Introduction to

Quantum Information Theory

Prof. Dr. Volker Bach

Technische Universität Braunschweig
Sommersemester 2025

Version as of 02-Jun-2025

Contents

I. Mathematical Prerequisites

I.1. Analysis in one and several Real Variables

We list a few topics from analysis in one and in several real variables that we assume the reader to be familiar with:

- Real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, and their d-fold cartesian products $\mathbb{R}^d$ and $\mathbb{C}^d$, $d \in \mathbb{N}$.
- Real and complex sequences, series, their convergence, and criteria to decide for convergence or divergence.
- Basic topological notions such as inner points, accumulation points, open sets, closed sets, compact sets in $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^d$, and $\mathbb{C}^d$.
- Continuity of maps and its various characterizations.
- Differentiability and basic rules of differentiation, such as Leibniz rule and the chain rule.
- (Riemann) Integration, integration by parts, the fundamental theorem of calculus.
- Partial derivatives, gradient, and Jacobi matrix.
- Local extrema, local extrema under constraints, method of Lagrange multipliers.
- Integration of several variables.
- Basic inequalities: Cauchy-Schwarz, Hölder, Minkowski.

I.2. Introductory Linear Algebra

We also list a few topics from linear algebra that we assume the reader to be familiar with:

- Real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, and their d-fold cartesian products $\mathbb{R}^d$ and $\mathbb{C}^d$, $d \in \mathbb{N}$.

- Vector spaces, subspaces, linear span and their generating sets.
- Linear dependence, linear independence, basis, and dimension.
- Linear maps and their matrix representations.
- Matrices, matrix product, deteminants, equivalence of invertibility of a matrix to the nonvanishing of its determinant.
- Eigenvalues and eigenvectors, diagonalizability.

I.3. Norms and Scalar Products

I.3.1. Banach Spaces

In this section we define Banach spaces and collect some of their basic properties. We recall that $\mathbb{K}$ denotes the field $\mathbb{R}$ of real numbers or the field $\mathbb{R}$ of complex numbers. Statements made involving $\mathbb{K}$ hold for both $\mathbb{K} = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$.

Definition I.1. Let X be a $\mathbb{K}$-vector space. A map $\|\cdot\| : X \to \mathbb{R}_0^+$ is called **Norm (on X)** :$\Leftrightarrow$

(i)

$$\forall\, x \in X: \qquad \big\{\|x\| = 0 \;\Leftrightarrow\; x = 0\big\} \tag{I.1}$$

(ii)

$$\forall\, x \in X,\ \lambda \in \mathbb{K}: \qquad \|\lambda x\| \;=\; |\lambda| \cdot \|x\|, \tag{I.2}$$

(iii)

$$\forall\, x, y \in X: \qquad \|x + y\| \;\leq\; \|x\| + \|y\|. \tag{I.3}$$

In this case $(X, \|\cdot\|)$ is said to be a **normed (vector) space**. We denote by

$$B_X(x, r) \;:=\; \big\{y \in X \;\big|\|x - y\| < r\big\} \tag{I.4}$$

the **open ball about $x \in X$ of radius $r > 0$**.

Definition I.2. Let $(X, \|\cdot\|)$ be a normed vector space over $\mathbb{K}$.

(i) A sequence $(x_n)_{n=1}^{\infty} \in X^{\mathbb{N}}$ is **convergent** :$\Leftrightarrow$

$$\exists x \in X\ \forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0: \quad \|x_n - x\| \leq \varepsilon. \tag{I.5}$$

(ii) A sequence $(x_n)_{n=1}^{\infty} \in X^{\mathbb{N}}$ is called **Cauchy sequence** :$\Leftrightarrow$

$$\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall m > n \geq n_0: \quad \|x_m - x_n\| \leq \varepsilon. \tag{I.6}$$

(iii) If every Cauchy sequence in X is convergent, $(X, \|\cdot\|)$ is said to be **complete**, and we call $(X, \|\cdot\|)$ a **Banach space**.

(iv) A subset $S \subseteq X$ is **dense**, if $\overline{S} = X$ or, equivalently, if

$$\forall\, x \in X\,,\ \varepsilon > 0\ \exists\, y_\varepsilon \in S: \qquad \|x - y_\varepsilon\| \ \leq\ \varepsilon\,. \tag{I.7}$$

Remarks and Examples. We first list a few examples of Banach spaces.

- For $d \in \mathbb{N}$ the $\mathbb{K}$-vector space $\big(\mathbb{K}^d, \|\cdot\|_2\big)$ is a Banach space with respect to the euclidean/unitary norm $\|x\|_2 := \langle x|x\rangle^{1/2}$, with $\langle x|y\rangle := \sum_{\nu=1}^d x_\nu y_\nu$ ($\mathbb{K} = \mathbb{R}$) or $\langle x|y\rangle := \sum_{\nu=1}^d \overline{x}_\nu y_\nu$ ($\mathbb{K} = \mathbb{C}$).
- For $d \in \mathbb{N}$ and $1 \leq p < \infty$, the vector space $\big(\mathbb{K}^d, \|\cdot\|_p\big)$ is a $\mathbb{K}$-Banach space with respect to the p-norm $\|x\|_p := \big(|x_1|^p + \ldots + |x_d|^p\big)^{1/p}$. The triangle inequality $\|x+y\|_p \leq \|x\|_p + \|y\|_p$ is the classical Minkowski inequality in analysis.
- For $d \in \mathbb{N}$, the vector space $\big(\mathbb{K}^d, \|\cdot\|_\infty\big)$ is a $\mathbb{K}$-Banach space with respect to the supremum norm or ∞-norm $\|x\|_\infty := \max\big(|x_1|, \ldots, |x_d|\big)$. This corresponds to the case $p = \infty$.
- Recall that a **subspace** of a $\mathbb{K}$-vector space X is a subset $Z \subseteq X$ which itself is a $\mathbb{K}$-vector space. If $\big(X, \|\cdot\|_X\big)$ is a Banach space and $Z \subseteq X$ is a subspace then $\big(Z, \|\cdot\|_X\big)$ is itself a Banach space if, and only if, it is a closed subset of X.

I.3.2. Linear Operators

Definition I.3. Let $(X, \|\cdot\|_X)$ and $(Y, \|\cdot\|_Y)$ be two $\mathbb{K}$-Banach spaces. Wir denote by

$$\mathcal{B}(X;Y) \ := \ \Big\{ A : X \to Y \ \Big|\ A \text{ is linear},\ \|A\|_{\mathcal{B}(X;Y)} < \infty \Big\} \tag{I.8}$$

the space of **bounded (linear) operators (from X to Y)**, where

$$\|A\|_{\mathcal{B}(X;Y)} \ := \ \sup_{x \in X\setminus\{0\}} \left\{ \frac{\|Ax\|_Y}{\|x\|_X} \right\} \ = \ \sup_{x \in X, \|x\|_X = 1} \big\{ \|Ax\|_Y \big\} \tag{I.9}$$

is the **operator norm of A**. If no confusion is possible, we frequently write $\|\ \cdot\ \|_{\mathcal{B}(X;Y)} =: \|\cdot\|_{\mathrm{op}}$.

Remarks and Examples.

- $\big(\mathcal{B}(X;Y), \|\cdot\|_{\mathcal{B}(X;Y)}\big)$ is itself a $\mathbb{K}$-Banach space, where the vector space structure is defined by $(A + \lambda B)(x) := A(x) + \lambda B(x)$.
- If $(X, \|\cdot\|_X)$ and $(Y, \|\cdot\|_Y)$ are two Banach spaces over $\mathbb{K}$ and $A : X \to Y$ is linear, then the following two statements are equivalent:

$$\big\{\ \|A\|_{\mathcal{B}(X;Y)} \ < \ \infty\ \big\} \qquad \Leftrightarrow \qquad \big\{\ A:\ X \to Y \text{ is continuous}\ \big\}. \tag{I.10}$$

I.3.3. Hilbert Spaces

In this section we define (complex) Hilbert spaces and collect some basic facts about these and about the spectral theory of bounded operators on Hilbert spaces.

Definition I.4.

(i) Let X be an $\mathbb{C}$-Vector space. A map $\langle\cdot|\cdot\rangle : X \times X \to \mathbb{R}$ is called **sesquilinear form (on X)**

$$:\Leftrightarrow \forall\, \alpha, \beta \in \mathbb{R}\, \forall\, x, y, w, z \in X : \quad \langle \alpha x + y \mid \beta w + z\rangle \;=\; \overline{\alpha}\beta\langle x|w\rangle + \overline{\alpha}\langle x|z\rangle + \beta\langle y|z\rangle + \langle y|z\rangle. \tag{I.11}$$

If furthermore

$$:\Leftrightarrow \forall\, x, y \in X : \quad \langle x|y\rangle \;=\; \overline{\langle y|x\rangle}, \tag{I.12}$$

holds true, the sesquilinear form $\langle\cdot|\cdot\rangle$ is called **symmetric**.

(ii) A symmetric sesquilinear form $\langle\cdot|\cdot\rangle : X \times X \to \mathbb{C}$ is called **positiv definite**

$$:\Leftrightarrow \quad \forall\, x \in X \setminus \{0\} : \quad \langle x|x\rangle \;>\; 0. \tag{I.13}$$

If only $\langle x|x\rangle \geq 0$ holds true, for all $x \in X$ (but possibly there are $x \neq 0$ with $\langle x|x\rangle = 0$), then $\langle\cdot|\cdot\rangle : X \times X \to \mathbb{C}$ is called **positiv semidefinite**.

(iii) If X is a $\mathbb{C}$-vector space and $\langle\cdot|\cdot\rangle : X \times X \to \mathbb{C}$ is a symmetric, positive definite sesquilinear form on X, then $\langle\cdot|\cdot\rangle$ is called **scalar product (X)** and $\big(X, \langle\cdot|\cdot\rangle\big)$ is called a **pre-Hilbert space**.

Theorem I.5 (Cauchy-Schwarz Inequality)**.** *If X is a $\mathbb{C}$-vector space equipped with a symmetric, positiv semidefinite sesquilinear form $\langle\cdot|\cdot\rangle : X \times X \to \mathbb{C}$ then*

$$\forall x, y \in X : \quad \big|\langle x|y\rangle\big| \;\leq\; \sqrt{\langle x|x\rangle}\,\sqrt{\langle y|y\rangle}. \tag{I.14}$$

Corollary I.6. *If $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a $\mathbb{C}$-pre-Hilbert space then*

$$\|\cdot\| : \mathcal{H} \;\to\; \mathbb{R}_0^+, \quad \|x\| \;:=\; \langle x|x\rangle^{1/2} \tag{I.15}$$

*defines a norm on $\mathcal{H}$, the **norm induced by** $\langle\cdot|\cdot\rangle$.*

Definition I.7. If a pre-Hilbert space $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ over $\mathbb{C}$ is complete with respect to the norm induced by $\langle\cdot|\cdot\rangle$, then we call $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ a **Hilbert space**.

Remarks and Examples.

- For $d \in \mathbb{N}$, the space $\big(\mathbb{C}^d, \langle\cdot|\cdot\rangle_{\text{unit}}\big)$ is a (complex) Hilbert space, where

$$\forall\, \vec{x} = (x_1, \ldots, x_d)^t\,,\ \vec{y} = (y_1, \ldots, y_d)^t \in \mathbb{C}^d : \quad \big\langle \vec{x} \big| \vec{y} \big\rangle_{\text{unit}} := \sum_{\nu=1}^{d} \overline{x_\nu}\, y_\nu \tag{I.16}$$

  defines the **unitary scalar product**.

- Let $(\Omega, \mathfrak{A}, \mu)$ be a measure space. Then $\big(L^2(\Omega;\mathbb{C}), \langle\cdot|\cdot\rangle\big)$ is a Hilbert space with scalar product

$$\forall f, g \in L^2(\Omega;\mathbb{C}) : \qquad \langle f|g\rangle := \int_\Omega \overline{f(\omega)}\, g(\omega)\, d\mu(\omega). \tag{I.17}$$

Definition I.8. Suppose that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a Hilbert space.

(i) Two vectors $x, y \in \mathcal{H}$ are **orthogonal, $x \perp y$** $:\Leftrightarrow \langle x|y\rangle = 0$.

(ii) If $\mathcal{A} \subseteq \mathcal{H}$ is a subset then

$$\mathcal{A}^\perp := \big\{ x \in \mathcal{H} \,\big|\, \forall a \in \mathcal{A} : \ \langle a|x\rangle = 0 \big\} \tag{I.18}$$

is the **orthogonal complement to $\mathcal{A}$**.

(iii) A subset $\mathcal{B} \subseteq \mathcal{H}$ is called **orthonormal** $:\Leftrightarrow$

$$\forall x, y \in \mathcal{B},\ x \neq y : \qquad \langle x|x\rangle = \langle y|y\rangle = 1, \quad \langle x|y\rangle = 0. \tag{I.19}$$

(iv) A subset $\mathcal{E} \subseteq \mathcal{H}$ is called an **orthonormal basis (ONB) (of $\mathcal{H}$)**

$$\begin{aligned} :\Leftrightarrow \quad & \mathcal{E} \text{ is orthonormal} \quad \text{and} \quad \overline{\operatorname{span}(\mathcal{E})} = \mathcal{H} \\ \Leftrightarrow \quad & \mathcal{E} \text{ is orthonormal} \quad \text{and} \quad \text{for any given } x \in \mathcal{H} \text{ and } \varepsilon > 0 \\ & \exists\, e_1, \ldots, e_N \in \mathcal{E},\ \alpha_1, \ldots, \alpha_N \in \mathbb{C} : \ \Big\| x - \big(\alpha_1 e_1 + \ldots + \alpha_N e_N\big) \Big\| \ \leq\ \varepsilon\,. \end{aligned} \tag{I.20}$$

Remarks and Examples.

- For any subset $\mathcal{A} \subseteq \mathcal{H}$ its orthogonal complement $\mathcal{A}^\perp$ is a closed subspace.
- For any subset $\mathcal{A} \subseteq \mathcal{H}$, we have that $\mathcal{A} \cap \mathcal{A}^\perp \subseteq \{0\}$ is a closed subspace.
- If $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{H}$ then $\mathcal{A}^\perp \supseteq \mathcal{B}^\perp$.
- If a subset $\mathcal{A} \subseteq \mathcal{H}$ is orthonormal then it is linearly independent.
- The canonical basis $\{e_1, \ldots, e_d\} \subseteq \mathbb{C}^d$, with

$$e_1 \ = \ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 \ = \ \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots \quad e_d \ = \ \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \tag{I.21}$$

  is an ONB in $\mathbb{C}^d$ with respect to the euclidean or unitary scalar product, respectively.

Theorem I.9 (Gram-Schmidt Orthonormalization Procedure)**.** *Suppose that* $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ *is a separable Hilbert space. Then there exists a countable ONB* $\{e_n\}_{n=1}^{L} \subseteq \mathcal{H}$*, where* $L = \dim_{\mathbb{C}}(\mathcal{H}) \in \mathbb{N} \cup \{\infty\}$ *denotes the dimension of* $\mathcal{H}$*. If* $\{e_n\}_{n=1}^{L} \subseteq \mathcal{H}$ *is such an ONB, then*

$$\forall x \in \mathcal{H}: \qquad x \;=\; \sum_{n=1}^{L} \langle e_n|x\rangle \; e_n \,. \tag{I.22}$$

Remarks and Examples.

- Eq. (I.22) says that the coefficients in the approximation (I.20) can be computed by taking scalar products $\alpha_n = \langle e_n|x\rangle$.
- For $\varphi, \psi \in \mathcal{H}$ we use **Dirac's ket-bra notation** and define $|\varphi\rangle\langle\psi| \in \mathcal{B}(\mathcal{H})$ by

$$\forall x \in \mathcal{H}: \qquad |\varphi\rangle\langle\psi|(x) \;:=\; \langle\psi|x\rangle \; \varphi \,. \tag{I.23}$$

- Note that, given $\varphi, \psi \in \mathcal{H}$ and $A \in \mathcal{B}(\mathcal{H})$, we have for all $x \in \mathcal{H}$ that

$$\big[A \circ |\varphi\rangle\langle\psi|\big](x) \;=\; A\big[\langle\psi|x\rangle \; \varphi\big] \;=\; \langle\psi|x\rangle \; A(\varphi) \;=\; |A\varphi\rangle\langle\psi|(x) \tag{I.24}$$

  and

$$\Big\langle y\Big||\varphi\rangle\langle\psi|(x)\Big\rangle \;=\; \Big\langle y\Big|\langle\psi|x\rangle \; \varphi\Big\rangle \;=\; \langle\psi|x\rangle \; \langle y|\varphi\rangle \;=\; \Big\langle \langle\varphi|y\rangle \; \psi\Big|x\Big\rangle \;=\; \Big\langle |\psi\rangle\langle\varphi|(y)\Big|x\Big\rangle \,. \tag{I.25}$$

  Eqs. (I.24) and (I.25) imply that

$$A \circ |\varphi\rangle\langle\psi| \;=\; |A\varphi\rangle\langle\psi| \,, \;\; \big(|\varphi\rangle\langle\psi|\big)^* \;=\; |\psi\rangle\langle\varphi| \,, \;\text{ and }\; |\varphi\rangle\langle\psi| \circ A \;=\; |\varphi\rangle\langle A^*\psi| \,. \tag{I.26}$$

- If $L \in \mathbb{N} \cup \{\infty\}$ and $\{\varphi_1, \ldots, \varphi_L\} \subseteq \mathcal{H}$ is an ONB then (I.22) can be written by means of Dirac's ket-bra notation as a decomposition of the identity,

$$\mathbf{1}_{\mathcal{H}} \;=\; \sum_{n=1}^{L} |\varphi_n\rangle\langle\varphi_n| \,. \tag{I.27}$$

- If $N < \infty$ and $\{m_1, \ldots, m_N\} \subseteq \mathcal{M}$ is an ONB then the orthogonal projection $P \in \mathcal{B}(\mathcal{H})$ onto $\mathcal{M}$ is given by

$$P \;=\; \sum_{n=1}^{N} |m_n\rangle\langle m_n| \,. \tag{I.28}$$

Theorem I.10 (Riesz Representation Theorem)**.** *Let* $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ *be a Hilbert space and* $\mathcal{H}^* := \mathcal{B}(\mathcal{H}; \mathbb{C})$ *its dual space (see Definition I.11). Then, for every bounded linear functional* $\ell \in \mathcal{H}^*$*, there exists exactly one vector* $y_\ell \in \mathcal{H}$*, such that* $\ell = \langle y_\ell|\cdot\rangle$*, i.e.*

$$\forall x \in \mathcal{H}: \qquad \ell(x) \;=\; \langle y_\ell|x\rangle. \tag{I.29}$$

Furthermore $\|\ell\|_{\mathcal{H}^*} = \|y_\ell\|_{\mathcal{H}}$ *and*

$$\forall x \in \mathcal{H}: \qquad \|x\| \;=\; \sup\Big\{ |\langle y|x\rangle| \;\Big|\; y \in \mathcal{H} \,,\; \|y\| = 1 \Big\}. \tag{I.30}$$

Proof. We only give a proof of Eq. (I.30) because the argument is instructive. Note that (I.30) holds trivially true for $x = 0$, and we may assume that $x \neq 0$. We abbreviate the right side of (I.30) by

$$N(x) \;:=\; \sup\Big\{ |\langle y|x\rangle| \;\Big|\; y \in \mathcal{H}\,,\; \|y\| = 1 \Big\}\,. \tag{I.31}$$

If $y \in \mathcal{H}$ with $\|y\| = 1$ then the Cauchy-Schwarz inequality implies that

$$|\langle y|x\rangle| \;\leq\; \|x\| \cdot \|y\| \;=\; \|x\|\,. \tag{I.32}$$

Taking the supremum over all $y \in \mathcal{H}$ with $\|y\| = 1$, we obtain $N(x) \leq \|x\|$. Next we define $\hat{x} := \frac{1}{\|x\|} x \in \mathcal{H}$, which is possible thanks to $x \neq 0$, and observe that $\|\hat{x}\| = 1$. Hence,

$$\|x\| \;= \frac{\|x\|^2}{\|x\|} \;=\; \frac{\langle x|x\rangle}{\|x\|} \;=\; \langle \hat{x}|x\rangle \;\leq\; |\langle \hat{x}|x\rangle| \;\leq\; N(x)\,, \tag{I.33}$$

which yields $\|x\| \leq N(x)$. Hence $\|x\| = N(x)$. □

I.4. SUPPLEMENTARY MATERIAL

I.4.1. Banach Spaces

Remarks and Examples.

