rangle$ on $\mathbb{C}^d \times \mathbb{C}^d$ is an* inner product *if it satisfies the following for all $u, v, w \in \mathbb{C}^d$ and $c \in \mathbb{C}$:*

[1] An *isomorphism* is, generally speaking, a structure-preserving bijective mapping. We are not going to dive into the detailed terminologies since they are not the main focus in this course.

[2] A *field* is a set on which addition and multiplication are properly defined. In this course, we only consider complex numbers ($F = \mathbb{C}$) and finite fields (e.g. $F = \{0, 1\}$).

- (*Linearity in the second argument*) $\langle u, cv + w\rangle = c\langle u, v\rangle + \langle u, w\rangle$.
- (*Conjugate symmetry*) $\overline{\langle u, v\rangle} = \langle v, u\rangle$.
- (*Positive definitness*) $\langle u, u\rangle \geq 0$, *with equality if and only if* $u = 0$

If not explicitly stated otherwise, we consider the inner product of $u, v \in \mathbb{C}^d$ *as*

$$\langle u, v\rangle := u^\dagger v := \sum_{i=1}^{d} \overline{u_i} v_i.$$

A complex vector space with an inner product defined on it is an *inner product space*. Moreover, every inner product space is a *normed space*, with the *Euclidean norm* being defined as $\|u\| := \sqrt{\langle u, u\rangle}$. A complete[3] inner product space is called *Hilbert space*. As described above, we usually consider the Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$ in this course, and an element in $\mathbb{C}^d$ is a d-tuple column vector.

If $\langle u, v\rangle = 0$ for vectors u and v of a Hilbert space $\mathcal{H}$, then u and v are called *orthogonal*, denoted by $u \perp v$. A family $\{e_i\}$ of vectors is called orthonormal if $\langle e_i, e_i\rangle = 1$ and $\langle e_i, e_j\rangle = 0$ for $i \neq j$ (namely, each vector $u \in \mathcal{H}$ has unit norm). An *orthonormal basis* for a Hilbert space $\mathcal{H}$ is a maximal orthonormal set. The cardinality of an orthonormal basis is called the dimension of the Hilbert space.

(a) Let $x = x_1x_2\ldots x_n, y = y_1y_2\ldots y_n, z = z_1z_2\ldots z_n \in \{0,1\}^n$ be n-bit binary strings. Let $\oplus$ denote bitwise addition modulo 2. Namely, $x \oplus y = z$ means that for each $i \in \{1,\ldots,n\}$, $z_i = x_i + y_i \bmod 2$. Also, let $\cdot$ denote the a dot product: $x \cdot y = (x_1y_1 + x_2y_2 + \cdots x_ny_n) \bmod 2$. Prove that n-bit strings $\{0,1\}^n$ over field $\{0,1\}$ with the above mentioned dot product is an inner product space. Find a basis for it.

(b) Prove the *Cauchy–Schwarz inequality*: if u and v are in a Hilbert space $\mathcal{H}$, then

$$|\langle u, v\rangle|^2 \leq \|u\|^2\|v\|^2.$$

(c) Given *linear independent* vectors $v_1, v_2, \ldots, v_d$ in d-dimensional Hilbert space $\mathcal{H}$, show that an orthonormal basis for $\mathcal{H}$ can be obtained by the *Gram–Schmidt procedure*:

$$\begin{aligned}
e_1 &:= \tfrac{1}{\|v_1\|} v_1, \\
e_2 &:= \tfrac{v_2 - \langle e_1, v_2\rangle e_1}{\|v_2 - \langle e_1, v_2\rangle e_1\|}, \\
e_3 &:= \tfrac{v_3 - \langle e_1, v_3\rangle e_1 - \langle e_2, v_3\rangle e_2}{\|v_3 - \langle e_1, v_3\rangle e_1 - \langle e_2, v_3\rangle e_2\|}, \\
&\vdots \\
e_d &:= \tfrac{v_d - \langle e_1, v_d\rangle e_1 - \cdots - \langle e_{d-1}, v_d\rangle e_{d-1}}{\|v_d - \langle e_1, v_d\rangle e_1 - \cdots - \langle e_{d-1}, v_d\rangle e_{d-1}\|}.
\end{aligned}$$

(d) Given a basis $\{e_i\}_i$ of a Hilbert space$\mathcal{H}$, show that any vector $u \in \mathcal{H}$ admits a *basis expansion*:

$$u = \sum_i \langle e_i, u\rangle e_i.$$

[3] It means that every Cauchy sequence of elements in the space $\mathcal{H}$ must converges to a unique element in $\mathcal{H}$. Nonetheless, in a finite-dimensional Hilbert space, the completeness always holds

In other words, any vector $u \in \mathcal{H}$ is determined by its coordinates $\{\langle u, e_i\rangle\}_i$ with respect to the basis $\{e_i\}_i$.

