Lecture 6

Elements of linear algebra

Before we introduce the formalism of quantum theory we will review some basics of linear algebra. This should serve both as a reminder of these facts and also as an opportunity to see some of the notation we are going to use.

6.1 Complex Euclidean spaces

Modern quantum mechanics is defined in the language of functional analysis, using the notion of complex *Hilbert spaces*. Since large parts of quantum information theory can be studied using finite-dimensional spaces, we will restrict to this case throughout this course. We start with the following definition:

Definition 6.1 (Complex Euclidean space)**.** *A complex Euclidean space is a finite-dimensional vector space $\mathcal{H}$ equipped with a complex form $\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ with the following properties:*

1. *We have $\langle x|x\rangle \geq 0$ for every $x \in \mathcal{H}$, with equality if and only if $x = 0$.*
2. *We have $\langle x + \lambda y|z\rangle = \langle x|y\rangle + \overline{\lambda}\langle y|z\rangle$ for every $x, y, z \in \mathcal{H}$ and every $\lambda \in \mathbb{C}$.*
3. *We have $\langle x|y\rangle = \overline{\langle y|x\rangle}$ for every $x, y \in \mathcal{H}$.*

These properties guarantee that the function $x \mapsto \sqrt{\langle x|x\rangle}$ defines a norm on $\mathcal{H}$. This norm is called the Euclidean norm *or* 2-norm *and it is denoted by $\|\cdot\|_2$.*

Note that we define the inner product to be conjugate-linear in the first argument and linear in the second argument, which is the usual convention in the physics literature (contrary to the mathematics literature).

Every vector space has a basis, but on Euclidean spaces there is a stronger notion:

Definition 6.2 (Orthonormal basis)**.** *An* orthonormal basis *is a set of vectors $\{x_1, \ldots, x_n\}$ that is maximal with the following properties*[1]*:*

1. *We have $\|x_i\|_2 = \langle x_i|x_i\rangle = 1$ for all $i \in \{1, \ldots, n\}$.*
2. *We have $\langle x_i|x_j\rangle = 0$ whenever $i \neq j$.*

An orthonormal basis is, in particular, a basis. Hence, the cardinality $n \in \mathbb{N}$ of an orthonormal basis of $\mathcal{H}$ coincides with the dimension $\dim(\mathcal{H})$. Given an orthonormal basis $\{x_1, \ldots, x_n\}$ of a complex Euclidean space $\mathcal{H}$, we can write any element $y \in \mathcal{H}$ as a linear combination

$$y = \sum_{i=1}^{n} \langle x_i|y\rangle x_i. \tag{6.1}$$

[1] i.e., it cannot be extended by an additional vector x_{n+1} such that the properties still hold.

Another way of saying this, is that the identity map $\mathbb{1}_{\mathcal{H}} : \mathcal{H} \to \mathcal{H}$ admits the decomposition

$$\mathbb{1}_{\mathcal{H}} = \sum_{i=1}^{n} \langle x_i | \cdot \rangle x_i. \tag{6.2}$$

Recall the following theorem:

Theorem 6.3. *Every complex Euclidean space has an orthonormal basis.*

By choosing an orthonormal basis, any complex Euclidean $\mathcal{H}$ can be identified with $\mathbb{C}^d$ equipped with the standard inner product and for $d = \dim(\mathcal{H})$. *Throughout this course, we will always make this identification implicitely, and when saying "complex Euclidean space" we always mean $\mathbb{C}^d$ for some $d \in \mathbb{N}$.* We will usually denote complex Euclidean spaces by $\mathcal{H}$ and we will be using indices such as $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_{AB}, \ldots$ to keep track of different Euclidean spaces. Moreover, we will sometimes omit the "complex" in "complex Euclidean spaces" for brevity: When saying "Euclidean space" we will always mean "complex Euclidean space" in these lecture notes.

6.2 The bra-ket notation

A fundamental property of Hilbert spaces is an identification with their dual space $\mathcal{H}^*$ known as Riesz' representation theorem:

Theorem 6.4 (Baby version of Riesz' representation)**.** *Let $\mathcal{H}$ denote a complex Euclidean space. For any linear functional $f : \mathcal{H} \to \mathbb{C}$ there is a unique $y \in \mathcal{H}$ satisfying*

$$f(x) = \langle y | x \rangle,$$

for all $x \in \mathcal{H}$. We sometimes write $f = y^\dagger$ to denote this functional.