- For a normed space $(X, \|\cdot\|)$
- Let $(X, \|\cdot\|)$ be a normed space. The **norm topology** is the topology generated by the system of open balls in X.
- Two norms $\|\cdot\|_1, \|\cdot\|_2 : X \to \mathbb{R}_0^+$ on a $\mathbb{K}$-vector space X are called **equivalent**, if there exists a constant $c > 0$, such that

$$\forall\, x \in X : \qquad c\,\|x\|_1 \;\leq\; \|x\|_2 \;\leq\; c^{-1}\,\|x\|_1 \tag{I.34}$$

  holds true. In this case $\|\cdot\|_1$ and $\|\cdot\|_2$ induce the same topology on X.
- If $(X, \|\cdot\|)$ is a Banach space, which contains a countable dense set, then $(X, \|\cdot\|)$ is called **separable**.

Remarks and Examples. We illustrate the notion of separablity on examples.

- The subset of vectors $(x_1, \ldots, x_d) \in \mathbb{K}^d$ with rational coefficients $x_\nu \in \mathbb{K}_\mathbb{Q}$ is countable and dense in $\mathbb{K}^d$. Here, $\mathbb{K}_\mathbb{Q} := \mathbb{Q}$, if $\mathbb{K} = \mathbb{R}$, and $\mathbb{K}_\mathbb{Q} := \mathbb{Q} + i\mathbb{Q}$, if $\mathbb{K} = \mathbb{C}$. Therefore, $\big(\mathbb{K}^d, \|\cdot\|_2\big)$ is separable.

Next, for $1 \leq p < \infty$, we define

$$\ell^p(\mathbb{N}) \;:=\; \left\{ \underline{x} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \|\underline{x}\|_p := \Big(\sum_{\nu=1}^{\infty} |x_\nu|^p \Big)^{1/p} < \infty \right\}, \tag{I.35}$$

$$\ell^\infty(\mathbb{N}) \;:=\; \left\{ \underline{x} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \|\underline{x}\|_\infty := \sup_{\nu \in \mathbb{N}} |x_\nu| < \infty \right\}. \tag{I.36}$$

Then $\big(\ell^p(\mathbb{N}), \|\cdot\|_p\big)$ is a $\mathbb{K}$-Banach space, for $1 \leq p \leq \infty$. We further define

$$c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N}) \;:=\; \left\{ \underline{x} \in \mathbb{K}_{\mathbb{Q}}^{\mathbb{N}} \;\middle|\; \exists \nu_0 \in \mathbb{N}\ \forall \nu \geq \nu_0 : \quad x_\nu = 0 \right\}, \tag{I.37}$$

$$c_{\text{fin}}(\mathbb{N}) \;:=\; \left\{ \underline{x} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \exists \nu_0 \in \mathbb{N}\ \forall \nu \geq \nu_0 : \quad x_\nu = 0 \right\}, \tag{I.38}$$

$$c_0(\mathbb{N}) \;:=\; \left\{ \underline{x} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \lim_{\nu \to \infty} x_\nu = 0 \right\}, \tag{I.39}$$

and observe that

$$c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N}) \;\subseteq\; c_{\text{fin}}(\mathbb{N}) \;\subseteq\; \ell^p(\mathbb{N}) \;\subseteq\; \ell^{\tilde{p}}(\mathbb{N}) \;\subseteq\; c_0(\mathbb{N}) \;\subseteq\; \ell^\infty(\mathbb{N}), \tag{I.40}$$

where $1 \leq p < \tilde{p} < \infty$.

- Both $\big(c_0(\mathbb{N}),\, \|\cdot\|_\infty\big)$ and $\big(\ell_\infty(\mathbb{N}),\, \|\cdot\|_\infty\big)$ are Banach spaces with respect to the supremum norm $\|\cdot\|_\infty$. Note that $c_0(\mathbb{N}) \subset \ell_\infty(\mathbb{N})$ is a strict inclusion because, e.g., $(1, 1, 1, \ldots) \in \ell_\infty(\mathbb{N}) \setminus c_0(\mathbb{N})$.
- The set $c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N}) = \bigcup_{d=1}^{\infty} \mathbb{K}_{\mathbb{Q}}^d$ is a countable union of countable sets and, hence, countable itself.
- The countable subset $c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N}) \subseteq c_{\text{fin}}(\mathbb{N})$ is dense in $c_{\text{fin}}(\mathbb{N})$ with respect to the supremum norm $\|\cdot\|_\infty$.
- If $\underline{x} \in c_0(\mathbb{N})$ and $\varepsilon > 0$, there exists an $N \in \mathbb{N}$, such that $|x_\nu| \leq \varepsilon$, for all $\nu > N$. Moreover, for all $\nu \in \mathbb{N}$ and $x_\nu \in \mathbb{K}$, we can find a $\tilde{x}_\nu \in \mathbb{K}_{\mathbb{Q}}$ with $|x_\nu - \tilde{x}_\nu| \leq \varepsilon$. Defining $\underline{\tilde{x}} := (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_N, 0, 0, \ldots)$, we hence obtain $\underline{\tilde{x}} \in c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N})$ and $\|\underline{x} - \underline{\tilde{x}}\|_\infty \leq \varepsilon$. In other words, $c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N}) \subseteq c_0(\mathbb{N})$ is dense, and the Banach space $\big(c_0(\mathbb{N}),\, \|\cdot\|_\infty\big)$ is separable.
- If $\underline{x} \in \ell^p(\mathbb{N})$ and $\varepsilon > 0$, then there exists an $N \in \mathbb{N}$, such that $\sum_{\nu=N}^{\infty} |x_\nu|^p \leq \varepsilon^p / 2^p$. Moreover, to every $\nu \in \mathbb{N}$ and $x_\nu \in \mathbb{K}$ we can find an $\tilde{x}_\nu \in \mathbb{K}_{\mathbb{Q}}$, such that $|x_\nu - \tilde{x}_\nu| \leq \varepsilon / 2N$. Setting $\underline{\tilde{x}} := (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{\nu_0}, 0, 0, \ldots)$, we observe that $\underline{\tilde{x}} \in c_{\text{fin}}(\mathbb{N})$ and

  $$\|\underline{x} - \underline{\tilde{x}}\|_p \;\leq\; \left[\sum_{\nu=1}^{N} \Big(\frac{\varepsilon}{2N} \Big)^p \right]^{1/p} + \frac{\varepsilon}{2} \;=\; \frac{\varepsilon}{2N^{(p-1)/p}} + \frac{\varepsilon}{2} \;\leq\; \varepsilon. \tag{I.41}$$

  It follows that $c_{\text{fin}}^{\mathbb{Q}}(\mathbb{N}) \subseteq \ell^p(\mathbb{N})$ is dense, and that the Banach space $\big(\ell^p(\mathbb{N}),\, \|\cdot\|_p\big)$ is separable.

- Let $\{\underline{x}^{(k)}\}_{k=1}^{\infty} \subseteq \ell^\infty(\mathbb{N})$ be a countable subset, where $\underline{x}^{(k)} = \big(x_\nu^{(k)}\big)_{\nu=1}^{\infty}$. We define $\underline{\tilde{x}} = (\tilde{x}_\nu)_{\nu=1}^{\infty} \in \ell^\infty(\mathbb{N})$ by

$$\tilde{x}_\nu \;:=\; \begin{cases} 2, & \text{if } |x_\nu^{(\nu)}| \le 1, \\ 0, & \text{if } |x_\nu^{(\nu)}| > 1. \end{cases} \tag{I.42}$$

  Then, for all $k \in \mathbb{N}$, we have that

$$\big\|\underline{\tilde{x}} - \underline{x}^{(k)}\big\|_\infty \;\ge\; \big|\tilde{x}_k - x_k^{(k)}\big| \;\ge\; 1. \tag{I.43}$$

  Consequently, $\{\underline{x}^{(k)}\}_{k=1}^{\infty} \subseteq \ell^\infty(\mathbb{N})$ is not dense. Since $\{\underline{x}^{(k)}\}_{k=1}^{\infty}$ is an arbitrary countable subset, $\ell^\infty(\mathbb{N})$ cannot be separable.

I.4.2. Linear Operators

Definition I.11. Let $(X, \|\cdot\|)$ be a Banach space over $\mathbb{K}$. The $\mathbb{K}$-Banach space $\mathcal{B}(X;\mathbb{K})$ of the bounded linear operators from X to $\mathbb{K}$ is called **dual space $\boldsymbol{X^* := \mathcal{B}(X;\mathbb{K})}$ (of $\boldsymbol{X}$)**. Elements $y^* \in X^*$ of X^* are called **bounded linear functionals** or **continuous linear functionals** [according to (I.10)]. For the value $y^*(x)$ of $y^* \in X^*$ at the point $x \in X$ we write

$$x^*(x) \;=:\; \big\langle x^*,\, x\big\rangle. \tag{I.44}$$

Remarks and Examples.

- If $y^* \in X^*$ then

$$\|y^*\|_{X^*} \;=\; \sup_{x\in X\setminus\{0\}} \Big\{\frac{|\langle y^*,\, x\rangle|}{\|x\|_X}\Big\}. \tag{I.45}$$

- For $X = \mathbb{K}^d$, with $d \in \mathbb{N}$ and norm $\|\cdot\|$, the dual space X^* is isomorph zu X, that is $X^* = \mathbb{K}^d$. More specifically,
- If $\{x_1, \ldots, x_d\} \subseteq X$ is a basis then there exists a unique basis $\{x_1^*, \ldots, x_d^*\} \subseteq X^*$, such that

$$\forall\, 1 \le i, j \le d: \qquad \langle x_j^*,\, x_i\rangle \;=\; \delta_{ij}. \tag{I.46}$$

  This fact motivates the notation (I.44) $x^*(x) \;=:\; \big\langle x^*,\, x\big\rangle$.
- If $(X, \|\cdot\|)$ is a $\mathbb{K}$-Banach space and $Y \subseteq X$ is a closed subspace (and hence a Banach space itself), then $X^* \subseteq Y^*$. Namely, if $x^* \in X^*$ then $x^* \restriction_Y \in Y^*$.
- A $\mathbb{K}$-Banach space $\big(X, \|\cdot\|\big)$ is **reflexive**, if the dual space of its dual space is X itself, $\big((X, \|\cdot\|)^*\big)^* = (X, \|\cdot\|)$.
- For $d \in \mathbb{N}$, the Banach spaces $\big(\mathbb{K}^d, \|\cdot\|_p\big)$ are reflexive, for all $1 \le p \le \infty$, since $\big(\mathbb{K}^d, \|\cdot\|_p\big)^* = \big(\mathbb{K}^d, \|\cdot\|_q\big)$ with $\frac{1}{p} + \frac{1}{q} = 1$.

- For $1 < p < \infty$, the Banach spaces $\big(\ell^p(\mathbb{N}), \|\cdot\|_p\big)$ are reflexive, with $\big(\ell^p(\mathbb{N}), \|\cdot\|_p\big)^* = \big(\ell^q(\mathbb{N}), \|\cdot\|_q\big)$ with $\frac{1}{p} + \frac{1}{q} = 1$. This is essentially a consequence of Hölder's inequality,

$$\left| \sum_{\nu=1}^{\infty} \overline{x_\nu}\, y_\nu \right| \;\leq\; \left(\sum_{\nu=1}^{\infty} |x_\nu|^p \right)^{1/p} \left(\sum_{\nu=1}^{\infty} |y_\nu|^q \right)^{1/q}. \tag{I.47}$$

I.4.3. Hilbert Spaces

Lemma I.12. *Suppose that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a Hilbert space, $\mathcal{M} \subseteq \mathcal{H}$ is a closed subspace, and $x \in \mathcal{H}$. Then there is a unique vector $z \in \mathcal{M}$, such that*

$$\|x - z\| \;=\; \inf_{y \in \mathcal{M}} \|x - y\|. \tag{I.48}$$

Theorem I.13. *If $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a Hilbert space and $\mathcal{M} \subseteq \mathcal{H}$ is a closed subspace, then $\mathcal{M}$ is complementable, namely,*

$$\mathcal{H} \;=\; \mathcal{M} \,\oplus\, \mathcal{M}^\perp. \tag{I.49}$$

Corollary I.14. *Suppose that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a Hilbert space and $\mathcal{M} \subseteq \mathcal{H}$ a closed subspace. Define $P : \mathcal{H} \to \mathcal{H}$ by $P(x) \in \mathcal{M}$ and $\|x - P(x)\| = \inf_{y\in\mathcal{M}} \|x - y\|$. Then $P = P^2 \in \mathcal{B}(\mathcal{H})$ is an idempotent bounded linear operator on $\mathcal{H}$ with $\mathrm{Ran}P = \mathcal{M}$ and $\|P\|_{\mathrm{op}} = 1$, provided $\mathcal{M} \neq \{0\}$, and $P = 0$ otherwise. The operator P is called* ***orthogonal projection onto $\mathcal{M}$****.*

II. Bounded Linear Operators on Hilbert Spaces

II.1. Self-Adjoint, Normal, and Unitary Operators

In this section we collect some basic facts about the spectral theory of bounded linear operators on Hilbert spaces. Note that any Hilbert space $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is, in particular, a Banach space with norm $\|x\| = \sqrt{\langle x|x\rangle}$. We recall from (I.8) that

$$\mathcal{B}(\mathcal{H}) \;=\; \Big\{ A : \mathcal{H} \to \mathcal{H} \;\Big|\; A \text{ is linear, } \|A\|_{\mathcal{B}(\mathcal{H})} < \infty \Big\}, \tag{II.1}$$

where

$$\|A\|_{\mathcal{B}(\mathcal{H})} \;:=\; \sup_{x\in\mathcal{H}\setminus\{0\}} \left\{ \frac{\|Ax\|}{\|x\|} \right\} \;=\; \sup_{x\in\mathcal{H},\|x\|=1} \big\{ \|Ax\| \big\} \;=\; \sup_{x,y\in\mathcal{H},\|x\|=\|y\|=1} \Big\{ \big|\langle y|Ax\rangle\big| \Big\} \tag{II.2}$$

is the operator norm of A, where the last inequality follows from (I.30).

Fix $A \in \mathcal{B}(\mathcal{H})$. For any $y \in \mathcal{H}$, the map $\ell_y(x) := \langle y|Ax\rangle$ defines a bounded linear functional $\ell_y \in \mathcal{H}^*$ with $\|\ell_y\|_{\mathcal{H}^*} \le \|y\| \cdot \|A\|_{\mathrm{op}}$. By the Riesz representation theorem I.10 there exists a unique vector $z_y \in \mathcal{H}$ such that

$$\forall\, x \in \mathcal{H} : \qquad \langle y|Ax\rangle \;=\; \ell_y(x) \;=\; \langle z_y|x\rangle\,. \tag{II.3}$$

Definition II.1. Let $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ be a complex Hilbert space and $A \in \mathcal{B}(\mathcal{H})$ a bounded operator on $\mathcal{H}$.

(i) The map $y \mapsto z_y =: A^*(y)$, where $z_y \in \mathcal{H}$ is the unique vector in (II.3), is linear and defines a bounded operator $A^* \in \mathcal{B}(\mathcal{H})$ called the **adjoint operator to A**. This operator is uniquely determined by

$$\forall\, x, y \in \mathcal{H} : \qquad \langle y|Ax\rangle \;=\; \langle A^* y|x\rangle\,. \tag{II.4}$$

(ii) If $A = A^*$ then A is called **self-adjoint**.

(iii) If $AA^* = A^*A$ then A is said to be **normal**.

(iv) A bounded operator A is called **(bounded) invertible** if there exists a bounded operator $A^{-1} \in \mathcal{B}(\mathcal{H})$ such that $AA^{-1} = A^{-1}A = \mathbf{1}_{\mathcal{H}}$. In this case the operator $A^{-1} \in \mathcal{B}(\mathcal{H})$ is called the **inverse of A**. The set of bounded invertible operators on $\mathcal{H}$ form a group with respect to composition, the **automorphism group $\mathbf{Aut}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H})$**.

(v) The **spectrum $\sigma(A) \subseteq \mathbb{C}$** and the **resolvent set $\rho(A) \subseteq \mathbb{C}$** of a bounded operator $A \in \mathcal{B}(\mathcal{H})$ are defined by

$$\sigma(A) := \left\{ \lambda \in \mathbb{C} \;\middle|\; A - \lambda \cdot \mathbf{1}_{\mathcal{H}} \text{ is not bounded invertible} \right\}, \tag{II.5}$$

$$\rho(A) := \left\{ \lambda \in \mathbb{C} \;\middle|\; A - \lambda \cdot \mathbf{1}_{\mathcal{H}} \text{ is bounded invertible} \right\}, \tag{II.6}$$

i.e., $\rho(A) = \mathbb{C} \setminus \sigma(A)$.