2. **Linear Operators and the Matrix Representation:**

Definition 3. *Let $\mathcal{H}$ and $\mathcal{K}$ be Hilbert spaces. A mapping $A : \mathcal{H} \to \mathcal{K}$; $A : u \mapsto A(u) \equiv Au$ is linear if it preserves linear combinations:*

$$A(au + bv) = aAu + bAv \in \mathcal{K}, \quad \forall u, v \in \mathcal{H},\ a, b \in \mathbb{C}.$$

Such a mapping is called linear operators, *or simply* operator. *We denote by $\mathcal{L}(\mathcal{H}, \mathcal{K})$ the set of all operators $A : \mathcal{H} \to \mathcal{K}$, and shorthand $\mathcal{L}(\mathcal{H}) \equiv \mathcal{L}(\mathcal{H}, \mathcal{H})$.*

A linear operator $A : \mathcal{H} \to \mathcal{H}$ is a bounded operator *if there exists a finite number $t \geq 0$ such that*

$$\|Au\| \leq t\|u\|, \quad \forall u \in \mathcal{H}. \tag{1}$$

We denote by $\mathcal{B}(\mathcal{H})$ the set of bounded operators on $\mathcal{H}$.

For a finite-dimensional Hilbert space $\mathcal{H}$, every linear operator is a bounded operator[4], and hence $\mathcal{L}(\mathcal{H}) = \mathcal{B}(\mathcal{H})$.

For a bounded operator $A \in \mathcal{B}(\mathcal{H})$, we use the following notation[5]:

- (Kernel) $\texttt{ker}(A) := \{u \in \mathcal{H} : Au = 0\}$;
- (Range) $\texttt{rang}(A) := \{Au \in \mathcal{H} : u \in \mathcal{H}\}$, and the *rank* of A means the dimension of $\texttt{rang}(\mathrm{A})$;
- (Support) $\texttt{supp}(A) := \{u \in \mathcal{H} : v \perp u,\ \forall v \in \texttt{ker}(A)\} \equiv \texttt{ker}(A)^{\perp}$.

It is not hard to show that all these subsets correspond to certain linear subspace of $\mathcal{H}$.

The set of bounded operators is itself a vector space since the usual addition and scalar multiplication are defined by the linear combination: for linear mappings $A, B : \mathcal{H}_1 \to \mathcal{H}_2$:

$$(aA + bB)u \mapsto aAu + bBu,$$
$$[aA + bB]_{ij} \mapsto a[A]_{ij} + b[B]_{ij}.$$

Hence, we denote by O and I the *null operator* and the *identity operator*, respectively; they are defined by $Ou = 0$ and $Iu = u$ for every $u \in \mathcal{H}$. The null operator plays the role of the null vector in the vector space of bounded operators.

The vector space $\mathcal{B}(\mathcal{H})$ is a *normed space* with a norm defined via formula

$$\|A\|_\infty := \sup_{u:\|u\|=1} \|Au\|.$$

[4]However, this statement is no longer true for infinite-dimensional Hilbert spaces. Since the Hilbert spaces we consider in this course (and in most research papers) are either finite dimensional or countably infinite dimensional. We will only impose the boundedness condition if necessary.

[5]The kernel, range, and the support spaces can be defined for general operators $A : \mathcal{H} \to \mathcal{K}$ instead of the bounded operators $\mathcal{B}(\mathcal{H})$. The definitions here are sufficient in this course.

In other words, $\|A\|_\infty$ is the least number t that satisfies (1). This norm on $\mathcal{B}(\mathcal{H})$ is called the *operator norm*[6]. We remark that there are various useful norms for bounded operators that we will encounter in this course.