Most researchers in quantum information theory use the so-called *bra-ket notation*, and we will do the same throughout the course. The basic idea of this notation is to cleverly encode the identification between a complex Euclidean space $\mathcal{H}$ and its dual space $\mathcal{H}^*$ given by Riesz' representation theorem. This is done by writing vectors in $\mathcal{H}$ using the notation $|x\rangle$ and to write the functional $y^\dagger$ associated to the vector $|y\rangle$ as $\langle y|$. The vectors $|x\rangle$ are usually called *kets* and the functionals $\langle y|$ are called *bras*. Applying a bra $\langle y|$ to a ket $|x\rangle$ creates a *bra-ket* (or bracket) $\langle y|x\rangle$, i.e., the inner product of two vectors in $\mathcal{H}$. Note that the correspondence from Riesz' representation theorem associates to a ket $\lambda|x\rangle$ the bra $\overline{\lambda}\langle x|$, since otherwise the conjugation in first entry of the inner product would not be reproduced. We sometimes say that the identification of $|x\rangle$ and $\langle x|$ is conjugate-linear instead of just linear. Working with the bra-ket notation is very natural in the setting of complex Euclidean spaces, and even if you are skeptical now, please give it a chance.

It is helpful to make the identification from Riesz' representation theorem explicit in a fixed basis. By choosing an orthonormal basis of $\mathcal{H}$, we can always identify $\mathcal{H}$ with the space $\mathbb{C}^d$ (equipped with the usual inner product) where $d = \dim(\mathcal{H})$. We will often assume that some orthonormal basis for $\mathcal{H}$ is serving as a standard basis, which we will refer to as the *computational basis*. The term "computational basis" is inspired by quantum computing, where a quantum system is used to do some computation and where the computational basis serves as a reference for information stored in the system. We will commonly denote the

computational basis by $\{|1\rangle, \ldots, |d\rangle\}$, and in the case where $\mathcal{H} = \mathbb{C}^d$, we will simply set

$$|i\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

with the 1 appearing in the ith position.

Using the computational basis $\{|1\rangle, \ldots, |d\rangle\} \subset \mathcal{H}$, we may define a corresponding (dual) basis of $\mathcal{H}^*$ by $\{\langle 1|, \ldots, \langle d|\}$ such that

$$\langle i| \left(|j\rangle\right) = \langle i|j\rangle = \delta_{ij},$$

for any $i, j \in \{1, \ldots, d\}$. How does the identification $|x\rangle \leftrightarrow \langle x|$ look like with respect to these bases. Using that the identification of $|x\rangle$ and $\langle x|$ is conjugate-linear we find

$$|x\rangle = \sum_{i=1}^{d} x_i |i\rangle \leftrightarrow \langle x| = \sum_{i=1}^{d} \overline{x_i} \langle i|,$$

i.e., where we conjugate the coefficients on the right-hand side. It should be noted that this formula works for any choice of orthonormal basis, and it expresses the map $|x\rangle \mapsto |x\rangle^\dagger = \langle x|$ as the composition of a transpose, i.e., the map $|i\rangle \mapsto \langle i|$ considered as a linear map on the basis vectors, and a conjugation of the coordinates in the basis $\{|1\rangle, \ldots, |d\rangle\} \subset \mathcal{H}$.