(vi) A bounded invertible operator $U \in \mathrm{Aut}(\mathcal{H})$ is called **unitary** if $U^{-1} = U^*$. The set of unitary operators on $\mathcal{H}$ form a subgroup of $\mathrm{Aut}(\mathcal{H})$, the **unitary group $\mathcal{U}(\mathcal{H})$**.

II.2. Linear Operators on finite-dimensional Hilbert Spaces

We first discuss the finite-dimensional case. Let $d \in \mathbb{N}$ fixed and $\mathcal{H} = \mathbb{C}^d$ equipped with the unitary scalar product (I.16).

- If $d \in \mathbb{N}$, $\{e_1, \ldots, e_d\} \subseteq \mathcal{H} := \mathbb{C}^d$ is the canonical ONB, and $A \in \mathcal{B}(\mathbb{C}^d)$ is a (bounded) linear operator then

$$A \;=\; \mathbf{1}_{\mathcal{H}}\, A\, \mathbf{1}_{\mathcal{H}} \;=\; \sum_{m,n=1}^{d} |e_m\rangle\langle e_m|\, A\, |e_n\rangle\langle e_n| \;=\; \sum_{m,n=1}^{d} A_{m,n}\, |e_m\rangle\langle e_n|\,, \tag{II.7}$$

  where the matrix elements $A_{m,n}$ of A are given by

$$A_{m,n} \;=\; \langle e_m | A e_n \rangle\,. \tag{II.8}$$

- In the finite-dimensional case, the spectrum $\sigma(A) \subseteq \mathbb{C}$ of $A \in \mathcal{B}(\mathbb{C}^d)$ coincides with the set of eigenvalues and these, in turn, with the zeroes of the characteristic polynomial,

$$\sigma(A) \;= \left\{ \lambda \in \mathbb{C} \;\middle|\; \lambda \text{ is an eigenvalue of } A \right\} \;=\; \left\{ \lambda \in \mathbb{C} \;\middle|\; \det[A - \lambda \cdot \mathbf{1}] \;=\; 0 \right\}. \tag{II.9}$$

  Note that $\sigma(A)$ is a set of at most d numbers in the complex plane, and $\rho(A)$ is the entire complex plane except for these isolated points.

- In particular, $(A^*)_{m,n} = \overline{A_{n,m}}$, i.e., $A^* = \overline{A^t}$, for (finite-dimensional) matrices.

- If $A = A^* \in \mathcal{B}(\mathbb{C}^d)$ is self-adjoint then A is **diagonalizable**, i.e., there exists an ONB $\{\varphi_1, \ldots, \varphi_d\} \subseteq \mathcal{H} := \mathbb{C}^d$ of eigenvectors and d corresponding eigenvalues $\{\lambda_1, \ldots, \lambda_d\} \subseteq \mathbb{C}$ such that

$$A \;=\; \sum_{j=1}^{d} \lambda_j \, |\varphi_j\rangle\langle\varphi_j| \,. \tag{II.10}$$

  Moreover, all eigenvalues of a self-adjoint operator are real, $\sigma(A) \subseteq \mathbb{R}$.

- Furthermore, if $A = A^* \in \mathcal{B}(\mathbb{C}^d)$ is self-adjoint then

$$\|A\|_{\mathrm{op}} \;=\; \max\big\{|\lambda| \;:\; \lambda \in \sigma(A)\big\} \,. \tag{II.11}$$

  Indeed, if $\{\varphi_1, \ldots, \varphi_d\} \subseteq \mathbb{C}^d$ is an ONB of eigenvectors with corresponding eigenvalues $\{\lambda_1, \ldots, \lambda_d\} = \sigma(A) \subseteq \mathbb{R}$ such that

$$A \;=\; \sum_{j=1}^{d} \lambda_j \, |\varphi_j\rangle\langle\varphi_j| \,, \tag{II.12}$$

  then $\|A\varphi_j\| = |\lambda_j|$, for any $j \in \mathbb{Z}_1^d$, and hence $\|A\|_{\mathrm{op}} = \sup_{\|\psi\|=1} \|A\psi\| \geq \max_{1\leq j\leq d} |\lambda_j|$. Conversely, if $\varphi, \psi \in \mathbb{C}^d$ then

$$\begin{aligned}
\big|\langle\varphi|A\psi\rangle\big| \;&\leq\; \sum_{j=1}^{d} |\lambda_j| \, \big|\langle\varphi|\varphi_j\rangle \, \langle\varphi_j|\psi\rangle\big| \\
&\leq \Big(\max_{1\leq j\leq d} |\lambda_j|\Big) \Big(\sum_{j=1}^{d} \big|\langle\varphi|\varphi_j\rangle\big|^2\Big)^{1/2} \Big(\sum_{j=1}^{d} \big|\langle\varphi_j|\psi\rangle\big|^2\Big)^{1/2} \\
&= \Big(\max_{1\leq j\leq d} |\lambda_j|\Big) \, \|\varphi\| \, \|\psi\| \,,
\end{aligned} \tag{II.13}$$

  which implies that $\|A\|_{\mathrm{op}} \leq \max_{1\leq j\leq d} |\lambda_j|$.

- Note that here and henceforth we count multiplicities, i.e., the eigenvalues are not necessarily distinct. For instance, the unit matrix $(\mathbf{1}_{\mathbb{C}^d})_{m,n} = \delta_{m,n}$ is self-adjoint, its eigenvalues are $\lambda_1 = \ldots = \lambda_d = 1$, and its spectrum consists of a single point $\sigma(\mathbf{1}) = \{1\}$.

- More generally, if $K \in \mathbb{N}$ and $A_1 = A_1^*$, $A_2 = A_2^*$, ..., $A_K = A_K^* \in \mathcal{B}(\mathbb{C}^d)$ are mutually commuting self-adjoint operators,

$$\forall\, k, \ell \in \mathbb{Z}_1^K : \qquad [A_k, A_\ell] \;=\; A_k \, A_\ell \;-\; A_\ell \, A_k \;=\; 0 \,, \tag{II.14}$$

  then $A_1, A_2, \ldots, A_K$ are simultaneously diagonalizable. That is, there exists an ONB $\{\varphi_j | j \in \mathbb{Z}_1^d\} \subseteq \mathbb{C}^d$ of joint eigenvectors and $K \cdot d$ corresponding real eigenvalues $\sigma(A_k) = \{\lambda_{k,j} | j \in \mathbb{Z}_1^d\} \subseteq \mathbb{R}$ such that

$$A_k \;=\; \sum_{j=1}^{d} \lambda_{k,j} \, |\varphi_j\rangle\langle\varphi_j| \,. \tag{II.15}$$

- The latter statement (II.15) for $K = 2$ implies that normal operators, i.e., those for which $AA^* = A^*A$, are diagonalizable, too.

  Namely, defining the **real part** $\mathbf{Re}(\boldsymbol{A})$ and the **imaginary part** $\mathbf{Im}(\boldsymbol{A})$ of an operator $A \in \mathcal{B}(\mathcal{H})$ by

  $$\mathrm{Re}(A) \;:=\; \frac{1}{2}\big(A + A^*\big) \quad \text{and} \quad \mathrm{Im}(A) \;:=\; \frac{1}{2i}\big(A - A^*\big)\,, \tag{II.16}$$

  we observe that

  $$A \;=\; \mathrm{Re}(A) \;+\; i\mathrm{Im}(A)\,, \tag{II.17}$$

  much like $z = \mathrm{Re}(z) + i\mathrm{Im}(z)$ for $z \in \mathbb{C}$ with $\mathrm{Re}(z), \mathrm{Im}(z) \in \mathbb{R}$. It is easy to check that the normality of A is equivalent to $[\mathrm{Re}(A)\,,\, \mathrm{Im}(A)] = 0$. Hence, $\mathrm{Re}(A)$ and $\mathrm{Im}(A)$ are simultaneously diagonalizable, and there exists an ONB $\{\varphi_j | j \in \mathbb{Z}_1^d\} \subseteq \mathbb{C}^d$ of joint eigenvectors and $2d$ real eigenvalues $\{\alpha_1, \beta_1, \ldots, \alpha_d, \beta_d\} \subseteq \mathbb{R}$ such that $\mathrm{Re}(A) = \sum_{j=1}^d \alpha_j\, |\varphi_j\rangle\langle\varphi_j|$ and $\mathrm{Im}(A) = \sum_{j=1}^d \beta_j\, |\varphi_j\rangle\langle\varphi_j|$. Therefore, A is diagonalizable, namely,

  $$A \;=\; \sum_{j=1}^{d} (\alpha_j + i\beta_j)\, |\varphi_j\rangle\langle\varphi_j|\,. \tag{II.18}$$

- An important class of normal operators, besides self-adjoint ones, are unitary operators $U \in \mathcal{U}(\mathcal{H})$, since $UU^* = \mathbf{1}_{\mathcal{H}} = U^*U$. It follows that unitary operators are diagonalizable and that their spectra are contained in the unit circle, $\sigma(U) \subseteq \{z \in \mathbb{C} :\; |z| = 1\}$
- If $A_{m,n} = \langle e_m | A e_n\rangle$ is the matrix representation of A with respect to the canonical ONB $\{e_1, \ldots, e_d\} \subseteq \mathbb{C}^d$ then the self-adjointness of A is equivalent to $A_{n,m} = \overline{A_{m,n}}$. Its diagonalizability is equivalent to the existence of a **unitary matrix** $U \in \mathcal{U}(\mathbb{C}^d)$ such that

  $$A \;=\; U^*\, D\, U\,, \tag{II.19}$$

  where $D \in \mathcal{B}(\mathbb{C}^d)$ is a diagonal matrix,

  $$D_{i,j} \;=\; \langle e_i | D e_j\rangle \;=\; \delta_{i,j}\, \lambda_j \quad \Leftrightarrow \quad D \;=\; \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_d \end{pmatrix}. \tag{II.20}$$

  Indeed, if U has the matrix representation $U_{i,n} = \langle e_i | U e_n\rangle$ then $U_{i,n} := \langle \varphi_i | e_n\rangle$ has the desired properties.

The general form to which any operator on a finite-dimensional Hilbert space can be transformed to is given by the **singular value decomposition** described in the following theorem.

Theorem II.2 (Singular Value Decomposition)**.** *Let $d \in \mathbb{N}$ and $\big(\mathcal{H} = \mathbb{C}^d, \langle\cdot|\cdot\rangle = \langle\cdot|\cdot\rangle_{\text{unit}}\big)$ be the d-dimensional complex Hilbert space defined by the unitary scalar product and $A \in \mathcal{B}(\mathcal{H})$ a bounded operator on $\mathcal{H}$. Then there exist ONB $\{f_1, \ldots, f_d\}, \{g_1, \ldots, g_d\} \subseteq \mathcal{H}$ and nonnegative numbers $\rho_1, \ldots, \rho_d \in \mathbb{R}_0^+$ called **singular values of A** such that*

$$A \;=\; \sum_{n=1}^{d} \rho_n \, |f_n\rangle\langle g_n| \,. \tag{II.21}$$

Equivalently, if $A_{m,n} = \langle e_m | A e_n\rangle$ denote the matrix elements of A in the canonical ONB $\{e_1, \ldots, e_d\} \subseteq \mathcal{H}$ then there exist unitary matrices $U, V \in \mathcal{U}(\mathbb{C}^d)$ such that

$$A \;=\; U^* \, D \, V \,, \tag{II.22}$$

where $D \in \mathcal{B}(\mathbb{C}^d)$ is the diagonal matrix,

$$D \;=\; \begin{pmatrix} \rho_1 & 0 & \cdots & 0 \\ 0 & \rho_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \rho_d \end{pmatrix} \,, \tag{II.23}$$

with $\rho_1, \ldots, \rho_d \in \mathbb{R}_0^+$.

II.3. Positivity and Functional Calculus

Definition II.3 (Functional Calculus)**.** Let $d \in \mathbb{N}$ and $\big(\mathcal{H} = \mathbb{C}^d, \langle\cdot|\cdot\rangle = \langle\cdot|\cdot\rangle_{\text{unit}}\big)$ be the d-dimensional complex Hilbert space defined by the unitary scalar product, $A = A^* \in \mathcal{B}(\mathcal{H})$ a self-adjoint operator on $\mathcal{H}$, and $\{\varphi_1, \ldots, \varphi_d\} \subseteq \mathcal{H}$ an ONB of eigenvectors of A with corresponding eigenvalues $\{\lambda_1, \ldots, \lambda_d\} = \sigma(A) \subseteq \mathbb{R}$, such that

$$A \;=\; \sum_{j=1}^{d} \lambda_j \, |\varphi_j\rangle\langle\varphi_j| \,. \tag{II.24}$$

If $f \in C(\mathbb{R}; \mathbb{C})$ then define

$$f(A) \;:=\; \sum_{j=1}^{d} f(\lambda_j) \, |\varphi_j\rangle\langle\varphi_j| \,. \tag{II.25}$$

- It easy to check that $f(A)$ defined by (II.25) is normal.
- If $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_N x^N$ is a complex polynomial, $\alpha_0, \alpha_1, \ldots, \alpha_N \in \mathbb{C}$, then $f(A)$ defined by (II.25) coincides with $\alpha_0 + \alpha_1 A + \ldots + \alpha_N A^N$.

- Suppose that $(a_k)_{k=0}^{\infty} \in \mathbb{C}^{\mathbb{N}_0}$ is a complex sequence with $\limsup_{k\to\infty} |a_k|^{1/k} := 1/R < \infty$ and $z_0 \in \mathbb{C}$. Then the power series $f(z) := \sum_{k=0}^{\infty} a_k (z - z_0)^k$ converges absolutely in $D(z_0, R) := \{z \in \mathbb{C} : \ |z - z_0| < R\}$. If $\sigma(A) \subseteq D(z_0, R)$ then $f(A)$ defined by (II.25) coincides with the norm-convergent power series

$$f(A) \ = \ \sum_{k=0}^{\infty} a_k \, (A - z_0)^k \, . \tag{II.26}$$

- This way and with $z_0 = 0$ and $R = \infty$, we obtain many elementary functions of self-adjoint operators $A = A^*$, e.g., the matrix exponential function and many others,

$$\exp(A) \ := \ \sum_{k=0}^{\infty} \frac{A^k}{k!} \, , \tag{II.27}$$

$$\sin(A) \ := \ \sum_{k=0}^{\infty} \frac{(-1)^k A^{2k+1}}{(2k+1)!} \, , \tag{II.28}$$

$$\cos(A) \ := \ \sum_{k=0}^{\infty} \frac{(-1)^k A^{2k}}{(2k)!} \, . \tag{II.29}$$

  Eqs. (II.27)-(II.29) define bounded operators on $\mathcal{H}$ as norm-convergent power series.

Definition II.4 (Positivity)**.** Let $\big(\mathcal{H}, \langle \cdot | \cdot \rangle\big)$ be a complex Hilbert space and $A = A^*, B = B^* \in \mathcal{B}(\mathcal{H})$ two self-adjoint operators on $\mathcal{H}$.

$$(i) \quad A \text{ is called } \textbf{positive, } \boldsymbol{A \geq 0} \ :\Leftrightarrow \ \forall \, \varphi \in \mathcal{H} : \quad \langle \varphi \, | \, A\varphi \rangle \ \geq \ 0 \, . \tag{II.30}$$

$$(ii) \qquad \boldsymbol{A \geq B} \ :\Leftrightarrow \ A - B \geq 0 \, . \tag{II.31}$$

- Using the diagonal form

$$A \ = \ \sum_{j=1}^{d} \lambda_j \, |\varphi_j\rangle\langle\varphi_j| \, , \tag{II.32}$$

  one easily checks that

$$\big\{ A \ \geq \ 0 \big\} \quad \Leftrightarrow \quad \big\{ \sigma(A) \ \subseteq \ \mathbb{R}_0^+ \big\} \, . \tag{II.33}$$

- Hence, if $f \in C(\mathbb{R}_0^+; \mathbb{R})$ and A is positive then $f(A)$ can be defined by (II.25).
- In particular, we have for positive A that

$$\sqrt{A} \ = \ \sum_{j=1}^{d} \sqrt{\lambda_j} \, |\varphi_j\rangle\langle\varphi_j| \, , \tag{II.34}$$

$$A \, \ln(A) \ = \ \sum_{j=1}^{d} \lambda_j \, \ln(\lambda_j) \, |\varphi_j\rangle\langle\varphi_j| \, , \tag{II.35}$$

where we use the convention that $0\,\ln(0) = 0$, which is consistent with the continuity of $\lim_{r\searrow 0}\{r\,\ln(r)\} = 0$ at $r = 0$.

Next, let $d \in \mathbb{N}$ and $\mathcal{H} = \mathbb{C}^d$ be the d-dimensional complex Hilbert space endowed with the unitary scalar product and $A \in \mathcal{B}(\mathcal{H})$ a bounded operator on $\mathcal{H}$. According to Theorem II.2, there exist ONB $\{f_1, \ldots, f_d\}, \{g_1, \ldots, g_d\} \subseteq \mathcal{H}$ and nonnegative numbers $\rho_1, \rho_2, \ldots, \rho_d \geq 0$, such that A assumes its singular value decomposition

$$A \;=\; \sum_{n=1}^{d} \rho_n \, |f_n\rangle\langle g_n| \,. \tag{II.36}$$

Then A^*A is positive,

$$A^*A \;=\; \sum_{m,n=1}^{d} \rho_m \, \rho_n \, |g_m\rangle\langle f_m|f_n\rangle\langle g_n| \;=\; \sum_{n=1}^{d} \rho_n^2 \, |g_n\rangle\langle g_n| \;\geq\; 0\,, \tag{II.37}$$

which can also be seen directly, as $\langle\varphi|A^*A\varphi\rangle = \langle A\varphi|A\varphi\rangle = \|A\varphi\| \geq 0$. We can thus define the **absolute value** $|\boldsymbol{A}|$ of A by (II.34),

$$|A| \;:=\; \sqrt{A^*\,A} \;=\; \sum_{n=1}^{d} \sqrt{\rho_n^2} \, |g_n\rangle\langle g_n| \,, \;=\; \sum_{n=1}^{d} \rho_n \, |g_n\rangle\langle g_n| \,. \tag{II.38}$$

Note that $|A|^* = |A|$, but $|A^*| = \sum_{n=1}^{d} \rho_n |f_n\rangle\langle f_n| \neq |A|$, in general. From these observations and taking $U := \sum_{n=1}^{d} |f_n\rangle\langle g_n|$, we obtain the polar decomposition of A,

Theorem II.5 (Polar Decomposition)**.** *Let $d \in \mathbb{N}$ and $\big(\mathcal{H} = \mathbb{C}^d, \langle\cdot|\cdot\rangle = \langle\cdot|\cdot\rangle_{\text{unit}}\big)$ be the d-dimensional complex Hilbert space defined by the unitary scalar product and $A \in \mathcal{B}(\mathcal{H})$ a bounded operator on $\mathcal{H}$. Then there exist a unitary operator $U \in \mathcal{U}(\mathcal{H})$ such that*

$$A \;=\; U\,|A| \,. \tag{II.39}$$

The right side of (II.39) *is called the* ***polar decomposition*** *of A.*

II.4. Traces and Trace Norms

Definition II.6. Let $d \in \mathbb{N}$ and $\big(\mathcal{H} = \mathbb{C}^d, \langle\cdot|\cdot\rangle = \langle\cdot|\cdot\rangle_{\text{unit}}\big)$ be the d-dimensional complex Hilbert space defined by the unitary scalar product, $\{\varphi_1, \ldots, \varphi_d\} \subseteq \mathcal{H}$ an ONB, and $A \in \mathcal{B}(\mathcal{H})$ a bounded operator on $\mathcal{H}$.