Let $e_1, e_2, \ldots, e_n$ be a basis of the Hilbert space $\mathcal{H}$ and $f_1, f_2, \ldots, f_m$ be a basis of the Hilbert space $\mathcal{K}$. The linear operator $A : \mathcal{H} \to \mathcal{K}$ is determined by the vectors $\{Ae_j\}_{j=1}^n$. Moreover, each vector Ae_j is determined by its coordinates:

$$Ae_j = c_{1,j} f_1 + c_{2,j} f_2 + \cdots c_{m,j} f_m.$$

The number $\{c_{i,j}\}_{(i,j)=(1,1)}^{(m,n)}$ forms an $m \times n$ matrix, and this is called the *matrix representation* of the linear operator A with respect to the bases $\{e_i\}_i$ and $\{f_j\}_j$. We denote by $[A]_{ij}$ the element (or entry) of the matrix A:

$$[A]_{ij} := \langle f_i, Ae_j \rangle = c_{ij}.$$

Note that the order of the basis vectors matters when we refer to the matrix representation. If no explicitly specified, the underlying basis for the matrix is taken by the *standard basis* (or called the *computational basis*):

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad e_d = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Conversely, starting with a matrix A (with its matrix elements) we recover the action of the linear mapping $A : \mathcal{H} \to \mathcal{K}$ on a vector $u \in \mathcal{H}$ via the formula:

$$A = \sum_{i,j=(1,1)}^{(n,m)} [A]_{ij} f_i e_j^\dagger \quad \text{(outer product decomposision)};$$
$$Au = \sum_{i,j=(1,1)}^{(n,m)} [A]_{ij} \langle e_j, u \rangle f_i.$$

In other words, for $\mathcal{H} \simeq \mathbb{C}^d$, to each operator $A \in \mathcal{B}(\mathcal{H})$ an $d \times d$ matrix A is associated. The correspondence between the linear mapping and its matrix representation is an algebraic isomorphism from $\mathcal{B}(\mathcal{H})$ to the algebra $\mathbb{C}^{d\times d}$ of $d \times d$ matrices. This isomorphism shows that the theory of linear operators on an d-dimensional Hilbert space is the same as the theory of $d \times d$ matrices. Hence, when the underlying bases are specified, we will use the term linear mapping, linear operator, or matrix interchangeably[7].

Let $\mathcal{H}_1, \mathcal{H}_2$ and $\mathcal{H}_3$ be Hilbert spaces and let us fix a basis in each of them. If $B : \mathcal{H}_1 \to \mathcal{H}_2$ and $A : \mathcal{H}_2 \to \mathcal{H}_3$ are linear mappings, then the composition $u \mapsto A(Bu) \in \mathcal{H}_3$ for $u \in \mathcal{H}_1$ is linear as

[6] One can show that $\mathcal{B}(\mathcal{H})$ is complete in the operator norm topology. Complete normed vector spaces are called *Banach spaces*.

[7] Note that the term *operator* is usually reserved for linear mapping in the infinite-dimensional case, while the term matrix is for the finite-dimensional case. Since we will only consider up to countably infinite-dimensional Hilbert space, the indices in the considered infinite-dimensional matrices will be also countable.

well, and it is denoted by AB. Its matrix representation is given by the matrix representations of A, B and standard matrix multiplication as follows:

$$[AB]_{ij} = \sum_k [A]_{ik}[B]_{kj}.$$

An operator $A \in \mathcal{B}(\mathcal{H})$ is *invertible* if there is a (unique) $B \in \mathcal{L}(\mathcal{H})$ such that $AB = BA = I$. This B is called the *inverse* of A, and is denoted by A^{-1}. Note that the inverse is not always exists.

Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces. If $A : \mathcal{H} \to \mathcal{K}$ is a linear operator, then its *adjoint*[8] $A^\dagger : \mathcal{K} \to \mathcal{H}$ is given by the formula

$$\langle v, Au \rangle = \langle A^\dagger v, u \rangle, \quad \forall u \in \mathcal{H}, v \in \mathcal{K}.$$

Note that the inner product on the left-hand side is defined on $\mathcal{K}$ and the inner product on the right-hand side is defined on $\mathcal{H}$. The matrix representation of the adjoint operator $A^\dagger$ corresponds to the *conjugate transpose* of the matrix representation of A:

$$\left[A^\dagger\right]_{ij} = \overline{[A]_{ji}}.$$

In the following we introduce some important classes of bounded operators.