In the case of $\mathcal{H} = \mathbb{C}^d$ we can express the kets living in $\mathbb{C}^d$ as "column vectors", and consequently we should think of the corresponding bras as "row vectors". For vectors

$$|x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \quad \text{and} \quad |y\rangle = \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix}$$

in $\mathbb{C}^d$ we can therefore compute their inner product in the usual way, by setting

$$\langle x|y\rangle = (\overline{x_1}, \ldots, \overline{x_d}) \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} = \sum_i \overline{x_i} y_i.$$

The bra-ket notation has many advantages when working with complex Euclidean spaces. For example, it is very useful to write $|x\rangle\langle y| : \mathcal{H} \to \mathcal{H}$ for the linear map acting as

$$|x\rangle\langle y| \left(|z\rangle\right) = \langle y|z\rangle |x\rangle$$

on vectors $|z\rangle \in \mathcal{H}$. You might recall that any orthonormal basis $\{x_1, \ldots, x_d\}$ of a complex Euclidean space $\mathcal{H}$ has the property that

$$|x\rangle = \sum_{i=1}^{d} \langle x_i|x\rangle |x_i\rangle,$$

for any $|x\rangle \in \mathcal{H}$. Using bra-ket notation, we can express this by decomposing the identity operator as

$$\mathbb{1}_{\mathcal{H}} = \sum_{i=1}^{d} |x_i\rangle\langle x_i|. \tag{6.3}$$

Maps of the form $|x\rangle\langle x|$ for $|x\rangle \in \mathcal{H}$ satisfying $\langle x|x\rangle = 1$ are easily seen to be projections since

$$|x\rangle\langle x| \cdot |x\rangle\langle x| = |x\rangle\langle x|x\rangle\langle x| = |x\rangle\langle x|,$$

and they are of rank 1 since their image is $\mathrm{span}\{|x\rangle\}$. We therefore note that (6.3) decomposes the identity operator as a sum of rank-1 projections, and this equation holds whenever $\{|x_1\rangle, \ldots, |x_d\rangle\}$ is an orthonormal basis of $\mathcal{H}$.

6.3 Linear operators and the Hilbert-Schmidt inner product space

In the following, let $\mathcal{H} = \mathbb{C}^d$, $\mathcal{H}_A = \mathbb{C}^{d_A}$ and $\mathcal{H}_B = \mathbb{C}^{d_B}$ denote complex Euclidean spaces. For any linear operator $L : \mathcal{H}_A \to \mathcal{H}_B$, we define the *operator norm* as

$$\|L\| = \sup_{x \in \mathcal{H}_A} \frac{\|Lx\|_2}{\|x\|_2}.$$

We will denote by $B(\mathcal{H}_A, \mathcal{H}_B)$ the set of (bounded) linear operators from $\mathcal{H}_A$ to $\mathcal{H}_B$, and by $B(\mathcal{H})$ the set of (bounded) linear operators from $\mathcal{H}$ into itself. Of course, every linear operator between complex Euclidean spaces (which are by definition finite-dimensional) is automatically bounded. We choose this notation anyway, since it is standard in functional analysis. Using the computational basis, we can identify operators in $B(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ with $d_B \times d_A$-matrices with complex entries. Throughout this course, we will often use these two descriptions interchangeably.

Let us briefly mention some operations on linear operators: Given linear operators $L_1, L_2 \in B(\mathcal{H})$, we denote their *commutator* by

$$[L_1, L_2] = L_1 L_2 - L_2 L_1,$$

and their *anticommutator* by

$$\{L_1, L_2\} = L_1 L_2 + L_2 L_1.$$

We say that the operators L_1 and L_2 *commute* if $[L_1, L_2] = 0$ and that they *anticommute* if $\{L_1, L_2\} = 0$. These notions will play an important role in the foundations of quantum mechanics. We will also need the trace functional: After fixing an orthonormal basis $\{x_1, \ldots, x_d\}$ of $\mathcal{H}$, we may define a functional $\mathrm{Tr} : B(\mathcal{H}) \to \mathbb{C}$ by

$$\mathrm{Tr}[L] = \sum_{i=1}^{d} \langle x_i|L|x_i\rangle,$$

for any $L \in B(\mathcal{H})$. It can be shown, that this definition does not depend on the choice of the orthonormal basis, and we might as well consider the computational basis. Therefore, we can take it as a general definition of the *trace*. Note that $\mathrm{Tr}[L] = \sum_{i=1}^{d} \lambda_i$, where λ_i are the eigenvalues of L, i.e., the d complex roots of the characteristic polynomial with multiplicities. This will sometimes be useful.