(i) The **trace** $\mathbf{Tr}(\boldsymbol{A})$ of A is defined as

$$\mathrm{Tr}(A) \;:=\; \sum_{j=1}^{d} \langle\varphi_j \,|\, A\varphi_j\rangle \,. \tag{II.40}$$

(ii) For $p \in [1,\infty)$ define the **trace norm** $\|\boldsymbol{A}\|_{\boldsymbol{p}}$ of A by

$$\|A\|_p \;:=\; \big[\mathrm{Tr}\big(|A|^p\big)\big]^{1/p}. \tag{II.41}$$

Remarks and Examples.

- The trace $\mathrm{Tr}(A)$ of $A \in \mathcal{B}(\mathcal{H})$ is well-defined, i.e., independent of the choice of the ONB $\{\varphi_1,\ldots,\varphi_d\} \subseteq \mathcal{H}$. Indeed, if $\{f_1,\ldots,f_d\} \subseteq \mathcal{H}$ is any ONB and $A = \sum_{i,j=1}^N a_{i,j}\,|f_i\rangle\langle f_j|$ then

$$\mathrm{Tr}(A) \;=\; \sum_{i,j=1}^{d} a_{i,j}\,\langle f_j|f_i\rangle \;=\; \sum_{i=1}^{d} a_{i,i} \;=\; \sum_{i=1}^{d}\langle f_i|Af_i\rangle\,, \tag{II.42}$$

  independent of the choice of the ONB $\{f_1,\ldots,f_d\}$ in $\mathcal{H}$.

- If $\{\lambda_1,\ldots,\lambda_d\} \subseteq \mathbb{C}$ are the zeros of the characteristic polynomial $\chi(\lambda) = \det[A - \lambda\cdot \mathbf{1}] = (\lambda_1-\lambda)\cdots(\lambda_d-\lambda)$ (counting multiplicities), then $\mathrm{Tr}(A) = \lambda_1 + \ldots + \lambda_d$ is the sum of these zeroes. Indeed, it is easy to check that $\mathrm{Tr}(A) = -\alpha_{d-1} = \lambda_1+\ldots+\lambda_d$, when writing $\chi(\lambda) = \alpha_0 + \ldots + \alpha_{d-1}\lambda^{d-1} + \lambda^d$.

- If $\rho_1 \geq \rho_2 \geq \cdots \geq \rho_d \geq 0$ are the eigenvalues of $|A|$, then $\|A\|_p = \big(\sum_{n=1}^N \rho_n^p\big)^{1/p}$.

- If $\rho_1 \geq \rho_2 \geq \cdots \geq \rho_d \geq 0$ and $A \neq 0$ then $\rho_1 > 0$. If furthermore $1 \leq q < p < \infty$ then

$$\|A\|_p^p \;=\; \sum_{n=1}^{N}\rho_n^p \;=\; \rho_1^p \sum_{n=1}^{N}\left(\frac{\rho_n}{\rho_1}\right)^p \;\leq\; \rho_1^p \sum_{n=1}^{N}\left(\frac{\rho_n}{\rho_1}\right)^q \;=\; \rho_1^{p-q}\,\|A\|_q^q\,. \tag{II.43}$$

Theorem II.7. *Let $\big(\mathcal{H}=\mathbb{C}^d, \langle\cdot|\cdot\rangle = \langle\cdot|\cdot\rangle_{\mathrm{unit}}\big)$ be a finite-dimensional complex Hilbert space and $A, B \in \mathcal{B}(\mathcal{H})$ two linear operators on $\mathcal{H}$.*

$$(i) \qquad \|AB\|_1 \;\leq\; \|A\|_{\mathrm{op}}\cdot\|B\|_1\,; \tag{II.44}$$

$$(ii) \qquad \|A\|_{\mathrm{op}} \;=\; \sup\big\{\mathrm{Tr}(AB)\;\big|\; B\in\mathcal{L}^1(\mathcal{H})\,,\; \|B\|_1 = 1\big\}\,. \tag{II.45}$$

$$(iii) \qquad A = A^* \;\;\Rightarrow\;\; \|A\|_{\mathrm{op}} \;=\; \sup\big\{\mathrm{Tr}(\rho A)\;\big|\rho\in\mathcal{DM}(\mathcal{H})\big\}\,, \tag{II.46}$$

where

$$\mathcal{DM}(\mathcal{H}) \;:=\; \big\{\rho\in\mathcal{L}^1(\mathcal{H})\;\big|\;\rho=\rho^*\geq 0\,,\;\mathrm{Tr}(\rho)=1\big\} \;\subseteq\; \mathcal{L}^1(\mathcal{H}) \tag{II.47}$$

is the convex subset of ***density matrices****.*

II.5. Tensor Products of Hilbert Spaces

In this section we define tensor products of Hilbert spaces and observe some basic facts about these. To this end we suppose that $\big(\mathcal{H},\langle\cdot|\cdot\rangle\big)$ and $\big(\mathcal{H}',\langle\cdot|\cdot\rangle'\big)$ are two (separable, complex) Hilbert spaces. For $f\in\mathcal{H}$ and $f'\in\mathcal{H}'$ we define a map $f\otimes f' : \mathcal{H}\times\mathcal{H}'\to\mathbb{C}$ by

$$\forall\, h\in\mathcal{H},\; h'\in\mathcal{H}': \qquad \big(f\otimes f'\big)[h,h'] \;:=\; \langle h|f\rangle\,\langle h'|f'\rangle\,. \tag{II.48}$$

Obviously, $f \otimes f'$ is a bi-antilinear form,

$$\big(f \otimes f'\big)[g + \alpha h, g' + \beta h'] \;= \big(f \otimes f'\big)[g, g'] \;+\; \overline{\alpha}\,\big(f \otimes f'\big)[h, g'] \;+\; \overline{\beta}\,\big(f \otimes f'\big)[g, h'] \\ +\; \overline{\alpha\,\beta}\,\big(f \otimes f'\big)[h, h']\,. \tag{II.49}$$

With these bi-antilinear forms we build a complex vector space $\mathcal{G}_{\text{fin}}$ by the usual pointwise operations,

$$\big((f \otimes f') + \alpha(g \otimes g')\big)[h, h'] \;:=\; \big(f \otimes f'\big)[h, h'] \;+\; \alpha\big(g \otimes g'\big)[h, h']\,. \tag{II.50}$$

This vector space contains all (finite) linear combinations of bilinear forms $f \otimes f'$,

$$\mathcal{G}_{\text{fin}} \;=\; \left\{ \sum_{j=1}^{L} \alpha_j (f_j \otimes f'_j) \;\middle|\; L \in \mathbb{N},\; \forall\, j \in \mathbb{Z}_1^L :\; \alpha_j \in \mathbb{C},\; f_j \in \mathcal{H},\; f'_j \in \mathcal{H}' \right\}. \tag{II.51}$$

We define a quadratic form $\langle \cdot | \cdot \rangle_{\mathcal{G}} : \mathcal{G}_{\text{fin}} \times \mathcal{G}_{\text{fin}} \to \mathbb{C}$ by continuation by antilinearity of

$$\langle f \otimes f' | g \otimes g' \rangle_{\mathcal{G}} \;:=\; \langle f | g \rangle\, \langle f' | g' \rangle\,, \tag{II.52}$$

i.e.,

$$\left\langle \sum_{i=1}^{L} \alpha_i\, f_i \otimes f'_i \;\middle|\; \sum_{j=1}^{L} \beta_j\, g_j \otimes g'_j \right\rangle_{\mathcal{G}} \;:=\; \sum_{i,j=1}^{L} \overline{\alpha_i}\, \beta_j\, \langle f_i | g_j \rangle\, \langle f'_i | g'_j \rangle\,. \tag{II.53}$$

Lemma II.8. *The quadratic form $\langle \cdot | \cdot \rangle_{\mathcal{G}} : \mathcal{G}_{\text{fin}} \times \mathcal{G}_{\text{fin}} \to \mathbb{C}$ as in* (II.52) *defines a scalar product on $\mathcal{G}_{\text{fin}}$.*

Proof. Sesquilinearity and symmetry of $\langle \cdot | \cdot \rangle_{\mathcal{G}}$ are trivial, and we concentrate on its positive definiteness. Let $\{\varphi_k\}_{k=1}^{\infty} \subseteq \mathcal{H}$ and $\{\varphi'_\ell\}_{\ell=1}^{\infty} \subseteq \mathcal{H}'$ be two ONB and assume that $\Psi = \sum_{j=1}^{L} \alpha_j (f_j \otimes f'_j) \in \mathcal{G}_{\text{fin}}$. Then

$$\langle \Psi | \Psi \rangle_{\mathcal{G}} \;=\; \sum_{i,j=1}^{L} \overline{\alpha_i}\, \alpha_j\, \langle f_i | f_j \rangle\, \langle f'_i | f'_j \rangle' \;=\; \sum_{k,\ell=1}^{\infty} \sum_{i,j=1}^{L} \overline{\alpha_i}\, \alpha_j\, \langle f_i | \varphi_k \rangle\, \langle \varphi_k | f_j \rangle\; \langle f'_i | \varphi'_\ell \rangle'\, \langle \varphi'_\ell | f'_j \rangle' \\ = \sum_{k,\ell=1}^{\infty} \left| \sum_{j=1}^{L} \alpha_j\, \big(f_j \otimes f'_j\big)[\varphi_k, \varphi'_\ell] \right|^2 \;=\; \sum_{k,\ell=1}^{\infty} \big|\Psi[\varphi_k, \varphi'_\ell]\big|^2\,. \tag{II.54}$$

This proves that $\langle \Psi | \Psi \rangle_{\mathcal{G}} \geq 0$. Moreover, $\langle \Psi | \Psi \rangle_{\mathcal{G}} = 0$ implies that $\Psi[\varphi_k, \varphi'_\ell] = 0$, for all $k, \ell \in \mathbb{N}$. Since $\{\varphi_k\}_{k=1}^{\infty} \subseteq \mathcal{H}$ and $\{\varphi'_\ell\}_{\ell=1}^{\infty} \subseteq \mathcal{H}'$ are ONB, this in turn yields $\Psi = 0$. □

Definition II.9. Suppose that $\big(\mathcal{H}, \langle \cdot | \cdot \rangle\big)$ and $\big(\mathcal{H}', \langle \cdot | \cdot \rangle'\big)$ are two separable, complex Hilbert spaces. Define $\mathcal{G}_{\text{fin}}$ as in (II.51) and equip it with the scalar product $\langle \cdot | \cdot \rangle_{\mathcal{G}} : \mathcal{G}_{\text{fin}} \times \mathcal{G}_{\text{fin}} \to \mathbb{C}$ as in (II.52). We define a separable, complex Hilbert space $\big(\mathcal{G},\, \langle \cdot | \cdot \rangle_{\mathcal{G}}\big)$ as the completion

$$\mathcal{G} \;:=\; \overline{\mathcal{G}_{\text{fin}}}^{\langle \cdot | \cdot \rangle_{\mathcal{G}}} \tag{II.55}$$

of $\mathcal{G}_{\text{fin}}$ with respect to the norm induced by $\langle \cdot | \cdot \rangle_{\mathcal{G}}$. The Hilbert space $\mathcal{G}$ is called the **tensor product** of $\mathcal{H}$ and $\mathcal{H}'$, and we write $\mathcal{G} =: \boldsymbol{\mathcal{H} \otimes \mathcal{H}'}$ and $\langle \cdot | \cdot \rangle_{\mathcal{G}} =: \boldsymbol{\langle \cdot | \cdot \rangle_{\mathcal{H} \otimes \mathcal{H}'}}$.

Remarks and Examples.

- If $\{\varphi_k\}_{k=1}^{\infty} \subseteq \mathcal{H}$ and $\{\varphi'_\ell\}_{\ell=1}^{\infty} \subseteq \mathcal{H}'$ are ONB then so is $\{\varphi_k \otimes \varphi'_\ell\}_{k,\ell=1}^{\infty} \subseteq \mathcal{H} \otimes \mathcal{H}'$.
- Definition II.9 can be easily generalized to $N \in \mathbb{N}$ factors: If $\big(\mathcal{H}_n, \langle\cdot|\cdot\rangle_n\big)$ is a Hilbert space with an ONB $\{\varphi_{n;k}\}_{k=1}^{\infty} \subseteq \mathcal{H}_n$, for $n \in \mathbb{Z}_1^N$, then $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ is the tensor product of $\mathcal{H}_1, \ldots, \mathcal{H}_N$ and $\big\{\varphi_{1;k_1} \otimes \cdots \otimes \varphi_{N;k_N} \,\big|\, k_1, \ldots, k_N \in \mathbb{N}\big\} \subseteq \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ is an ONB.
- Assume that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a separable, complex Hilbert space. Then the space $\mathcal{L}^2(\mathcal{H})$ of Hilbert-Schmidt operators on $\mathcal{H}$ is a Hilbert space $\big(\mathcal{L}^2(\mathcal{H}), \langle\cdot|\cdot\rangle_{\mathcal{L}^2(\mathcal{H})}\big)$ with respect to the scalar product

$$\langle A|B\rangle_{\mathcal{L}^2(\mathcal{H})} \;:=\; \mathrm{Tr}_{\mathcal{H}}\big(A^*\,B\big)\,. \tag{II.56}$$

- Assume that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a separable, complex Hilbert space. Then the Hilbert space $\big(\mathcal{L}^2(\mathcal{H}), \langle\cdot|\cdot\rangle_{\mathcal{L}^2(\mathcal{H})}\big)$ of Hilbert-Schmidt operators is isomorphic to $\big(\mathcal{H} \otimes \mathcal{H}^*,\, \langle\cdot|\cdot\rangle_{\mathcal{H}\otimes\mathcal{H}^*}\big)$, the isomorphism being

$$J:\; \mathcal{L}^2(\mathcal{H}) \;\to\; \mathcal{H} \otimes \mathcal{H}^*\,, \quad |\varphi\rangle\langle\psi| \;\mapsto\; \varphi \otimes \psi\,. \tag{II.57}$$

- If $(\Omega, \mathfrak{A}, \mu)$ and $(\Omega', \mathfrak{A}', \mu')$ are two measure spaces then $L^2(\Omega \times \Omega', d\mu \otimes d\mu')$ is isomorphic to $L^2(\Omega, d\mu) \otimes L^2(\Omega', d\mu')$. The isomorphism $I : L^2(\Omega, d\mu) \otimes L^2(\Omega', d\mu') \to L^2(\Omega \times \Omega', d\mu \otimes d\mu')$ derives from the extension by linearity and continuity of

$$\varphi \otimes \varphi' \;\mapsto\; \varphi \cdot \varphi'\,, \quad \text{where} \quad (\varphi \cdot \varphi')[x, x'] \;:=\; \varphi(x) \cdot \varphi'(x')\,. \tag{II.58}$$

II.6. SUPPLEMENTARY MATERIAL

II.6.1. Proof of Theorem II.2 - Singular Value Decomposition

Proof. We only prove (II.21). We may assume that $A \neq 0$. Observe that $A^*A \in \mathcal{B}(\mathcal{H})$ is a self-adjoint matrix and, hence, diagonalizable. In other words, there exists an ONB $\{g_1, \ldots, g_d\} \subseteq \mathcal{H}$ of eigenvectors of A^*A and corresponding real eigenvalues $\lambda_1, \ldots, \lambda_d \in \mathbb{R}$ such that

$$A^*A \;=\; \sum_{j=1}^{d} \lambda_j \, |g_j\rangle\langle g_j|\,. \tag{II.59}$$

Note that the eigenvalues $\lambda_j = \langle g_j|A^*Ag_j\rangle = \|Ag_j\|^2 \geq 0$ are nonnegative, and we may define $\rho_j \in \mathbb{R}_0^+$ by $\rho_j := \sqrt{\lambda_j} = \|Ag_j\|$. Moreover, we may assume w.l.o.g. these numbers to be sorted in descending order such that $\rho_1 \geq \ldots \geq \rho_c > \rho_{c+1} = \ldots = \rho_d = 0$, for some $c \in \mathbb{Z}_1^d$. Hence, $\mathrm{Ker}(A) = \mathrm{span}\{g_{c+1}, \ldots, g_d\}$ and $\dim \mathrm{Ker}(A) = d - c$.