1. *Normal operators*. An operator A is called *normal* if it satisfies $AA^\dagger = A^\dagger A$. As we will show later, every normal operator admits the spectral decomposition.
2. *Self-adjoint operators*. An operator $A \in \mathcal{B}(\mathcal{H})$ is called *self-adjoint* if $A^\dagger = A$. Using the matrix representation, the (i, j) element of the matrix of A equals the conjugate of the (j, i) element. In particular, all diagonal entries of $[A]$ are real. Such self-adjoint operators are called *Hermitian* matrices. Self-adjoint operators play a crucial role rule since its expectation with respect to a state vector[9] and its eigenvalues (as we will describe later) are all real numbers. Thus, in some sense, a self-adjoint can be viewed as a "real" vector in an operator space. Note that every Hermitian operator is a normal operator.
3. *Positive semi-definite operators*. A self-adjoint operator A is called *positive semi-definite* if $\langle u, Au \rangle \geq 0$ for all $u \in \mathcal{H}$. Let A, B be self-adjoint operators. We write $A \geq B$ if the operators $A - B$ is positive semi-definite. By definition, an operator A is positive semi-definite exactly when $A \geq 0$. It can be shown that the relation $\geq$ is a *partial ordering* on the set of self-adjoint operators[10]. The interior of the set of positive semi-definite operators are called *positive definite operators*, i.e. the set of operators A on $\mathcal{H}$ satisfying $\langle u, Au \rangle > 0$ for all $u \in \mathcal{H}$.
4. *Projection operators*. A self-adjoint operator P is a *projection* if $P^2 = P$. It immediately follows from definition that a projection is positive semi-definite and it projects the vectors onto its range space. A unit vector $u \in \mathcal{H}$ forms an rank-one projection $P = uu^\dagger$.

[8] Mathematicians often use '$*$' to denote the adjoint, while physicists use '$\dagger$' as in many quantum literature.

[9] That is, for a self-adjoint operator H on Hilbert space $\mathcal{H}$ and vector $u \in \mathcal{H}$, one has $u^\dagger H u \in \mathbb{R}$.

[10] It is not the total ordering because not every pair of self-adjoint operators is comparable. It is the same situation for real-valued Euclidean vectors.

5. *Isometries*. An operator $A : \mathcal{H} \to \mathcal{K}$ is an *isometry* if it preserves the Euclidean norm: $\|Au\| = \|u\|$ for all $u \in \mathcal{H}$. This condition is equivalent to $A^\dagger A = I$. In order for an isometry of the form $A : \mathcal{H} \to \mathcal{K}$ to exist, it must hold that the dimension of $\mathcal{K}$ is larger than that of $\mathcal{H}$. Every isometry preserves not only the Euclidean norm, but inner products as well: $\langle Au, Av\rangle = \langle u, v\rangle$ for all $u, v \in \mathcal{H}$.
6. *Unitary operators*. An operator $U : \mathcal{H} \to \mathcal{H}$ is *unitary* if it satisfies $UU^\dagger = U^\dagger U = I$.
7. *Diagonal operators*. An operator $A \in \mathcal{B}(\mathcal{H})$ is a *diagonal operator* if $[A]_{ij} = 0$ for all $i \neq j$.

Let $\mathcal{H}$ be a Hilbert space with an orthonormal basis $\{e_i\}_i$. Let $A \in \mathcal{B}(\mathcal{H})$ such that $\sum_i |\langle e_i, Ae_i\rangle| < \infty$. We define the *trace* of A by:

$$\mathrm{Tr}[A] := \sum_i \langle e_i, Ae_i\rangle.$$

Note that the trace of an operator (if it exits) is *independent* of the choice of the basis. Using the matrix representation, the trace of a square matrix equals to the sum of diagonal elements.

Given two bounded operators A and B, we define the *Hilbert–Schmidt inner product* as:

$$\langle A, B\rangle_{\mathrm{HS}} := \mathrm{Tr}\left[A^\dagger B\right].$$

(a) Let $A, B \in \mathcal{B}(\mathcal{H})$. Then for every $u, v \in \mathcal{H}$, prove that

$$\begin{aligned} \|Au\| &\leq \|A\|\|u\|; \\ |\langle v, Au\rangle\| &\leq \|v\|\|u\|\|A\|; \\ \|AB\| &\leq \|A\|\|B\|. \end{aligned}$$

(b) Let $A, B \in \mathcal{B}(\mathcal{H})$. If $\langle u, Au\rangle = \langle u, Bu\rangle$ for every $u \in \mathcal{H}$, then $A = B$.

Remark. The diagonal elements of a matrix do not determine the matrix completely. However, Problem 2b shows that if the diagonal elements of an operator are known in *all* orthonormal bases, then A is determined.