Next, we will review the notion of adjoints:

Definition 6.5 (Adjoint operator)**.** *For any linear operator $L \in B(\mathcal{H}_A, \mathcal{H}_B)$ we define the* adjoint *$L^\dagger \in B(\mathcal{H}_B, \mathcal{H}_A)$ as the unique operator satisfying*

$$\langle y|Lx\rangle = \langle L^\dagger y|x\rangle,$$

for every $|x\rangle \in \mathcal{H}_A$ and $|y\rangle \in \mathcal{H}_B$.

The adjoint operation takes a concrete form when expressed in the computational basis, and we have

$$L^\dagger = \overline{L}^T,$$

where $\overline{(\cdot)}$ denotes the entrywise complex conjugation, and $(\cdot)^T$ the matrix transpose in the computational basis. If not stated otherwise, all transposes and complex conjugations of operators should be understood in the computational basis (although it is usually possible to choose another basis without changing the definitions).

The vector space $B(\mathcal{H}_A, \mathcal{H}_B)$ is itself a complex Euclidean space when equipped with the *Hilbert-Schmidt* inner product

$$\langle L_1, L_2 \rangle_{HS} = \mathrm{Tr}\left[L_1^\dagger L_2\right],$$

for $L_1, L_2 \in B(\mathcal{H}_A, \mathcal{H}_B)$. Using the computational basis, we can define a canonical orthonormal basis for the Hilbert-Schmidt inner product space $B(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$:

Definition 6.6 (Matrix units)**.** *For $i \in \{1, \ldots, d_A\}$ and $j \in \{1, \ldots, d_B\}$ we define the* matrix units *as*

$$|i\rangle\langle j| = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

with the 1 appearing in the (i, j)th position. The matrix units form an orthonormal basis of $B(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ with the Hilbert-Schmidt inner product.

The Hilbert-Schmidt inner product can be understood as the usual inner product on $\mathbb{C}^{d_A d_B}$ by "viewing matrices as vectors", i.e., by taking the entries of the corresponding matrix as the entries of a vector. The corresponding 2-norm, given by $\|L\|_{HS} = \sqrt{\langle L, L\rangle_{HS}}$, is called the *Hilbert-Schmidt norm* or *Frobenius norm*.

Many important classes of operators can be defined by properties involving their adjoints. A linear operator $L \in B(\mathcal{H})$ is called

- *normal*, if $\left[L, L^\dagger\right] = 0$.
- *selfadjoint*, if $L = L^\dagger$.
- *projection*[2], if $L = L^\dagger = L^2$.
- *unitary*, if $L^{-1} = L^\dagger$.

We will denote the set of selfadjoint operators on $\mathcal{H}$ by $B(\mathcal{H})_{sa}$, the set of unitary operators on $\mathcal{H}$ by $\mathcal{U}(\mathcal{H})$, and the set of projections by $\mathrm{Proj}(\mathcal{H})$. All of these are subsets of the normal operators. We will often need the following normal form (no pun intended) of normal operators:

Theorem 6.7 (Spectral decomposition)**.** *For any normal operator $L \in B(\mathcal{H})$, there exists an orthonormal basis $\{|x_1\rangle, \ldots, |x_d\rangle\}$ of $\mathcal{H}$ consisting of eigenvectors of L such that*

$$L = \sum_{i=1}^{d} \lambda_i |x_i\rangle\langle x_i|,$$

[2]Some authors would call this an *orthogonal projection*, and they would refer to an operator satisfying $L = L^2$ as a projection. Throughout our course, we will only consider orthogonal projections and we will simply call them "projections" for brevity.

where $\lambda_i \in \mathbb{C}$ are the eigenvalues of L corresponding to the eigenvector $|x_i\rangle$.

The spectral decomposition is often referred to as a *diagonalization*, since the matrix corresponding to the operator L in the orthonormal basis $\{|x_1\rangle, \ldots, |x_d\rangle\}$ is diagonal. If two normal operators $L_1, L_2 \in B(\mathcal{H})$ commute, then there exists an orthonormal basis $\{|x_1\rangle, \ldots, |x_d\rangle\}$ of joint eigenvectors such that

$$L_1 = \sum_{i=1}^{d} \lambda_i |x_i\rangle\langle x_i| \quad \text{and} \quad L_2 = \sum_{i=1}^{d} \mu_i |x_i\rangle\langle x_i|,$$

where $\lambda_i, \mu_i \in \mathbb{C}$ are the eigenvalues of L_1 and L_2, respectively. In this case, we also say that L_1 and L_2 are *simultaneously diagonalizable*.