Next, by (I.26),

$$A \;=\; \sum_{j=1}^{d} |Ag_j\rangle\langle g_j| \;=\; \sum_{j=1}^{c} |Ag_j\rangle\langle g_j| \;=\; \sum_{j=1}^{c} \rho_j \, |f_j\rangle\langle g_j| \,, \tag{II.60}$$

where $f_j := \rho_j^{-1} A g_j$, for $j \in \mathbb{Z}_1^c$, using that $\rho_j > 0$ in this case. Then $f_1, f_2, \ldots, f_c \in \mathcal{H}$ are normalized, by definition, and for all $1 \leq m < n \leq c$ we observe that

$$\langle f_m | f_n \rangle \;=\; \frac{\langle Ag_m | Ag_n \rangle}{\rho_m \rho_n} \;=\; \frac{\langle g_m | A^* A g_n \rangle}{\rho_m \rho_n} \;=\; \frac{\rho_n \, \langle g_m | g_n \rangle}{\rho_m} \;=\; 0 \,. \tag{II.61}$$

It follows that $\{f_1, f_2, \ldots, f_c\} \subseteq \mathcal{H}$ is an orthonormal system which we can complement (e.g., using the Gram-Schmidt orthonormalization procedure) with vectors $f_{c+1}, \ldots, f_d$ to an ONB $\{f_1, f_2, \ldots, f_d\} \subseteq \mathcal{H}$. Using that $\rho_{c+1} = \ldots = \rho_d = 0$, we finally obtain

$$A \;=\; \sum_{j=1}^{c} \rho_j \, |f_j\rangle\langle g_j| \;=\; \sum_{j=1}^{d} \rho_j \, |f_j\rangle\langle g_j| \,, \tag{II.62}$$

as asserted. □

II.6.2. Proof of Theorem II.5 - Polar Decomposition

Proof. Let $\{f_1, \ldots, f_d\}, \{g_1, \ldots, g_d\} \subseteq \mathcal{H}$ be ONB and $\rho_1, \rho_2, \ldots, \rho_d \geq 0$ nonnegative numbers of a polar decomposition of

$$A \;=\; \sum_{n=1}^{d} \rho_n \, |f_n\rangle\langle g_n| \,, \tag{II.63}$$

which exists according to Theorem II.2. We define

$$U \;=\; \sum_{n=1}^{d} |f_n\rangle\langle g_n| \tag{II.64}$$

and observe that $U^* = \sum_{n=1}^{d} |g_n\rangle\langle f_n|$. Thus

$$U^* U \;=\; \sum_{m,n=1}^{d} |g_m\rangle\langle f_m | f_n\rangle\langle g_n| \;=\; \sum_{n=1}^{d} |g_n\rangle\langle g_n| \;=\; \mathbf{1} \,, \tag{II.65}$$

and similary $UU^* = \mathbf{1}$, so U is unitary. Moreover,

$$U \, |A| \;=\; \sum_{m,n=1}^{d} \rho_n \, |f_m\rangle\langle g_m | g_n\rangle\langle g_n| \;=\; \sum_{n=1}^{d} \rho_n \, |f_n\rangle\langle g_n| \;=\; A \,, \tag{II.66}$$

as asserted. □

II.6.3. Compact Operators, Trace Class Operators, Hilbert–Schmidt Operators

In this section we pass to infinite-dimensional Hilbert spaces, but we will restrict ourselves to compact operators, which are well-approximated by matrices (as opposed to the identity operator $\mathbf{1}_{\mathcal{H}}$ on $\mathcal{H}$ or differential operators like $-i\nabla$, say).

Definition II.10. Suppose that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a (separable, complex) Hilbert space.

(i) We define by

$$\boldsymbol{\mathcal{B}_{\text{fin}}(\mathcal{H})} \;:=\; \left\{ \sum_{i,j=1}^{N} a_{i,j}\, |f_i\rangle\langle f_j| \;\middle|\; N \in \mathbb{N}\,,\; \{a_{i,j}\}_{i,j=1}^{N} \subseteq \mathbb{C}\,,\; \{f_i\}_{i=1}^{N} \subseteq \mathcal{H} \right\} \;\subseteq\; \mathcal{B}(\mathcal{H}) \tag{II.67}$$

the space of linear operators (on $\mathcal{H}$) of **finite rank**.

(ii) The closure of $\mathcal{B}_{\text{fin}}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H})$ in operator norm,

$$\mathbf{Com(\mathcal{H})} \;:=\; \overline{\mathcal{B}_{\text{fin}}(\mathcal{H})}^{\|\cdot\|_{\text{op}}} \;\subseteq\; \mathcal{B}(\mathcal{H})\,, \tag{II.68}$$

defines the space of **compact operators** (on $\mathcal{H}$).

Remarks and Examples.

- The **rank** $\mathbf{rk}(\boldsymbol{A})$ of an operator $A \in \mathcal{B}(\mathcal{H})$ is defined to be the dimension of its range, $\mathrm{rk}(A) := \dim[\mathrm{Ran}(A)] \in \mathbb{N}_0 \cup \{\infty\}$.
- It follows that $\mathcal{B}_{\text{fin}}(\mathcal{H}) = \big\{A \in \mathcal{B}(\mathcal{H}) \big|\; \mathrm{rk}(A) + \mathrm{rk}(A^*) < \infty\}$.
- The set of finite-rank operators $\mathcal{B}_{\text{fin}}(\mathcal{H})$ is a subspace of $\mathcal{B}(\mathcal{H})$ which is not closed in the operator norm topology. Its closure is the space of compact operators $\mathrm{Com}(\mathcal{H})$. That is, $A \in \mathcal{B}(\mathcal{H})$ is compact iff for any $\varepsilon > 0$ there are $N \in \mathbb{N}$, $\{a_{i,j}\}_{i,j=1}^{N} \subseteq \mathbb{C}$, and $\{f_i\}_{i=1}^{N} \subseteq \mathcal{H}$ such that

$$\left\| A \;-\; \sum_{i,j=1}^{N} a_{i,j}\, |f_i\rangle\langle f_j| \right\|_{\text{op}} \;\leq\; \varepsilon\,. \tag{II.69}$$

- Its closure, the set of compact operators $\mathrm{Com}(\mathcal{H})$, is a closed subspace of the Banach space $\big(\mathcal{B}(\mathcal{H}), \|\cdot\|_{\text{op}}\big)$. and, hence, a Banach (sub-)space $\big(\mathrm{Com}(\mathcal{H}), \|\cdot\|_{\text{op}}\big)$ itself. This Banach subspace $\mathrm{Com}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H})$ cannot, however, be complemented by another closed subspace $X \subseteq \mathcal{B}(\mathcal{H})$, such that $\mathcal{B}(\mathcal{H}) = \mathrm{Com}(\mathcal{H}) \oplus X$.
- Since this holds true for finite-rank operators, it follows that every compact operator $A \in \mathrm{Com}(\mathcal{H})$ possesses a **singular value decomposition (SVD)**, i.e., there exist ONB $\{f_n\}_{n=1}^{\infty}, \{g_n\}_{n=1}^{\infty} \subseteq \mathcal{H}$ and singular values $\{\rho_n\}_{n=1}^{\infty} \subseteq \mathbb{R}_0^+$ of A with $\rho_n \geq \rho_{n+1}$ such that

$$A \;=\; \sum_{n=1}^{\infty} \rho_n\, |f_n\rangle\langle g_n|\,. \tag{II.70}$$

It is here where the use of Dirac's ket-bra notation pays off: We never have to introduce and use infinitly extended matrices, but only let the summation range extend to infinitly many terms.

- For $p \in [1,\infty)$, the trace norm $\|\cdot\|_p$ in (II.68) defines a norm, indeed, on the complex vector space $\mathcal{B}_{\text{fin}}(\mathcal{H})$ of finite-rank operators.
- The triangle inequality is the only nontrivial part of the latter statement. We only comment on the cases $p = 1$ and $p = 2$. For $p = 1$, it rests on the representation

$$\|A\|_1 \;=\; \sup\left\{ \sum_{n=1}^{\infty} \big|\langle\psi_n|A\varphi_n\rangle\big| \;\middle|\; \{\psi_m\}_{m=1}^{\infty},\ \{\varphi_n\}_{n=1}^{\infty} \subseteq \mathcal{H} \text{ ONB} \right\}, \tag{II.71}$$

while for $p = 2$, the key ingredient of the proof is the representation

$$\|A\|_2 \;=\; \sup\left\{ \frac{\operatorname{Tr}(B^*A)}{\operatorname{Tr}(B^*B)^{1/2}} \;\middle|\; B \in \mathcal{B}_{\text{fin}}(\mathcal{H}) \setminus \{0\} \right\}. \tag{II.72}$$

To see that (II.71) is the crucial input in the case $p = 1$, let $A, B \in \mathcal{B}_{\text{fin}}(\mathcal{H})$ and observe that

$$\begin{aligned}
\|A+B\|_1 \;&=\; \sup\left\{ \sum_{n=1}^{\infty} \big|\langle\psi_n|(A+B)\varphi_n\rangle\big| \;\middle|\; \{\psi_m\}_{m=1}^{\infty},\ \{\varphi_n\}_{n=1}^{\infty} \subseteq \mathcal{H} \text{ ONB} \right\} \\
&\leq\; \sup\left\{ \sum_{n=1}^{\infty} \big|\langle\psi_n|A\varphi_n\rangle\big| \;\middle|\; \{\psi_m\}_{m=1}^{\infty},\ \{\varphi_n\}_{n=1}^{\infty} \subseteq \mathcal{H} \text{ ONB} \right\} \\
&\quad +\; \sup\left\{ \sum_{n=1}^{\infty} \big|\langle\psi_n|B\varphi_n\rangle\big| \;\middle|\; \{\psi_m\}_{m=1}^{\infty},\ \{\varphi_n\}_{n=1}^{\infty} \subseteq \mathcal{H} \text{ ONB} \right\} \\
&= \|A\|_1 + \|B\|_1 \,.
\end{aligned} \tag{II.73}$$

The case $p = 2$ uses (II.72) in a similar way.

Definition II.11. Suppose that $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ is a (separable, complex) Hilbert space and that $1 \leq p < \infty$. We define by

$$\boldsymbol{\mathcal{L}^p(\mathcal{H})} \;:=\; \overline{\mathcal{B}_{\text{fin}}(\mathcal{H})}^{\|\cdot\|_p} \;\subseteq\; \mathcal{B}(\mathcal{H})\,, \tag{II.74}$$

the space of ***p*-summable operators** (on $\mathcal{H}$). Specifically, the Banach space $\big(\mathcal{L}^1(\mathcal{H}), \|\cdot\|_1\big)$ is called the space of **trace class operators**, and the Banach space $\big(\mathcal{L}^2(\mathcal{H}), \|\cdot\|_2\big)$ is called the space of **Hilbert-Schmidt operators**.

Theorem II.12. *Let $\big(\mathcal{H} = \mathbb{C}^d, \langle\cdot|\cdot\rangle = \langle\cdot|\cdot\rangle_{\text{unit}}\big)$ be a complex Hilbert space with an ONB $\{\varphi_j\}_{j=1}^{\infty} \subseteq \mathcal{H}$ and $A \in \mathcal{L}^1(\mathcal{H})$. Then the **trace of A***

$$\operatorname{Tr}(A) \;:=\; \sum_{j=1}^{\infty} \langle\varphi_j|\, A\varphi_j\rangle \tag{II.75}$$

exists and is independent of the ONB $\{\varphi_j\}_{j=1}^{\infty} \subseteq \mathcal{H}$*. If* $A_1, A_2, \ldots, A_L \in \mathcal{L}^1(\mathcal{H})$ *then the trace is* ***cyclic****,*

$$\mathrm{Tr}(A_1 A_2 \cdots A_{L-1} A_L) \;=\; \mathrm{Tr}(A_L A_1 A_2 \cdots A_{L-1} A_L)\,. \tag{II.76}$$

Proof. Due to (II.71), the sum on the right side of (II.75) exists and is bounded in absolute value by $\|A\|_1$,

$$\left| \sum_{j=1}^{\infty} \langle \varphi_j |\, A\varphi_j \rangle \right| \;\leq\; \|A\|_1\,. \tag{II.77}$$

Let $\{\psi_k\}_{k=1}^{\infty} \subseteq \mathcal{H}$ be a second ONB. Given $\varepsilon > 0$, we can find a finite-rank operator $A_\varepsilon \in \mathcal{B}_{\mathrm{fin}}(\mathcal{H})$ such that $\|A - A_\varepsilon\|_1 \leq \varepsilon$. Since A_ε is of finite rank,

$$\sum_{j=1}^{\infty} \langle \varphi_j |\, A_\varepsilon \varphi_j \rangle \;=\; \mathrm{Tr}(A_\varepsilon) \;=\; \sum_{k=1}^{\infty} \langle \psi_k |\, A_\varepsilon \psi_k \rangle\,. \tag{II.78}$$

It follows from (II.78) and an application of (II.77) to $A - A_\varepsilon$ that

$$\begin{aligned} \left| \sum_{j=1}^{\infty} \langle \varphi_j |\, A\varphi_j \rangle \;-\; \sum_{k=1}^{\infty} \langle \psi_k |\, A\psi_k \rangle \right| \;&= \left| \sum_{j=1}^{\infty} \langle \varphi_j |\, (A - A_\varepsilon)\varphi_j \rangle \;-\; \sum_{k=1}^{\infty} \langle \psi_k |\, (A - A_\varepsilon)\psi_k \rangle \right| \\ &\leq 2\,\|A - A_\varepsilon\|_1 \;\leq\; 2\varepsilon\,. \end{aligned} \tag{II.79}$$

Since $\varepsilon > 0$ can be chosen arbitrarily small, (II.79) implies that

$$\sum_{j=1}^{\infty} \langle \varphi_j |\, A\varphi_j \rangle \;=\; \sum_{k=1}^{\infty} \langle \psi_k |\, A\psi_k \rangle\,. \tag{II.80}$$

The proof of cyclicity is similar: First, one observes that it suffices to prove $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for two trace-class operators $A, B \in \mathcal{L}^1(\mathcal{H})$. Then both A and B are approximated by finite-rank operators A_ε and B_ε up to errors in trace norm of size $\varepsilon > 0$. For A_ε and B_ε the identity $\mathrm{Tr}(A_\varepsilon B_\varepsilon) = \mathrm{Tr}(B_\varepsilon A_\varepsilon)$ is trivial. Hence,

$$\begin{aligned} \big|\mathrm{Tr}(AB) - \mathrm{Tr}(BA)\big| \;&\leq \big|\mathrm{Tr}(AB) - \mathrm{Tr}(A_\varepsilon B_\varepsilon)\big| \;+\; \big|\mathrm{Tr}(B_\varepsilon A_\varepsilon) - \mathrm{Tr}(BA)\big| \\ &\leq 2\big|\mathrm{Tr}[A(B - B_\varepsilon)]\big| \;+\; 2\big|\mathrm{Tr}[(A - A_\varepsilon)B_\varepsilon]\big| \\ &\leq 2\varepsilon\Big(\|A\|_1 + \|B\|_1 + \varepsilon\Big)\,, \end{aligned} \tag{II.81}$$

and $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ follows in the limit $\varepsilon \to 0$. □

III. Classical and Quantum Frameworks

In this section we describe the basic ingredients of the mathematical framework of classical and quantum computing in a somewhat peculiar way. That is, we first introduce the frameworks for classical mechanics of point particles, then for classical mechanics formulated as transport theory, and finally for quantum mechanics. Having introduced these we then develop the notion of classical computing in parallel to the classical mechanics of point particles. Similarly, we return to probabilistic methods of computation, such as simulated annealing, and finally come to the basic rules of quantum computing.

This approach is somewhat unorthodox, as it does not start with Qubits as the generalizations in quantum computing of bits. We hope, however, that basic concepts are clearer this way.

III.1. Classical and Quantum Mechanics of Particles in Space

Classical Mechanics of Point Particles. Suppose we wish to describe the motion of $N \in \mathbb{N}$ point particles moving in space $\mathbb{R}^3$. The motion of each particle is described by its position $q \in \mathbb{R}^3$ and its momentum $p \in \mathbb{R}^3$ which is put together in a phase space coordinate $x = (q, p) \in \Omega^{(1)} := \mathbb{R}^3 \times \mathbb{R}^3$. Then $x_k(t) = \big(q_k(t), p_k(t)\big) \in \Omega^{(1)}$ denotes the phase space coordinates of the k^{th} particle at a given time $t \in \mathbb{R}$. Putting these coordinates together in one N-tuple, the vector

$$\underline{x}(t) \;:=\; \big(x_1(t),\, x_2(t),\, \ldots,\, x_N(t)\big) \;\in\; \Omega^{(N)} \;:=\; [\Omega^{(1)}]^N\,, \tag{III.1}$$

encodes the complete desciption of the particles' phase space coordinates which we call phase space configuration. For this reason $\Omega^{(N)}$ is called the **phase space** of the system of N particles.

Almost two hundred years ago, Hamilton obtained a formulation of Newtonian mechanics that determines the phase space configuration $\underline{x}(t) \in \Omega^{(N)}$ of the system at time $t \in \mathbb{R}$ under

the assumption that the configuration $\underline{x}(s) \in \Omega^{(N)}$ is known for some $s < t$. For the sake of simplicity, we assume that $t > 0 = s$. The **dynamics** of the particles is determined by the *Hamilton equations of motion* which is a system of first-order ordinary differential equations, namely,

$$\forall\, t > 0: \quad \dot{\underline{x}}(t) \;=\; H'[\underline{x}(t)]\,, \qquad \underline{x}(0) = \underline{x}_0\,, \tag{III.2}$$

where

$$H'[\underline{x}(t)] \;:=\; \Big(\nabla_{\underline{p}} H[\underline{x}(t)],\; -\nabla_{\underline{q}} H[\underline{x}(t)]\Big) \tag{III.3}$$

is a (symplectic) gradient of the *Hamiltonian function* $H \in C^1(\Omega^{(N)}; \Omega^{(N)})$ of the system whose precise form is immaterial for our purpose. We do not go into the fairly complicated theory of existence and uniqueness of the solutions of Hamilton's equation (III.2) of motion. Instead we assume these two properties by demanding that there exists a **flow** (map) $\Phi \in C^1(\mathbb{R} \times \Omega^{(N)}; \Omega^{(N)})$ such that

$$\forall\, (t, \underline{x}_0) \in \mathbb{R} \times \Omega^{(N)}: \quad \underline{x}(t) \;=\; \Phi_t(\underline{x}_0)\,. \tag{III.4}$$

That is, for any initial configuration $\underline{x}_0 \in \Omega^{(N)}$ of spatial positions and momenta, the system of N particles follows the **trajectory** $\big(t \mapsto \Phi_t(\underline{x}_0)\big) \in C^1(\mathbb{R}_0^+; \Omega^{(N)}$.

Suppose we are now given an **observable**, i.e., a measurable physical quantity represented by a bounded, measurable real function $A \in L^\infty(\Omega^{(N)}; \mathbb{R})$ on phase space. A good example to have in mind, although neither bounded nor real-valued, is the center of mass $A : \Omega^{(N)} \to \mathbb{R}^3$ of the particles defined for $\underline{x} = (q_1, \ldots, q_N,\, p_1, \ldots, p_N)$ as

$$A[\underline{x}] \;:=\; \frac{1}{N} \sum_{k=1}^{N} q_k\,. \tag{III.5}$$

The center of mass $A_t[\underline{x}_0] \in \mathbb{R}^3$ of the particles at time $t > 0$ with initial configuration $\underline{x}_0 \in \Omega^{(N)}$ is then given by

$$A_t[\underline{x}_0] \;:=\; A[\underline{x}(t)] \;=\; A[\Phi_t(\underline{x}_0)]\,. \tag{III.6}$$

This equation holds true for any observable $A \in L^\infty(\Omega^{(N)}; \mathbb{R})$ - not only for the center of mass.