(c) Prove the following properties for bounded operators in $\mathcal{B}(\mathcal{H})$:

(i) An operator $A \in \mathcal{B}(\mathcal{H})$ is self-adjoint if and only if $\langle u, Au\rangle$ is a real number for every $u \in \mathcal{H}$.

(ii) $(A + B)^\dagger = A^\dagger + B^\dagger$, and $(cA)^\dagger = \bar{c}A^\dagger$ for $c \in \mathbb{C}$.

(iii) $(A^\dagger)^\dagger = A$, and $(AB)^\dagger = B^\dagger A^\dagger$.

(iv) $(A^{-1})^\dagger = (A^\dagger)^{-1}$ if A is invertible.

(v) (Optional) $\|A\| = \|A^\dagger\|$, and $\|A^\dagger A\| = \|A\|^2$.

(d) Prove that A is a positive semi-definite operator if and only if $A = X^\dagger X$ for some operator $X \in \mathcal{L}(\mathcal{H}, \mathcal{K})$.

(e) Let P, Q be projections on a Hilbert space $\mathcal{H}$, and $O \neq P \neq I$. We write $P^\perp := I - P$ to be the *orthogonal complement* of P. Prove the following:

(i) $\|P\| = 1$;

(ii) $P = \sum_i p_i e_i e_i^\dagger$ for some orthonormal basis $\{e_i\}_i$ and p_i is either 0 or 1;

(iii) for every $u \in \mathcal{H}$, there are orthogonal vectors $u_0, u_1 \in \mathcal{H}$ such that

$$Pu_0 = 0, \quad Pu_1 = u_1, \quad \text{and} \quad u = u_0 + u_1.$$

(iv) $P^\perp$ is a projection;

(v) $(P^\perp)^\perp = P$;

(vi) if $Q \le P$, then $P^\perp \le Q^\perp$.

(f) Let P and Q be projections. The following conditions are equivalent:

(i) $P \ge Q$;

(ii) $PQ = QP = Q$;

(iii) $P - Q$ is a projection.

(g) Let $\mathcal{H}$ be a Hilbert space. The following are equivalent:

(i) $U \in \mathcal{B}(\mathcal{H})$ is unitary;

(ii) U^{-1} exists and $U^{-1} = U^\dagger$ is unitary too;

(iii) for every orthonormal basis $\{f_j\}_j$, $\{Uf_j\}_j$ is also an orthonormal basis;

(iv) for all $u, v \in \mathcal{H}$, one has $\langle Uu, Uv\rangle = \langle u, v\rangle$;

(v) the columns of U form an orthonormal basis of $\mathcal{H}$.

(h) Let a bounded operator A on $\mathcal{H}$ with trace $\mathrm{Tr}[A]$. Show that $\mathrm{Tr}[A] = \langle f_j, Af_j\rangle$ for any orthonormal basis $\{f_j\}_j$ on $\mathcal{H}$.

(i) Prove that the set of bounded operators $\mathcal{B}(\mathcal{H})$ endowed with the Hilbert–Schdmit inner product is a complex inner product space. Find a basis for it.

(j) Assume that the traces of bounded operators A and B both exist. Prove the following properties:

- (cyclic permutations) $\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$;
- (linearity) $\mathrm{Tr}[cA + B] = c\mathrm{Tr}[A] + \mathrm{Tr}[B]$ for all $c \in \mathbb{C}$;
- (trace of a dyad) $\mathrm{Tr}[uv\dagger] = \langle v, u\rangle$;
- (expectation value of A) $\mathrm{Tr}[Auu\dagger] = \langle u, Au\rangle$;
- (real inner product) $\langle A, B\rangle_{\mathrm{HS}}$ is a real number if operators A and B are self-adjoint;
- (unitary invariance) $\mathrm{Tr}[UAU^\dagger] = \mathrm{Tr}[A]$ for any unitary operator U.

3. **Spectrum and Eigenvalues:**

Definition 4. *Let $\mathcal{H}$ be a Hilbert space, and $A \in \mathcal{B}(\mathcal{H})$ be a bounded operator. A number $\lambda \in \mathbb{C}$ is*

- *an* eigenvalue *of A if there exists a non-zero vector $u \in \mathcal{H}$ such that $Au = \lambda u$. The vector u is an* eigenvector *of A associated with the eigenvalue λ;*
- *in the* spectrum *of A if the inverse mapping of the bounded operator $\lambda I - A$ does not exist.*

By definition it is clear that all eigenvalues of A are in the spectrum of A but the spectrum may contain numbers other than just the eigenvalues. However, in the finite-dimensional case, the spectrum is equal to the set of eigenvalues[11].