6.4 Applying functions to (normal) operators

How can we apply functions such as exp or log to operators in $B(\mathcal{H})$? A priori, there is no inherently correct way of defining an expression like $\exp(X)$ for a linear operator $X \in B(\mathcal{H})$, and it would be nice if this could be done in some consistent way preserving the usual composition rules of functions. Constructions to achieve this goal run under the name "functional calculus", and they differ in the kinds of functions and subsets of $B(\mathcal{H})$ they apply to. For this course, we will mostly need to apply functions on normal operators, and here the spectral decomposition will lead to a general theory. For completeness, we will briefly mention two classes of functions where it is intuitively clear how to apply them to operators.

First, consider a function $f : \mathbb{C} \to \mathbb{C}$ given by a polynomial, i.e.,

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots a_1 x + a_0,$$

with complex coefficients $a_0, \ldots, a_k \in \mathbb{C}$. Since $B(\mathcal{H})$ is an algebra with unit element $\mathbb{1}_{\mathcal{H}}$, it is clear how to define the operator $f(X) \in B(\mathcal{H})$ for any linear operator $X \in B(\mathcal{H})$. We simply set

$$f(X) = a_k X^k + a_{k-1} X^{k-1} + \cdots a_1 X + a_0 \mathbb{1}_{\mathcal{H}} \in B(\mathcal{H}).$$

From this example it is also clear how to apply certain non-polynomial functions on operators. Consider an entire function $f : \mathbb{C} \to \mathbb{C}$, i.e., a function f that is analytic everywhere in $\mathbb{C}$. Such a function can be expressed as a power series $f(x) = \sum_{k=0}^{\infty} a_k x^k$ which is absolutely convergent in $\mathbb{C}$. Consider a linear operator $X \in B(\mathcal{H})$. How should we define $f(X)$? To make this expression consistent with the expression for polynomials, we should define

$$f(X) = \lim_{N \to \infty} \sum_{k=0}^{N} a_k X^k =: \sum_{k=0}^{\infty} a_k X^k,$$

where we set $X^0 = \mathbb{1}_{\mathcal{H}}$. Does this define a linear operator? Yes, it does! It is easy to check that

$$\|f(X)\| \leq \sum_{k=0}^{\infty} |a_k| \|X\|^k < \infty.$$

An example where this construction can be applied is the exponential function $\exp(X)$, which is defined for any linear operator $X \in B(\mathcal{H})$ on the Euclidean space $\mathcal{H}$.

Obviously, not all complex functions are entire and during the course we will occasionally apply the logarithm to linear operators. Luckily, we do not need to apply such functions to any linear operator $X \in B(\mathcal{H})$, but only to normal operators. Here, the spectral theorem can be applied:

Definition 6.8 (Functions of normal operators)**.** *Let $D \subseteq \mathbb{C}$ denote some subset of complex numbers, $f : D \to \mathbb{C}$ a complex function and $X \in B(\mathcal{H})$ a normal operator with spectrum $\sigma(X) \subseteq D$. Then, we define*

$$f(X) = \sum_{i=1}^{d} f(\lambda_i)|x_i\rangle\langle x_i|,$$

where $\{|x_1\rangle, \ldots, |x_d\rangle\}$ is an orthonormal basis of eigenvectors of X (which exists by Theorem 6.7).

The reader should convince themselves that Definition 6.8 for a normal operator X gives the same operator $f(X)$ as derived above when f is a polynomial or an entire function.