Probabilistic Formulation of Classical Mechanics. We now broaden our perspective and describe the system's configurations at time t not by points $\underline{x}(t)$ in phase space but by *functions* (or, more precisely, probability distributions) *on phase space*. For this, we replace the initial configuration $\underline{x}_0 \in \Omega^{(N)}$ by an initial phase space density, i.e., a probability distribution $\rho_0 \in L^1(\Omega^{(N)}; \mathbb{R}_0^+)$, with $\int_{\Omega^{(N)}} \rho_0(\underline{x})\, d\underline{x} = 1$, where $d\underline{x} = d^N q\, d^N p$ is Lebesgue measure on phase space $\Omega^{(N)}$. The physical state of the system is now represented by the function $\rho_0 : \Omega^{(N)} \to \mathbb{R}_0^+$, not the point $\underline{x}_0 \in \Omega^{(N)}$. As each of the points $\underline{x}_0 \in \Omega^{(N)}$, considered a

potential initial configuration, follows its trajectory, the state of the system at time $t > 0$ is then given by

$$\rho_t \;=\; \rho_0 \circ \Phi_{-t}\,. \tag{III.7}$$

(Note the minus sign in the time variable.) Since the flow Φ_t leaves the measure on phase space invariant, $\rho_t \in L^1(\Omega^{(N)};\mathbb{R}_0^+)$ is a probability distribution, too. We now evaluate an observable $A \in L^\infty(\Omega^{(N)};\mathbb{R})$ at time $t \geq 0$. Since ρ_t is a probability distribution, this is actually an *expectation value* and is given by

$$\langle A\rangle_{\rho_t} \;:=\; \int_{\Omega^{(N)}} A[\underline{x}]\;\rho_t(\underline{x})\;d\underline{x} \;=\; \int_{\Omega^{(N)}} A[\underline{x}]\;\rho_0[\Phi_{-t}(\underline{x})]\;d\underline{x}\,. \tag{III.8}$$

Note that our first description in terms of phase space points is contained in this larger framework if, slightly more generally, we allow ρ_0 to be a probabilty measure -not necessarily an integrable function- and assume $A \in C(\Omega^{(N)};\mathbb{R})$ to be continuous. Namely, choosing $\rho_0(\underline{x}) := \delta(\underline{x} - \underline{x}_0)$, Eq. (III.8) yields

$$\langle A\rangle_{\rho_t} \;=\; \int_{\Omega^{(N)}} A[\underline{x}]\;\delta[\Phi_{-t}(\underline{x}) - \underline{x}_0]\;d\underline{x} \;=\; \int_{\Omega^{(N)}} A[\underline{x}]\;\delta[\underline{x} - \Phi_t(\underline{x}_0)]\;d\underline{x} \;=\; A[\Phi_t(\underline{x}_0)]\,, \tag{III.9}$$

indeed. This computation also illustrates the necessity of the minus sign in (III.7).

The formulation in terms of functions (here: probability distributions) on phase space has two decisive advantages.

- The first is that the (expectation) value $\langle A\rangle_{\rho_t}$ of an observable is a *linear functional* of both the observable $A \in L^\infty(\Omega^{(N)};\mathbb{R})$ and the function $\rho_t \in L^1(\Omega^{(N)};\mathbb{R}_0^+)$. More precisely, for all functions $\rho \in L^1(\Omega^{(N)})$, the expectation value

$$\big(A \mapsto \langle A\rangle_\rho\big) \;\in\; \big[L^\infty(\Omega^{(N)})\big]^* \tag{III.10}$$

  defines a continuous linear functional on $L^\infty(\Omega^{(N)})$. Conversely, if $\alpha \in (0,1)$ and $\rho, \widetilde{\rho} \in L^1(\Omega^{(N)};\mathbb{R}_0^+)$ are two probability densities on $\Omega^{(N)}$ then so is $[\alpha\rho + (1-\alpha)\widetilde{\rho}] \in L^1(\Omega^{(N)};\mathbb{R}_0^+)$, and for all observables $A \in L^\infty(\Omega^{(N)})$, the expectation value of $\alpha\rho + (1-\alpha)\widetilde{\rho}$ is given by

$$\langle A\rangle_{\alpha\rho+(1-\alpha)\widetilde{\rho}} \;=\; \alpha\,\langle A\rangle_\rho \;+\; (1-\alpha)\,\langle A\rangle_{\widetilde{\rho}}\,. \tag{III.11}$$

- The second, more important, advantage is that the form $\rho_t = \rho_0 \circ \Phi_{-t}$ of the solution of the time evolution in terms of a flow map is special and rather rigid. Most of the important evolution equations in physics and technology other than classical mechanics do not posess solutions of this form. We illustrate this argument on the example of the heat equation in $\mathbb{R}^3$. Given an initial temperature profile $\rho_0 \in L^1(\mathbb{R}^3;\mathbb{R}_0^+)$, the temperature profile at time $t > 0$ is the unique solution u_t of the heat equation

$$\forall\, t > 0,\; x \in \mathbb{R}^3 : \quad \dot{u}_t(x) \;=\; \Delta_x u_t(x)\,, \qquad u_0(x) = \rho_0(x)\,, \tag{III.12}$$

which can be explicitly computed by convolving the initial profile with the heat kernel,

$$\forall\, t > 0,\ x \in \mathbb{R}^3 : \quad u_t(x) \ = \ \int e^{-(x-y)^2/(4t)}\, \rho_0(y)\, \frac{d^3y}{(4\pi t)^{3/2}}\,. \tag{III.13}$$

There exists no flow map such that u_t could be written in the form $u_t(x) = \rho_0[\Phi_t(x)]$, for all $x \in \mathbb{R}^3$. (Nevertheless, the Ansatz $u_t(x) = \rho_0[\Phi_t(x)]$ is a useful method known as the *method of characteristics* in PDE theory to construct approximate solutions for small times.)

The corresponding generalization of Eq. (III.7) results from assuming that, given $t > 0$, there exists a conditional probability distribution $p_t : \Omega^{(N)} \times \Omega^{(N)} \to \mathbb{R}_0^+$ such that

$$\forall\, \underline{x} \in \Omega^{(N)} : \qquad \rho_t(\underline{x}) \ = \ \int_{\Omega^{(N)}} p_t(\underline{x}|\underline{y})\, \rho_0(\underline{y})\, d\underline{y}\,. \tag{III.14}$$

The requirement that p_t be a conditional probability distribution reads

$$\forall\, \underline{y} \in \Omega^{(N)} : \qquad \int_{\Omega^{(N)}} p_t(\underline{x}|\underline{y})\, d\underline{x} \ = \ 1\,, \tag{III.15}$$

which ensures by Fubini that

$$\int \rho_t(\underline{x})\, d\underline{x} \ = \ \iint p_t(\underline{x}|\underline{y})\, \rho_0(\underline{y})\, d\underline{x}\, d\underline{y} \ = \ \int \rho_0(\underline{y})\, d\underline{y}\,, \tag{III.16}$$

i.e., if $\rho_0 \in L^1(\Omega^{(N)}; \mathbb{R}_0^+)$ is a probability distribution then so is $\rho_t \in L^1(\Omega^{(N)}; \mathbb{R}_0^+)$. (Note that we are generous about measure-theoretic details such as (III.15) that actually is only required almost everywhere in $\Omega^{(N)}$.)

We illustrate the formulation (III.14) by two examples.

- The original motion of N point particles can be formulated as in (III.14) if we set

  $$p_t(\underline{x}|\underline{y}) \ := \ \delta[\underline{x} - \Phi_t(\underline{y})]\,, \tag{III.17}$$

  since, with this choice of p_t, we obtain

  $$\rho_t(\underline{x}) \ = \ \int_{\Omega^{(N)}} \delta[\underline{x} - \Phi_t(\underline{y})]\, \rho_0(\underline{y})\, d\underline{y} \ = \ \rho_0[\Phi_{-t}(\underline{x})]\,. \tag{III.18}$$

- The heat kernel $p_t(x|y) = (4\pi t)^{-3/2} \exp[-(x-y)^2/(4t)]$ used in (III.13) to solve the heat equation is a second, typical example for such conditional probability distribution. Indeed, for all $y \in \mathbb{R}^3$ and $t > 0$,

  $$\int_{\mathbb{R}^3} p_t(x|y)\, d^3x \ = \ \int_{\mathbb{R}^3} \frac{e^{-(x-y)^2/(4t)}\, d^3x}{(4\pi t)^{3/2}} \ = \ \int_{\mathbb{R}^3} \frac{e^{-x^2}\, d^3x}{\pi^{3/2}} \ = \ 1\,. \tag{III.19}$$

Compared to quantum mechanics, the probablilistic formulation of classical mechanics has the disadvantage that, unless we are in a special case like (III.17), the dynamics is irreversible: Given ρ_0, we can compute ρ_t for $t > 0$, but given $t > 0$ and ρ_t, the reconstruction of the initial data ρ_0 is a rather complicated and, in fact, in many cases impossible. For instance, if u_t is the solution of the heat equation according to (III.13) then it is not hard to see that $u_t \in C^\infty(\mathbb{R}^3)$ is smooth. Consequently, if $t > 0$ and u_t is lacking this high regularity, there is no initial datum u_0 for which u_t is the solution of the heat equation at time t.

Quantum Mechanics. Similar to the probabilistic description of mechanics, we do not represent the state of the system of N point particles in quantum mechanics by a configuration $\underline{x}(t)$ in phase space, but by a complex-valued function ψ_t on the space of configurations $\Omega^{(N)}$. We now go through the construction step by step.

- As opposed to classical mechanics, the configuration space of a quantum mechanical particle contains only positions, not momenta. In a first step the state of a particle at time $t \in \mathbb{R}$ is represented by a complex-valued, square-integrable function $\psi_t : \Omega^{(1)} \to \mathbb{C}$ of the particle's position $x \in \Omega^{(1)} := \mathbb{R}^3$. Thanks to their square-integrability, these functions are elements $\psi_t \in \mathfrak{h}$ of the Hilbert space $\mathfrak{h} := L^2(\mathbb{R}^3)$.
- We further assume ψ_t to be normalized, i.e.,

$$\|\psi_t\|_2^2 \;=\; \int_{\Omega^{(1)}} |\psi_t(\underline{x})|^2 \, d\underline{x} \;=\; 1\,, \tag{III.20}$$

  so that the square of the absolute value $|\psi_t|^2 : \mathbb{R}^3 \to \mathbb{R}_0^+$ allows for the intepretation to be the probability distribution of the particle at time t. I.e., $P_t(A) := \int_A |\psi_t(x)|^2 \, d^3x$ is the probability to find the particle in a (measurable) subset $A \subseteq \Omega^{(1)}$ of its configuration space $\Omega^{(1)}$.
- Similarly, the configuration space $\Omega^{(N)} := [\Omega^{(1)}]^N = (\mathbb{R}^3)^N$ of N quantum mechanical particles contains N positions in $\Omega^{(1)}$ (and no momenta). The state of the N-particle system at time $t \in \mathbb{R}$ is represented by a complex-valued, square-integrable function $\Psi_t : \Omega^{(N)} \to \mathbb{C}$ of the N-particle configurations $\underline{x} \in \Omega^{(N)}$. Again its square-integrability ensures that this function $\Psi_t \in \mathfrak{H}^{(N)}$ belongs to the Hilbert space $\mathfrak{H}^{(N)} := L^2(\Omega^{(N)})$.
- As a mathematical fact, if $\Omega = \Omega_1 \times \Omega_2 = \{(x_1, x_2) |\; x_1 \in \Omega_1, x_2 \in \Omega_2\}$ is the cartesian product of two sets Ω_1 and Ω_2 then $L^2(\Omega)$ is isomorphic to the tensor product $L^2(\Omega_1) \otimes L^2(\Omega_1)$.
- This can be generalized to N factors: If $(\Omega_n, \mathfrak{A}_n, \mu_n)$ are measure spaces, for all $n \in \mathbb{Z}_1^N$, and

$$\Omega \;=\; \Omega_1 \times \Omega_2 \times \cdots \times \Omega_N \;=\; \big\{(x_1, x_2, \ldots, x_N) \;\big|\; x_1 \in \Omega_1, x_N \in \Omega_N\big\} \tag{III.21}$$

  is their cartesian product, then

$$L^2(\Omega) \;=\; L^2(\Omega_1) \otimes L^2(\Omega_2) \otimes \cdots \otimes L^2(\Omega_N)\,. \tag{III.22}$$

The dynamics of the N-particle system is given by the Schrödinger equation,

$$\forall\, t \in \mathbb{R}: \quad \dot{\psi}_t \;=\; -iH\psi_t\,, \qquad \psi_0 \in \mathcal{H}^{(N)}\,. \tag{III.23}$$

Here, $H = H^*$ is the self-adjoint Hamiltonian operator acting on $\mathcal{H}^{(N)}$) (Very often H is actually an unbounded operator, but we ignore the mathematical complication that comes about with this unboundedness.) Thanks to its self-adjointness, H generates a one-parameter

group $(U_t)_{t\in\mathbb{R}} \subseteq \mathcal{U}(\mathcal{H}^{(N)})$ of unitary operators which is frequently called **propagator**, written as $\boldsymbol{U_t =: e^{-itH}}$. The unique solution of the Schrödinger equation is given by

$$\forall\, t \in \mathbb{R}: \qquad \psi_t \;=\; U_t\,\psi_0\,. \tag{III.24}$$

The Schrödinger equation can also be formulated as an evolution equation for the propagator, i.e.,

$$\forall\, t \in \mathbb{R}: \qquad \dot{U}_t \;=\; -iHU_t\,, \qquad U_0 = \mathbf{1}_{\mathcal{H}^{(N)}}\,. \tag{III.25}$$

Note that the quantum evolution (III.24) is perfectly reversible, namely, $\psi_0 = U_t^*\psi_t$, since $U_t^{-1} = U_t^*$, as U_t is unitary.

Observables in quantum mechanics are represented by self-adjoint operators $A = A^* \in \mathcal{B}(\mathcal{H}^{(N)})$. In fact, the Hamiltonian H is an observable, too, namely the system's energy. While H is an unbounded operator, we may always assume w.l.o.g. a given observable $A = A^* \in \mathcal{B}(\mathcal{H}^{(N)})$ to be bounded. Its expectation value at time $t \in \mathbb{R}$ is defined to be the diagonal matrix element

$$\forall\, t \in \mathbb{R}: \qquad \langle A_t\rangle_{\psi_0} \;=\; \langle\psi_0|A_t\psi_0\rangle \;:=\; \langle\psi_t|A\psi_t\rangle \;=\; \langle\psi_0|(U_t^*AU_t)\,\psi_0\rangle\,. \tag{III.26}$$

Note that this implies that $A_t = U_t^*AU_t$. Hence, using (III.25), we obtain the Heisenberg equation of motion

$$\forall\, t \in \mathbb{R}: \qquad \dot{A}_t \;=\; -i\big[H\,,\,A_t\big]\,, \tag{III.27}$$

which is actually equivalent to the Schrödinger equation.

Embedded Systems in Quantum Mechanics and Density Matrices Summarizing the framework of quantum mechanics presented so far, we note that states of a physical system S at time $t \in \mathbb{R}$ are represented by vectors $\psi_t \in \mathcal{H}_S$ in the system's Hilbert space $\mathcal{H}_S$, which typically is the space of complex-valued, square-integrable functions of the (classical spatial) coordinates $x \in \Omega_S$ of the system, i.e., $\mathcal{H}_S = L^2(\Omega_S)$.

Suppose now that S_1 is a physical system with coordinate space Ω_1 and quantum mechanical states in $\mathcal{H}_1 = L^2(\Omega_1)$. If S_1 is actually a subsystem of a larger total system S_{12} containing another subsystem S_2, besides S_1, with classical coordinates in Ω_2 then the coordinate space of the total system S_{12} is naturally $\Omega_{12} = \Omega_1 \times \Omega_2$, and the corresponding Hilbert space of states in S_{12} is $L^2(\Omega_{12}) = L^2(\Omega_1) \otimes L^2(\Omega_2)$.

More generally, tensor products appear in quantum mechanics whenever we have two physical subsystems S_1 and S_2 and the total system S_{12} consists of these two subsystems. If the states of S_1 and S_2 are vectors in a Hilbert space $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, then the states of the total system are vectors in their tensor product $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

Remarks and Examples.

- If S_1 represents an electron and S_2 represents a proton then $\Omega_1 = \Omega_2 = \mathbb{R}^3 \times \{\uparrow, \downarrow\}$ and $\mathcal{H}_1 = \mathcal{H}_2 = L^2(\mathbb{R}^3 \times \{\uparrow, \downarrow\})$. The total system S_{12} contains an electron and a proton and may be considered a hydrogen atom; its Hilbert space is $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2 = L^2(\mathbb{R}^3 \times \{\uparrow, \downarrow\}) \otimes L^2(\mathbb{R}^3 \times \{\uparrow, \downarrow\})$.
- If S_3 is the quantized photon field then its Hilbert space is the photon Fock space $\mathcal{F}(\mathfrak{h})$ over the one-photon Hilbert space $\mathfrak{h} = \left\{ f \in L^2(\mathbb{R}^3; \mathbb{R}^3) \,\middle|\, \forall\, \vec{k} \in \mathbb{R}^3 \setminus \{\vec{0}\} :\ \hat{f}(\vec{k}) \perp \vec{k} \right\}$ of square-integrable, divergent-free vector fields (Coulomb gauge).
- If the total system S_{123} consists of a hydrogen atom and the quantized radiation field then its Hilbert space is $\mathcal{H}_{123} = \mathcal{H}_{12} \otimes \mathcal{F}(\mathfrak{h})$.

We now consider a system S_1 whose states are represented by normalized vectors ψ_1 in a Hilbert space $\mathcal{H}_1$. We wish to account for the possibility that S_1 is a subsystem of a larger system S_{12} whose states are represented by normalized vectors Ψ_{12} in a Hilbert space $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{H}_2$ is the Hilbert space for the other constituent of S_{12}, namely, a subsystem S_2. For definiteness, we assume both $\mathcal{H}_1$ and $\mathcal{H}_2$ to be infinite dimensional.

If $A_1 = A_1^* \in \mathcal{B}(\mathcal{H}_1)$ is an observable of the system S_1 then its expectation value in the state $\Psi_{12} \in \mathcal{H}_{12}$ is given by

$$\langle A_1 \rangle_{\Psi_{12}} \;=\; \langle \Psi_{12} | (A_1 \otimes \mathbf{1}_2) \Psi_{12} \rangle_{12} \,. \tag{III.28}$$

This expectation value is of the form $\langle A_1 \rangle_{\Psi_{12}} = \langle \psi_1 | A_1 \psi_1 \rangle_{\mathcal{H}_1}$, for some $\psi_1 \in \mathcal{H}_1$ if, and only if, $\Psi_{12} = \psi_1 \otimes \psi_2$. This is, however, unphysical because it is equivalent to assuming the two subsystems S_1 and S_2 to be independent of each other and in absence of any interaction between them.