Given a normal operator A on a Hilbert space $\mathcal{H}$, the *spectral decomposition* of A is:

$$A = \sum_i \lambda_i P_i,$$

where each λ_i is an eigenvalue of A with multiplicity equal to the rank (i.e. the dimension of the range space) of P_i, and P_i is the projection operator onto the space spanned by the eigenvectors of A corresponding to the eigenvalue λ_i.

The above spectral decomposition theorem can be stated in a slightly different form: there exists an orthonormal basis $\{f_j\}_j$ of $\mathcal{H}$ such that

$$A = \sum_{j=1} \lambda_j f_j f_j^\dagger = UDU^\dagger,$$

where the columns of the unitary operator U consist of the orthonormal basis $\{f_j\}_j$ (in an ordered way), and the diagonal matrix $D = \texttt{diag}(\lambda_1, \lambda_2, \ldots)$.

In general, two normal operators $A, B \in \mathcal{B}(\mathcal{H})$ do not commute, i.e. $AB \neq BA$ or equivalently the *Lie bracket* or the *commutator* $[A, B] := AB - BA$ is not zero. This *non-commutativity* constitutes one of the main difference between quantum information processing from the the classical one. Using the spectral theorem, one can see that the non-commutativity means that the operators A and B cannot be diagonalized by the same set of eigenvectors.

(a) Let A be a normal operator with eigenvalues $\{\lambda_i(A)\}_i$. Prove the following:
   (i) $\mathrm{Tr}[A] = \sum_i \lambda_i(A)$ (counting multiplicity).
   (ii) if A is unitary, then $\lambda_i(A)$ is of the form $e^{i\varphi}$, for $\varphi \in \mathbb{R}$;
   (iii) if A is self-adjoint, then $\lambda_i(A) \in \mathbb{R}$;
   (iv) if A is a projection, then $\lambda_i(A) = 0$ or $\lambda_i(A) = 1$.

(b) For any positive semi-definite operators A and B, prove the following:
   (i) eigenvalues of A are all non-negative;
   (ii) $\langle A, B\rangle_{\mathrm{HS}} \geq 0$;
   (iii) if $A \perp B$ (in terms of the Hilbert–Schmidt inner product), then $AB = BA = O$.

(c) For any normal operator A, we denote by $UAU^\dagger$ the *unitary transformation* of A with respect to the unitary operator U. Show that the eigenvalues of A remain the same, while the eigenvectors, say $\{f_j\}_j$ becomes $\{Uf_j\}_j$.

(d) Given a normal operator A, show that if $B \geq O$, then $ABA^\dagger \geq 0$.

(e) Prove that for operators $A \leq B$ and $C \geq O$, it follows that $\mathrm{Tr}[AC] \leq \mathrm{Tr}[BC]$.

[11] Note that in infinite-dimensional Hilbert space, a bounded operator may not have any eigenvalues. However, we will not consider this scenario in this course.

(f) For normal operators A and B, prove that $[A, B] = 0$ if and only if there exists a unitary operator U and diagonal operators D_A and D_B such that $A = UD_AU^\dagger$ and $B = UD_BU^\dagger$.

(g) The set of self-adjoint operators, positive semi-definite operators, and positive definite operators are all convex.

3 References

Here are some great references that you may find useful:

- Stephen H. Friedberg, Arnold J. Insel, and Lawrence E. Spence. *Linear Algebra* (5th Edition). Pearson. 2019.
- Mário Ziman and Teiko Heinosaari. *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement*. Cambridge University Press, 2011.
- Stephen Bruce Sontz. *An Introductory Path to Quantum Theory—Using Mathematics to Understand the Ideas of Physics*. Springer Nature Switzerland, 2020.
- F. Hiai and D. Petz. *Introduction to Matrix Analysis and Applications*. Universitext, 2014.
- Fuzhen Zhang. *Matrix Theory: Basic Results and Techniques*. Springer-Verlag New York, 2011.
- R. Bhatia. *Matrix Analysis*. Springer, 1997.
- N. J. Higham. *Functions of Matrices: Theory and Computation*. Society for Industrial and Applied Mathematics, 2008.