6.5 Positive operators

We will also need the set of positive semidefinite operators:

Definition 6.9 (Positive operators)**.** *A linear operator $P \in B(\mathcal{H})$ is called* positive semidefinite *if*

$$\langle x|P|x\rangle \geq 0,$$

for any $|x\rangle \in \mathcal{H}$. If the previous inequality is always strict, we will call the operator positive definite*.*

For brevity, we will usually refer to positive semidefinite operators simply as *positive operators*. Note that this includes the zero operator! This is in contrast to real numbers, where we usually say *non-negative* to denote the positive real numbers and zero. The following theorem collects alternative characterizations of positive operators:

Theorem 6.10 (Characterizing positive operators)**.** *For a linear operator $P \in B(\mathcal{H})$ the following are equaivalent:*

1. *P is positive.*
2. *P is selfadjoint and has non-negative eigenvalues.*
3. *There exists a positive operator $Q \in B(\mathcal{H})$ such that $P = Q^2$.*
4. *There exists an operator $X \in B(\mathcal{H})$ such that $P = X^\dagger X$.*
5. *There exists an operator $Y \in B(\mathcal{H}, \mathcal{H}')$ for some Euclidean space $\mathcal{H}'$ such that $P = Y^\dagger Y$.*

The operator Q in 3. is unique and it is called the positive square root *of P. We will write $\sqrt{P}$ or $P^{1/2}$ to denote it.*

Proof. We will first show that 1. and 2. are equivalent. Assume that P is positive as in Definition 6.9. For any $x, y \in \mathcal{H}$ we have

$$\langle x + iy, P(x + iy)\rangle = \langle x, Px\rangle + \langle y, Py\rangle + i\left(\langle x, Py\rangle - \langle y, Px\rangle\right) \geq 0.$$

We conclude that $\mathrm{Re}\left(\langle x, Py\rangle - \langle y, Px\rangle\right) = 0$ and hence that

$$\mathrm{Re}\left(\langle P^\dagger x, y\rangle\right) = \mathrm{Re}\left(\langle Px, y\rangle\right), \tag{6.4}$$

for all $x, y \in \mathcal{H}$. Substituting $iy \mapsto y$ in (6.4) shows that the same equality also holds for the imaginary parts and hence that $\langle P^\dagger x, y\rangle = \langle Px, y\rangle$ for all $x, y \in \mathcal{H}$. Therefore, P is selfadjoint. Clearly, P has positive eigenvalues, since otherwise, there would be a normalized eigenvector $|x\rangle$ satisfying $\langle x|P|x\rangle < 0$ and contradicting our assumption.

For the other direction, assume that P is selfadjoint (and in particular normal) and has positive eigenvalues. By the spectral decomposition, Theorem 6.7, we can write

$$P = \sum_{i=1}^{d} \lambda_i |x_i\rangle\langle x_i|, \tag{6.5}$$

for an orthonormal basis $\{|x_1\rangle, \ldots, |x_d\rangle\}$ of $\mathcal{H}$ consisting of eigenvectors of P, and with the positive eigenvalues $\lambda_i \geq 0$. For any $|y\rangle \in \mathcal{H}$ we can verify that

$$\langle y|P|y\rangle = \sum_{i=1}^{d} \lambda_i |\langle y|x_i\rangle|^2 \geq 0,$$

and hence P is positive.

Now, we show the rest of the equivalences. Assume that P is selfadjoint and has positive eigenvalues, and consider the spectral decomposition (6.5). We can now define a linear operator $Q \in B(\mathcal{H})$ by

$$Q = \sum_{i=1}^{d} \sqrt{\lambda_i} |x_i\rangle\langle x_i|.$$

By the equivalence of 1. and 2., we conclude that Q is positive. Furthermore, it is easy to check that $Q^2 = P$ showing that 3. holds.

It is clear that 3. implies 4. and that 4. implies 5.. Finally, we assume that there exists an operator $Y \in B(\mathcal{H}, \mathcal{H}')$ for some Euclidean space $\mathcal{H}'$ such that $P = Y^\dagger Y$. For any $|x\rangle \in \mathcal{H}$ we have

$$\langle x|P|x\rangle = \langle x|Y^\dagger Y|x\rangle = \langle Yx|Yx\rangle \geq 0,$$

and hence P is positive.