Now we suppose that $\Psi \in \mathcal{H}_{12}$ is an arbitray normalized vector. We define a linear operator $\rho_1 \in \mathcal{B}(\mathcal{H}_1)$ by

$$\big\langle f \big|\, \rho_1\, f' \big\rangle_1 \;:=\; \sum_{n=1}^{\infty} \Big\langle f \otimes g_n \Big| \big(|\Psi\rangle\langle\Psi| \big)\, f' \otimes g_n \Big\rangle_{12} \;=\; \sum_{n=1}^{\infty} \langle f \otimes g_n | \Psi \rangle_{12}\, \langle \Psi | f' \otimes g_n \rangle_{12} \,, \tag{III.29}$$

where $\{g_n\}_{n=1}^{\infty} \subseteq \mathcal{H}_2$ is an arbitrary ONB. A simple application of the Cauchy-Schwarz inequality shows that (III.29) is convergent and independent of the ONB $\{g_n\}_{n=1}^{\infty}$. Obviously, $\rho_1 \geq 0$ is positive. If $\{f_m\}_{m=1}^{\infty} \subseteq \mathcal{H}_1$ is an ONB then

$$\sum_{m=1}^{\infty} \big\langle f_m \big|\, \rho_1\, f_m \big\rangle_1 \;:=\; \sum_{m,n=1}^{\infty} \Big\langle f_m \otimes g_n \Big| \big(|\Psi\rangle\langle\Psi| \big)\, f_m \otimes g_n \Big\rangle_{12} \;=\; \|\Psi\|^2 \;=\; 1 \,. \tag{III.30}$$

Hence, $\rho_1 \in \boldsymbol{\mathcal{DM}(\mathcal{H}_1)}$ is a **density matrix**, i.e., a positive trace class operator on a Hilbert space $\mathcal{H}$ of trace one,

$$\mathcal{DM}(\mathcal{H}) \;:=\; \Big\{ \rho \in \mathcal{L}^1(\mathcal{H}) \;\Big|\; \rho \geq 0 \,,\ \mathrm{Tr}(\rho) = 1 \Big\} \,. \tag{III.31}$$

We observe that $\mathcal{DM}(\mathcal{H}) \subseteq \mathcal{L}^1(\mathcal{H})$ is closed and convex. In fact, $\mathcal{DM}(\mathcal{H})$ is the convex hull of all pure states, i.e., density matrices of the form $|\psi\rangle\langle\psi|$, with ψ normalized.

Moreover, if $\rho_{12} \in \mathcal{DM}(\mathcal{H}_{12})$ is a density matrix of the total system S_{12} on the Hilbert space $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ and

$$\sum_{m=1}^{\infty} \big\langle f_m \big|\, \rho_1\, f_m \big\rangle_1 \;:=\; \sum_{m,n=1}^{\infty} \Big\langle f_m \otimes g_n \Big| \rho_{12}\, (f_m \otimes g_n) \Big\rangle_{12}\,, \tag{III.32}$$

then $\rho_1 \in \mathcal{DM}(\mathcal{H}_1)$ is a density matrix for the subsystem S_1 of S_{12}.

For this reason we replace wave functions by density matrices and represent states of physical systems by the latter, henceforth. If $A = A^* \in \mathcal{B}(\mathcal{H})$ is an observable of a system in a state represented by a density matrix $\rho \in \mathcal{DM}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$, then its expectation value is given by

$$\langle A \rangle_\rho \;:=\; \mathrm{Tr}(\rho\, A)\,. \tag{III.33}$$

If the density matrix $\rho_t \in \mathcal{DM}(\mathcal{H})$ at time $t \in \mathbb{R}$ is the pure state $\rho_t = |\psi_t\rangle\langle\psi_t|$, then ρ_t results from the initial value ρ_0 by conjugation by the unitary propagator $U_t \in \mathcal{U}(\mathcal{H})$ of (III.24)-(III.25), i.e.,

$$\rho_t \;=\; |U_t\psi_0\rangle\langle U_t\psi_0| \;=\; U_t\, |\psi_0\rangle\langle\psi_0|\, U_t^* \;=\; U_t\, \rho_0\, U_t^* \tag{III.34}$$

Taking convex combinations of such pure states, we derive the dynamical law for a general density matrix $\rho_t \in \mathcal{DM}(\mathcal{H})$ representing the state of the system at time $t \in \mathbb{R}$, given its value $\rho_0 \in \mathcal{DM}(\mathcal{H})$ at $t = 0$,

$$\rho_t \;=\; U_t\, \rho_0\, U_t^*\,, \quad \dot\rho_t \;=\; -i[H, \rho_t]\,. \tag{III.35}$$

It is interesting to note that the equation of motion $\dot\rho_t \;=\; -i[H, \rho_t]$ is (potentially) easier to solve than the Schrödinger equation $\dot\psi_t \;=\; -iH\psi_t$, because the former does not follow oscillations of the phase in ψ_t anymore. Namely, for any choice of $\theta : \mathbb{R} \to \mathbb{R}$ and with $\psi_t^{(\theta)} := e^{i\theta(t)}\psi_t$, the density matrix $\rho_t = |\psi_t^{(\theta)}\rangle\langle\psi_t^{(\theta)}|$ is independent of θ.[1]

Another reason that lets density matrices appear superior to wave functions is that, while a linear combination of wave functions is again a wave function, its normalization is not preserved, in general. In contrast, the set $\mathcal{DM}(\mathcal{H}) \subseteq \mathcal{L}^1(\mathcal{H})$ of density matrices over a Hilbert space $\mathcal{H}$ is convex (and closed). So, given two density matrices $\rho_0, \rho_1 \in \mathcal{DM}(\mathcal{H})$ and $\alpha \in [0, 1]$, the operator $\rho_\alpha := (1-\alpha)\rho_0 + \alpha\rho_1 \in \mathcal{DM}(\mathcal{H})$ is a density matrix, as well.

Remarks and Examples. We exemplify this on a single qubit, i.e., $\mathcal{H} = \mathbb{C}^2$. We analyze the space $\mathcal{SA}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H}) \cong \mathbb{C}^{2\times 2}$ by first observing that if $A \in \mathcal{B}(\mathcal{H})$ is given by

$$A \;=\; \begin{pmatrix} a & b \\ c & d \end{pmatrix}\,, \tag{III.36}$$

[1] I thank Thierry Paul for sharing this observation with me.

for some $a, b, c, d \in \mathbb{C}$ then $A = A^*$ iff $a, d \in \mathbb{R}$ and $c = \bar{b}$. So, any self-adjoint complex 2×2 matrix can be written as

$$\begin{aligned} A \;&=\; \begin{pmatrix} \alpha + \delta & \beta + i\gamma \\ \beta - i\gamma & \alpha - \delta \end{pmatrix} \\ &= \alpha\, \mathbf{1} \;+\; \beta\, \sigma^{(1)} \;+\; \gamma\, \sigma^{(2)} \;+\; \delta\, \sigma^{(3)}\,, \end{aligned} \tag{III.37}$$

for unique numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$, where $\mathbf{1} \in \mathbb{C}^{2\times 2}$ is the unit and $\sigma^{(1)}, \sigma^{(2)}, \sigma^{(3)} \in \mathbb{C}^{2\times 2}$ are the self-adjoint Pauli matrices defined as

$$\mathbf{1} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\,,\;\; \sigma^{(1)} \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\,,\;\; \sigma^{(2)} \;=\; \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\,,\;\; \sigma^{(3)} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\,. \tag{III.38}$$

It is convenient to equip the real vector space $\mathcal{SA}(\mathbb{C}^2)$ with the scalar product $\langle A, B\rangle := \mathrm{Tr}(AB)$ which makes it a real Hilbert space $\big(\mathcal{SA}(\mathbb{C}^2), \langle\cdot,\cdot\rangle\big)$. Using the fact that

$$\sigma^{(j)}\, \sigma^{(k)} \;=\; \delta_{j,k} \cdot \mathbf{1} \;+\; i \sum_{\ell=1}^{3} \varepsilon_{jk\ell}\, \sigma^{(\ell)}\,, \tag{III.39}$$

where the *totally antisymmetric symbol* $\varepsilon_{jk\ell}$ is defined by

$$\forall\, \{j,k,\ell\} \subseteq \{1,2,3\}: \quad \varepsilon_{jk\ell} \;:=\; \begin{cases} \mathrm{sgn} \begin{pmatrix} 1 & 2 & 3 \\ j & k & \ell \end{pmatrix}, & \text{for } \{j,k,\ell\} \;=\; \{1,2,3\}\,, \\ 0, & \text{for } \{j,k,\ell\} \;\neq\; \{1,2,3\}\,, \end{cases} \tag{III.40}$$

it is easy to check that

$$\big\{ \tfrac{1}{\sqrt{2}}\, \mathbf{1},\; \tfrac{1}{\sqrt{2}}\, \sigma^{(1)},\; \tfrac{1}{\sqrt{2}}\, \sigma^{(2)},\; \tfrac{1}{\sqrt{2}}\, \sigma^{(3)} \big\} \;\subseteq\; \mathcal{SA}(\mathbb{C}^2) \tag{III.41}$$

is orthonormal and thus an ONB, since $\dim_{\mathbb{R}}[\mathcal{SA}(\mathbb{C}^2)] = 4$. This implies that

$$\forall\, A \in \mathcal{SA}(\mathbb{C}^2): \quad A \;= \tfrac{1}{2}\mathrm{Tr}(A)\, \mathbf{1} \;+\; \tfrac{1}{2} \vec{v}_A \cdot \vec{\sigma}\,, \tag{III.42}$$

where $\vec{\sigma} = \big(\sigma^{(1)}, \sigma^{(2)}, \sigma^{(3)}\big)^t$, $\vec{v}_A = \big(v_A^{(1)}, v_A^{(2)}, v_A^{(3)}\big)^t$, and

$$\mathrm{Tr}(A) \;=\; \langle \mathbf{1}, A\rangle \quad \text{and} \quad v_A^{(j)} \;=\; \langle \sigma^{(j)}, A\rangle \;=\; \mathrm{Tr}\big(\sigma^{(j)}\, A\big)\,. \tag{III.43}$$

Moreover, from (III.37) we see that

$$\det(A) \;=\; \alpha^2 - \beta^2 - \gamma^2 - \delta^2 \;=\; \frac{1}{4}\Big([\mathrm{Tr}(A)]^2 - |\vec{v}_A|^2 \Big)\,. \tag{III.44}$$

Specifically, if $\rho \in \mathcal{DM}(\mathbb{C}^2)$ is a density matrix then it is positive, and therefore its determinant is nonnegative. Thus $|\vec{v}_\rho| \leq \mathrm{Tr}(\rho) = 1$, i.e., $\vec{v}_\rho \in \overline{B(0,1)} \subseteq \mathbb{R}^3$ is a vector of length less or equal to one in three-dimensional Euclidean space. Moreover, ρ has the eigenvalues

$\lambda, 1-\lambda \in [0,1]$. It follows that $\lambda(1-\lambda) = \det(\rho) = (1-\vec{v}_\rho^2)/4$ which, in turn, is equivalent to

$$\sigma(\rho) \;=\; \{\lambda,\, 1-\lambda\} \;=\; \Big\{\tfrac{1}{2}\big(1-|\vec{v}_\rho|\big)\,,\; \tfrac{1}{2}\big(1+|\vec{v}_\rho|\big)\Big\}\,. \tag{III.45}$$

In summary, it follows that

$$\mathcal{DM}(\mathbb{C}^2) \;=\; \Big\{\tfrac{1}{2}\big(\mathbf{1} \;+\; \vec{v}\cdot\vec{\sigma}\big)\;\Big|\vec{v}\in\mathbb{R}^3\,,\; |\vec{v}|_{\rm eucl}\leq 1\Big\}\,, \tag{III.46}$$

i.e., the convex set of density matrices on $\mathbb{C}^2$ can be identified with the closed unit ball in $\mathbb{R}^3$. The unit sphere in $\mathbb{R}^3$ is called the **Bloch sphere** in this context. It contains all extremal density matrices, i.e., all pure density matrices, i.e., all rank-one orthogonal projections. Any density matrix can be written as a convex combination of pure density matrices, and here we see that in the case of $\mathcal{H} = \mathbb{C}^2$, any density matrix can be written as a convex combination of (not more than) two pure density matrices.

III.2. Classical and Quantum Computation

Classical Computation. Now we turn away from physics but describe the framework of classical computation (by a computer) as if this was a physical system. The role of the particles is now played by *bits ($N = 1$)* or *bytes ($N \in \mathbb{N}$, $N \geq 2$)*, which we intepret as points $\underline{\sigma} = (\sigma_1, \ldots, \sigma_N) \in \Omega^{(N)}$ moving in the configuration space $\Omega^{(N)} := \{0,1\}^N$. A computation is a change of such a byte in time. Since computations are carried out in steps - not continuously, time is measured by integral numbers. That is, the state of a computation at time $t \in \mathbb{N}_0$ is

$$\underline{\sigma}(t) \;=\; \big(\sigma_1(t), \sigma_2(t), \ldots, \sigma_N(t)\big) \;\in\; \Omega^{(N)}\,. \tag{III.47}$$

Computations are trajectories $\underline{\sigma} : \mathbb{N}_0 \to \Omega^{(N)}$ of discrete time $t \in \mathbb{N}_0$, taking values in the finite set $\Omega^{(N)}$, $|\Omega^{(N)}| = 2^N$. The computation proceeds by applying a dynamical law to determine $\underline{\sigma}(t)$ from $\underline{\sigma}(t-1)$,

$$\forall\, t \in \mathbb{N}: \quad \underline{\sigma}(t) \;=\; F_t[\,\underline{\sigma}(t-1)]\,, \tag{III.48}$$

where $F_t : \Omega^{(N)} \to \Omega^{(N)}$, for any $t \in \mathbb{N}$. Any real-valued map $A : \Omega^{(N)} \to \mathbb{R}$ on the configuration space of all bytes defines an observable whose value at time $t \in \mathbb{N}_0$ for a given initial value $\underline{\sigma}(0) \in \Omega^{(N)}$ is given by

$$A_t[\underline{\sigma}(0)] \;:=\; A[\underline{\sigma}(t)] \;=\; A_t \circ F_t \circ F_{t-1} \circ \cdots \circ F_1[\underline{\sigma}(0)] \tag{III.49}$$

Probability in Classical Computations. Many problems in computation are naturally formulated in a probabilistic framework. One of these situations occurs in case our task is to

determine the minimum E_0 of a given function $H : \Omega^{(N)} \to \mathbb{R}$ and the set M of minimizers, i.e.,

$$M \;:=\; \big\{\underline{\sigma} \in \Omega^{(N)} \;\big|\; H(\underline{\sigma}) \;=\; E_0\big\}\,. \tag{III.50}$$

Among the methods to compute E_0 and M is *Simulated Annealing* or the *Monte Carlo Algorithm*, which we briefliy describe here.

(1) One chooses a starting point $\underline{\sigma}(0) = \big(\sigma_1(0), \ldots, \sigma_N(0)\big) \in \Omega^{(N)}$ and evaluates $H[\underline{\sigma}(0)]$. (The choice of the starting point may be random, but for many problems it is decisive to make a good guess which is not too far away from M.)

(2) For $t \in \mathbb{N}_0$ choose an index $j \in \mathbb{Z}_1^n$ randomly and set $\underline{\sigma}'(t+1) = \big(\sigma_1'(t+1), \ldots, \sigma_N'(t+1)\big) \in \Omega^{(N)}$ such that it differs from $\underline{\sigma}(t)$ exactly at the j^{th} position. Explicitly,

$$\forall\, k \in \mathbb{Z}_1^N : \quad \underline{\sigma}_k'(t+1) \;:=\; \begin{cases} \underline{\sigma}_k(t)\,, & \text{for} \quad k \neq j\,, \\ 1 - \underline{\sigma}_k(t)\,, & \text{for} \quad k = j\,. \end{cases} \tag{III.51}$$

(3) Evaluate $H[\underline{\sigma}(t+1)]$.

(3a) If $H[\underline{\sigma}(t)] \geq H[\underline{\sigma}'(t+1)]$ then $\underline{\sigma}(t+1) := \underline{\sigma}'(t+1)$.

(3b) Conversely, if $H[\underline{\sigma}(t)] < H[\underline{\sigma}'(1)]$ then

$$\underline{\sigma}(t+1) \;:=\; \begin{cases} \underline{\sigma}'(t+1) & \text{with probability} \quad e^{-\beta\{H[\underline{\sigma}(t)] - H[\underline{\sigma}'(t+1)]\}}\,, \\ \underline{\sigma}(t) & \text{with probability} \quad 1 - e^{-\beta\{H[\underline{\sigma}(t)] - H[\underline{\sigma}'(t+1)]\}}\,. \end{cases} \tag{III.52}$$

Now replace t by $t+1$ and repeat the procedure from (2) on.

It can be proved that the trajectory $\big(\underline{\sigma}(t)\big)_{t \in \mathbb{N}_0}$ generated by the algorithm above concentrates on M. We do not go into detail here but only note that, while the framework is probabilistic, the computations carried out here are classical.

Quantum Computations. For quantum computers, we proceed in analogy to quantum mechanics: A configuration of the computer specified by a single bit $\sigma \in \Omega^{(1)} = \{0, 1\}$ is replaced by a complex function $\psi(\sigma) \in \mathbb{C}$ of this bit. The configuration space $\Omega^{(1)} = \{0, 1\}$ of the bit is hence replaced by the Hilbert space $\mathcal{H}^{(1)} := \ell^2(\Omega^{(1)}) \cong \mathbb{C}^2$ and the configuration $\psi \in \mathcal{H}^{(1)}$ is called **qubit**. Here, $V \cong W$ denotes isomorphy of Hilbert spaces.