Finally, we need to show that the positive square root in 3. is unique. By polynomial interpolation, there exists a polynomial $f \in \mathbb{R}[X]$ with real coefficients satisfying $f(\lambda_i) = \sqrt{\lambda_i}$ for all eigenvalues $\lambda_1, \ldots, \lambda_d \geq 0$ of P. By the spectral theorem, we conclude that

$$Q = f(P). \tag{6.6}$$

Assume now, that there is another positive operator $\tilde{Q} \in B(\mathcal{H})^+$ satisfying $\tilde{Q}^2 = P$. By the spectral theorem we have $\tilde{Q} = \sum_{i=1}^{d} \mu_i |v_i\rangle\langle v_i|$ and therefore $P = \sum_{i=1}^{d} \mu_i^2 |v_i\rangle\langle v_i|$ for some $\mu_i \geq 0$ and an orthonormal basis of eigenvectors $\{|v_1\rangle, \ldots, |v_d\rangle\} \subset \mathcal{H}$. Since $\left[\tilde{Q}, P\right] = 0$, we conclude, by (6.6), that

$$\left[Q, \tilde{Q}\right] = 0.$$

Now, we know that there exists a common orthonormal basis of eigenvectors $\{|w_1\rangle, \ldots, |w_d\rangle\} \subset \mathcal{H}$ such that $Q = \sum_{i=1}^{d} \nu_i |w_i\rangle\langle w_i|$ and $\tilde{Q} = \sum_{i=1}^{d} \mu_i |w_i\rangle\langle w_i|$. By assumption, we have $\nu_i^2 = \mu_i^2$ for every $i \in \{1, \ldots, d\}$. Since $\nu_i, \mu_i \geq 0$, we conclude that $\mu_i = \mu_i'$ for all $i \in \{1, \ldots, d\}$ and therefore $Q = \tilde{Q}$. □

Based on the notion of positivity, there is another useful decomposition of general linear operators:

Theorem 6.11 (Singular value decomposition)**.** *For any linear operator $L \in B(\mathcal{H}_A, \mathcal{H}_B)$ there exist orthonormal bases $\{|x_1\rangle, \ldots, |x_{d_A}\rangle\}$ of $\mathcal{H}_A$ and $\{|y_1\rangle, \ldots, |y_{d_B}\rangle\}$ of $\mathcal{H}_B$ such that*

$$L = \sum_{i=1}^{R} s_i |y_i\rangle\langle x_i|,$$

for strictly positive $s_i \in \mathbb{R}^+$ called singular values *of L, and where R equals the rank of L.*

The singular value decomposition can also be written in a non-reduced form by setting

$$L = \sum_{i=1}^{D} s_i |y_i\rangle\langle x_i|,$$

with $D = \min(d_A, d_B)$ and where some singular values may be zero. Sometimes this is convenient, e.g., when we want to avoid mentioning the rank of L.

Proof. Consider the positive operators $L^\dagger L \in B(\mathcal{H}_A)$ and $LL^\dagger \in B(\mathcal{H}_B)$ and assume without loss of generality that $d_A \geq d_B$ (otherwise, exchange the roles of L and $L^\dagger$ in the following proof). By the spectral decomposition, there exists an orthonormal basis $\{|x_1\rangle, \ldots, |x_{d_A}\rangle\}$ of $\mathcal{H}_A$ consisting of eigenvectors of $L^\dagger L$ such that

$$L^\dagger L = \sum_{i=1}^{d_A} \lambda_i |x_i\rangle\langle x_i|,$$

where $\lambda_i \geq 0$ are the eigenvalues of $L^\dagger L$. We set

$$R = \#\{i \in \{1, \ldots, d_A\} \ : \ \lambda_i \neq 0\},$$

and we assume without loss of generality that $\lambda_1, \ldots, \lambda_R \neq 0$ and $\lambda_i = 0$ for any $i > R$. Since

$$\| L|x_i\rangle \|_2^2 = \langle x_i | L^\dagger L | x_i \rangle = \lambda_i,$$

we conclude that $L|x_i\rangle = 0$ if and only if $\lambda_i = 0$, and therefore R coincides with the rank of the linear operator L. Next, observe that

$$LL^\dagger \left(L|x_i\rangle\right) = L\left(L^\dagger L |x_i\rangle\right) = \lambda_i L|x_i\rangle,$$

for any $i \in \{1, \ldots, d_A\}$. For any $i \in \{1, \ldots, R\}$ we can define an eigenvector

$$|y_i\rangle := \frac{L|x_i\rangle}{\sqrt{\lambda_i}} \neq 0,$$

of the operator $LL^\dagger$ corresponding to eigenvalue λ_i. With this definition, we can verify that

$$\langle y_i | y_j \rangle = \frac{\langle x_i | L^\dagger L | x_j \rangle}{\sqrt{\lambda_i \lambda_j}} = \delta_{ij},$$

for all $i, j \in \{1, \ldots, R\}$, and we conclude that $\{|y_1\rangle, \ldots, |y_R\rangle\}$ is a set of orthonormal vectors in $\mathcal{H}_B$. Extending this set gives an orthonormal basis $\{|y_1\rangle, \ldots, |y_{d_B}\rangle\}$. Finally, we can check that

$$L|x_i\rangle = \sqrt{\lambda_i}|y_i\rangle,$$

for all $i \in \{1, \ldots, R\}$ and, since R is the rank of L, we obtain the singular value decomposition with singular values $s_i = \sqrt{\lambda_i}$.

□

We will sometimes need the fact that the positive semidefinite operators span the space $B(\mathcal{H})$. The next two theorems will show this:

Theorem 6.12 (Jordan-Hahn decomposition)**.** *Every selfadjoint operator $H \in B(\mathcal{H})_{sa}$ can be written as $H = P - Q$, where $P, Q \in B(\mathcal{H})^+$ are positive semidefinite and satisfy $PQ = 0$.*

Proof. This theorem is a consequence of the spectral decomposition. If $H \in B(\mathcal{H})_{sa}$ is a selfadjoint operator, then we can consider its spectral decomposition $H = UDU^\dagger$ with a diagonal operator $D \in B(\mathcal{H})$ and a unitary operator $U \in \mathcal{U}(\mathcal{H})$. Now, let D^+, D^- denote the positive and negative part of the operator D, i.e., both D^+ and D^- are diagonal with non-negative diagonal entries

$$D^+_{ii} = \begin{cases} D_{ii} & , \text{ if } D_{ii} \geq 0 \\ 0 & , \text{ otherwise,} \end{cases}, \quad D^-_{ii} = \begin{cases} -D_{ii} & , \text{ if } D_{ii} < 0 \\ 0 & , \text{ otherwise,} \end{cases}$$

for any $i \in \{1, \ldots, \dim(\mathcal{H})\}$. Note that by definition $D^+D^- = 0$. Now, we define positive semidefinite operators $P = UD^+U^\dagger$ and $Q = UD^-U^\dagger$. Clearly, we have $PQ = UD^+D^-U^\dagger = 0$ and $P - Q = U(D^+ - D^-)U^\dagger = H$. □

Theorem 6.13. *Every operator $X \in B(\mathcal{H})$ can be written as $X = H_1 + iH_2$, where $H_1, H_2 \in B(\mathcal{H})_{sa}$ are selfadjoint. Moreover, there exist positive semidefinite operators P_1, P_2, Q_1, Q_2 such that*

$$X = P_1 - Q_1 + i(P_2 - Q_2).$$

Proof. Consider an operator $X \in B(\mathcal{H})$ and define selfadjoint operators

$$H_1 = \frac{1}{2}\left(X + X^\dagger\right), \quad H_2 = \frac{1}{2i}\left(X - X^\dagger\right).$$

With these operators we have $X = H_1 + iH_2$. Finally, we can apply Theorem 6.12 to the selfadjoint operators H_1 and H_2 showing that $H_1 = P_1 - Q_1$ and $H_2 = P_2 - Q_2$ for positive semidefinite operators P_1, P_2, Q_1, Q_2. By construction, we have $X = P_1 - Q_1 + i(P_2 - Q_2)$. □

The previous theorem shows that every the vector space $B(\mathcal{H})$ is spanned by the operators in $B(\mathcal{H})^+$. The set $B(\mathcal{H})^+$ forms a convex cone, often called the *PSD cone*. Our argument from above shows that the real span of the operators in this cone is the real vector space $B(\mathcal{H})_{sa}$. One says that a cone is *generating* if it has this property.