Likewise, the configuration space of $N \in \mathbb{N}$ bits is replaced by the Hilbert space of N qubits,

$$\mathcal{H}^{(N)} \;:=\; \ell^2(\Omega^{(N)}) \;\cong\; \mathbb{C}^{2N} \;\cong\; \bigotimes^{N} \mathbb{C}^2\,, \tag{III.53}$$

The state of a quantum computer at time $t \in \mathbb{N}_0$ is described by a density matrix

$$\rho(t) \;\in\; \mathcal{DM}\big(\mathcal{H}^{(N)}\big)\,. \tag{III.54}$$

A quantum computation of $T \in \mathbb{N}$ steps is a family $u : \mathbb{Z}_1^T \to \mathcal{U}(\mathcal{H}^{(N)})$ such that $\rho(t)$ results from $\rho(t-1)$ by conjugation with $u(t) \in \mathcal{U}(\mathcal{H}^{(N)})$, for any time $t \in \mathbb{Z}_1^T$, that is

$$\rho(t) \;=\; u(t)\,\rho(t-1)\,u^*(t) \;=\; u(t)\cdots u(1)\,\rho(0)\,u^*(1)\cdots u^*(t)\,. \tag{III.55}$$

In particular, the final state is obtained from a unitary transformation of the initial state, too. More specifically,

$$\rho(T) \;=\; U(T)\,\rho(0)\,U^*(T)\,, \quad \text{with} \quad U(T) \;:=\; u(t)\cdots u(1) \;\in\; \mathcal{U}(\mathcal{H}^{(N)})\,. \tag{III.56}$$

Expectation values of states of quantum computers are defined just as in quantum mechanics: If $M = M^* \in \mathcal{B}(\mathcal{H}^{(N)})$ is a bounded self-adjoint operator representing an observable on N qubits, its expectation value in the state $\rho \in \mathcal{DM}(\mathcal{H}^{(N)})$ is given by

$$\langle M \rangle_\rho \;:=\; \mathrm{Tr}(\rho\, M)\,. \tag{III.57}$$

We also transfer the concept of measurement in quantum mechanics to quantum computation: We can access the state ρ only by expectation values (III.57) of observables $M = M^* \in \mathcal{B}(\mathcal{H}^{(N)})$. If a measurement is carried out, the state ρ is changed in such a way that it contains less information than before the measurements. We do not go into detail about this difficult conceptual problem but simply note that we can usually make only one single measurement with a given state. To obtain a reliable result one is bound to use redundancy, e.g., by preparing many identical copies of the initial state, run the quantum computation and make the same measurement many times, and eventually determine the correct result by using their statistics.

IV. States, Observables, and Statistics

In this chapter we turn to how measurements in quantum computing are mathematically defined and statistically interpreted. Throughout we assume $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ to be a complex Hilbert space which is separable and often even finite-dimensional. We recall from (II.47) that quantum states are represented by density matrices $\rho \in \mathcal{DM}(\mathcal{H})$, where

$$\mathcal{DM}(\mathcal{H}) \;=\; \big\{\rho \in \mathcal{L}^1(\mathcal{H}) \;\big|\; \rho = \rho^* \geq 0\,,\; \mathrm{Tr}(\rho) = 1\big\} \;\subseteq\; \mathcal{L}^1(\mathcal{H})\,, \tag{IV.1}$$

and that observables are represented by bounded self-adjoint operators $A \in \mathcal{SA}(\mathcal{H})$, where

$$\mathcal{SA}(\mathcal{H}) \;=\; \big\{A \in \mathcal{B}(\mathcal{H}) \;\big|\; A \;=\; A^*\big\} \;\subseteq\; \mathcal{B}(\mathcal{H})\,. \tag{IV.2}$$

Note that $\mathcal{SA}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H})$ is a real, but not a complex, subspace of $\mathcal{B}(\mathcal{H})$.

IV.1. Observables and Resolutions of the Identity

Given a density matrix $\rho \in \mathcal{DM}(\mathcal{H})$, we interpret the expectation value $\langle A\rangle_\rho := \mathrm{Tr}(\rho A)$ of an observable $A \in \mathcal{SA}(\mathcal{H})$ to be the outcome of the measurement of the physical quantity represented by A, e.g., the position of a particle or its spin. *These measurements are the only access to ρ we have.*

Note that $\rho \in \mathcal{DM}(\mathcal{H})$ is determined by the collection $\big(\langle A\rangle_\rho\big)_{A\in\mathcal{SA}(\mathcal{H})} \in \mathbb{R}^{\mathcal{SA}(\mathcal{H})}$ of the measurements of all observables. For if the measuments of two density matrices $\rho, \hat\rho \in \mathcal{DM}(\mathcal{H})$ all coincide then $\mathrm{Tr}\big[(\rho-\hat\rho)A\big] = \langle A\rangle_\rho - \langle A\rangle_{\hat\rho} = 0$, for all $A \in \mathcal{SA}(\mathcal{H})$ which implies that $\rho - \hat\rho = 0$.

We conclude that observables play the same role for states as random variables do for probability measures. A basic mathematical fact of stochastics is that a probability measure is determined by the collection of expectation values of all its random variables, and we may identify the probability measure with this collection. In practise, our access to observables

is limited and we have to use some other information to determine the state as precisely as possible.

We now suppose we have a set $\mathcal{A}$ of possible outcomes of a measurement. For simplicity, we assume $\mathcal{A}$ to be finite. It is a good idea to think of $\mathcal{A}$ as to divide the scale of a meter into $|\mathcal{A}|$ sectors. To each of these sectors $a \in \mathcal{A}$ we attribute a positive observable $M_a \geq 0$, and we require that these add to one, $\sum_{a\in\mathcal{A}} M_a = \mathbf{1}_{\mathcal{H}}$. The expectation value $p_a := \mathrm{Tr}(\rho\, M_a)$ of M_a in a given state $\rho \in \mathcal{DM}(\mathcal{H})$ then defines a probability distribution on $\mathcal{A}$. The value p_a is the probability that ρ yields the outcome a. We formalize this now.

Definition IV.1. Let $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ be a Hilbert space and $\mathcal{A}$ a finite set.

(i) A family $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ of positive observables $M_a \geq 0$ such that

$$\sum_{a\in\mathcal{A}} M_a \;=\; \mathbf{1}_{\mathcal{H}} \tag{IV.3}$$

is called **resolution of the identity** or **probability operator-valued measure (POVM)**. In this case, $\mathcal{A}$ is the **set of (possible) outcomes $a \in \mathcal{A}$**.

(ii) If $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ is a resolution of the identity and $M_a = M_a^2$ are orthogonal projections for all $a \in \mathcal{A}$, then M is called **orthogonal** or **sharp**.

Remarks and Examples.

- As indicated above, if we are given a state $\rho \in \mathcal{DM}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ and a probability operator-valued measure $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{B}(\mathcal{H})$ then we define $p : \mathcal{A} \to \mathbb{R}_0^+$ by $p_a := \mathrm{Tr}(\rho\, M_a)$ and observe that p is a probability distribution on $\mathcal{A}$.
- If $\mathcal{H}$ is a Hilbert space of dimension $D = \dim(\mathcal{H}) < \infty$ and $\{f_k\}_{k=1}^D \subseteq \mathcal{H}$ is an ONB then $\big\{\, |f_k\rangle\langle f_k| \,\big\}_{k=1}^D \in \mathcal{B}(\mathcal{H})$ is an orthogonal resolution of the identity.

In practise, our access to observables is limited and we have to use some other information to determine the state as precisely as possible. One model instance is given as follows:

Let $\{\rho_a\}_{a\in\mathcal{A}} \in \mathcal{DM}(\mathcal{H})$ be a collection of density matrices on a Hilbert space $\mathcal{H}$, where $\mathcal{A}$ is a finite set, $d := |\mathcal{A}| \in \mathbb{N}$, $d \geq 2$. We are given a random distribution of states $\rho \in \{\rho_a\}_{a\in\mathcal{A}}$, where the probability that $\rho = \rho_a$ equals π_a, i.e., $\sum_{a\in\mathcal{A}} \pi_a = 1$ and $0 < \pi_a < 1$ (we may assume strict inequalities w.l.o.g. to avoid trivial cases). Given an observable $B \in \mathcal{SA}(\mathcal{H})$, its expected (w.r.t. π) expectation value is given by

$$\mathbb{E}_\pi[\langle B\rangle_\rho] \;=\; \sum_{a\in\mathcal{A}} \pi_a \,\langle B\rangle_{\rho_a} \;=\; \sum_{a\in\mathcal{A}} \pi_a \,\mathrm{Tr}(\rho_a B) \;=\; \mathrm{Tr}(\rho_\pi\, B)\,, \tag{IV.4}$$

where $\rho_\pi := \sum_{a\in\mathcal{A}} \pi_a \rho_a \in \mathcal{DM}(\mathcal{H})$ is the average density matrix.

We now suppose to be given a resolution of the identity $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$. We relate the expectation value of M_a to the outcome $a \in \mathcal{A}$. More precisely, we define

$$p(a|b) \;:=\; \mathrm{Tr}(\rho_b M_a) \tag{IV.5}$$

to be the conditional probability of the outcome a under the condition that the state is ρ_b. The name is justified because, for any $b \in \mathcal{A}$,

$$\sum_{a\in\mathcal{A}} p(a|b) \;=\; \sum_{a\in\mathcal{A}} \mathrm{Tr}(\rho_b\, M_a) \;=\; \mathrm{Tr}(\rho_b) \;=\; 1\,. \tag{IV.6}$$

That is, $p(a|b)$ is the prediction that the density matrix is ρ_a while it actually is ρ_b. The goal is now to choose the resolution of the identity $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ such as to maximize the conditional probabilities $p(a|a)$ that predict the density matrix to be ρ_a when this is indeed the case. To aim at a single number to maximize, we weigh these conditional probabilities of correct prediction of ρ_a with the probability of the occurence of ρ_a and define the average probability of making a correct decision

$$\mathcal{P}(M) \;:=\; \sum_{a\in\mathcal{A}} \pi_a\, p(a|a) \;=\; \sum_{a\in\mathcal{A}} \pi_a\, \mathrm{Tr}(\rho_a\, M_a)\,. \tag{IV.7}$$

The above goal can now be formulated as the variational problem to determine a resolution of the identity $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$, such that $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$, where

$$\mathcal{P}_{\max} \;:=\; \sup\Big\{\mathcal{P}(M) \;\Big|\; M \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H}) \Big\} \tag{IV.8}$$

and the system $\mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ of all resolutions of the identity is given by

$$\mathfrak{M}_{\mathcal{A}}(\mathcal{H}) \;:=\; \Big\{M \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}} \;\Big|\; \forall a \in \mathcal{A}:\; M_a \geq 0\,,\quad \sum_{a\in\mathcal{A}} M_a = 1 \Big\}\,. \tag{IV.9}$$

Remarks and Examples. Let $\mathcal{A} = \mathbb{Z}_1^d = \{1, 2, \ldots, d\}$, with $d \in \mathbb{N}$, be a finite set and $\Omega = \mathbb{Z}_1^N = \{1, 2, \ldots, N\}$ be the configuration space such that $\mathcal{H} = \ell^2(\Omega) \cong \mathbb{C}^N$ is the Hilbert space of states. Suppose that we have a collection $\{\rho_a\}_{a\in\mathcal{A}} \subseteq \mathcal{DM}(\mathcal{H})$ of mutually commuting density matrices,

$$\forall\, a, b \in \mathcal{A}: \qquad [\rho_a, \rho_b] \;=\; 0\,. \tag{IV.10}$$

Then there exists an ONB $\{f_k\}_{k\in\Omega} \subseteq \mathcal{H}$ of joint eigenvectors of the ρ_a and nonnegative corresponding eigenvalues $\mu_a(k) \geq 0$ such that $\sum_{k\in\Omega} \mu_a(k) = 1$, for all $a \in \mathcal{A}$, and

$$\forall\, a \in \mathcal{A}: \qquad \rho_a \;=\; \sum_{k\in\Omega} \mu_a(k)\, |f_k\rangle\langle f_k|\,. \tag{IV.11}$$

Given the probability distribution $\pi : \mathcal{A} \to [0, 1]$ for the random choice of $\rho \in \{\rho_a\}_{a\in\mathcal{A}}$, we define $w_a(k) := \pi_a \mu_a(k)$ and

$$\forall\, a \in \mathcal{A}: \qquad W_a \;=\; \sum_{k\in\Omega} w_a(k)\, |f_k\rangle\langle f_k|\,. \tag{IV.12}$$

If $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ is a resolution of the identity, then

$$\begin{aligned}\mathcal{P}(M) \;&=\; \sum_{a\in\mathcal{A}} \mathrm{Tr}(W_a M_a) \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\langle f_k|\,M_a f_k\rangle \\ &\leq \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_{\max}(k)\,\langle f_k|\,M_a f_k\rangle \;=\; \sum_{k\in\Omega} w_{\max}(k)\,, \end{aligned} \tag{IV.13}$$

using $\sum_{a\in\mathcal{A}} M_a = \mathbf{1}_{\mathcal{H}}$ where

$$\forall\, k\in\Omega: \qquad w_{\max}(k) \;:=\; \max_{a\in\mathcal{A}}\{w_a(k)\}\,. \tag{IV.14}$$

Next we construct a resolution $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ of the identity for which $\mathcal{P}(\hat{M}) = \sum_{k\in\Omega} w_{\max}(k)$. To this end we assume to be given a disjoint partition $\{\Omega_a\}_{a\in\mathcal{A}} \subseteq \mathfrak{P}(\Omega)$ of Ω, i.e.,

$$\bigcup_{a\in\mathcal{A}} \Omega_a \;=\; \Omega\,, \qquad \forall\, a,b\in\mathcal{A}\,,\; a\neq b: \quad \Omega_a\cap\Omega_b \;=\; \emptyset\,, \tag{IV.15}$$

and define

$$\forall\, a\in\mathcal{A}: \qquad \hat{M}_a \;=\; \sum_{k\in\Omega} \mathbf{1}[k\in\Omega_a]\,|f_k\rangle\langle f_k|\,. \tag{IV.16}$$

Obviously, $\hat{M}_a \geq 0$. Furthermore, we observe that, due to (IV.15), we have $\sum_{a\in\mathcal{A}} \mathbf{1}[k\in\Omega_a] = 1$, for all $k\in\Omega$, which implies that $\sum_{a\in\mathcal{A}} \hat{M}_a = \mathbf{1}_{\mathcal{H}}$ and hence that $\hat{M}$ is a resolution of the identity, in fact a sharp one.

$$\mathcal{P}(\hat{M}) \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\langle f_k|\,M_a f_k\rangle \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\mathbf{1}[k\in\Omega_a]\,. \tag{IV.17}$$

For $a\in\mathcal{A}$, we now choose

$$\Omega_a \;:=\; \Big\{ k\in\Omega \;\Big|\; w_a(k) = w_{\max}(k)\,,\;\; \forall\, b\in\mathcal{A}\,,\; b<a: \;\; w_b(k) < w_{\max}(k) \Big\}\,, \tag{IV.18}$$

where the condition that $w_b(k) < w_{\max}(k)$, for $b<a$, ensures that a is the smallest element in $\mathcal{A}$ with $w_a(k) = w_{\max}(k)$ and therefore, for each $k\in\Omega$, there is precisely one $a\in\mathcal{A}$ with $\Omega_a \ni k$. It follows that $\{\Omega_a\}_{a\in\mathcal{A}} \subseteq \mathfrak{P}(\Omega)$ is a disjoint partition of Ω in the sense of (IV.15), and thus $\hat{M}$ is an orthogonal resolution of the identity. Moreover,

$$\begin{aligned}\mathcal{P}(\hat{M}) \;&=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\mathbf{1}[k\in\Omega_a] \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_{\max}(k)\,\mathbf{1}[k\in\Omega_a] \\ &=\; \sum_{k\in\Omega} w_{\max}(k)\,\Big(\sum_{a\in\mathcal{A}} \mathbf{1}[k\in\Omega_a]\Big) \;=\; \sum_{k\in\Omega} w_{\max}(k)\,. \end{aligned} \tag{IV.19}$$

It follows that

$$\mathcal{P}(M) \;\leq\; \sum_{k\in\Omega} w_{\max}(k) \;=\; \mathcal{P}(\hat{M}) \;=\; \mathcal{P}_{\max}\,. \tag{IV.20}$$

Finally, we define

$$\Lambda \;:=\; \sum_{k\in\Omega} w_{\max}(k)\,|f_k\rangle\langle f_k|\,. \tag{IV.21}$$

Then obviously $\Lambda \geq W_a$, for all $a \in \mathcal{A}$, and $\mathrm{Tr}(\Lambda) = \sum_{k\in\Omega} w_{\max}(k) = \mathcal{P}_{\max}$. Thus $\widetilde{\mathcal{P}}_{\max} = \mathcal{P}_{\max}$, as asserted in Theorem IV.3 (iii), below.

We conclude that if the density matrices ρ_a mutually commute, then the average probability of making a correct prediction is maximized by an *orthogonal* resolution of the identity.

In the above example, the assumption that the density matrices $\rho_1, \rho_2, \ldots, \rho_d$ are mutually commuting is of key importance for the explicit determination of the optimal resolution $\hat{M}$ of the identity which maximizes the average probability $\mathcal{P}(M)$ of making a correct prediction property.

There is a second special situation in which the optimal resolution of the identity can be determined, namely, for $d = 2$, as is demonstrated in Theorem **??**. Before going into this we recall a few facts from matrix analysis. First we note that if $A, B \in \mathcal{SA}(\mathcal{H})$ with $A, B \geq 0$ then $A^{1/2}BA^{1/2} \geq 0$ and hence

$$\mathrm{Tr}(AB) \;=\; \mathrm{Tr}\big(A^{1/2}BA^{1/2}\big) \;\geq\; 0\,. \tag{IV.22}$$

If furthermore $B \leq C$ then $A^{1/2}(C-B)A^{1/2} \geq 0$ and (IV.22) implies that

$$\mathrm{Tr}(AB) \;=\; \mathrm{Tr}\big(A^{1/2}BA^{1/2}\big) \;\leq\; \mathrm{Tr}\big(A^{1/2}CA^{1/2}\big) \;=\; \mathrm{Tr}(AC)\,. \tag{IV.23}$$

Eqs. (IV.22) can alternatively be shown by using the spectral theorem for $A = \sum_{j=1}^{D} \lambda_j |f_j\rangle\langle f_j|$, where $\lambda_j \geq 0$ are the eigenvalues and f_j the orthonormal eigenvectors of A, respectively.

We also note that the *positive part* $(\cdot)_+ \in C(\mathbb{R}; \mathbb{R}_0^+)$ of a real number is defined by

$$\forall\,\lambda \in \mathbb{R}: \quad (\lambda)_+ \;:=\; \max\{\lambda,\, 0\} \;=\; \lambda\,\mathbf{1}[\lambda > 0] \;=\; \frac{1}{2}|\lambda| + \frac{1}{2}\lambda\,. \tag{IV.24}$$

Theorem IV.2. *Let $U, V \in \mathcal{SA}(\mathcal{H})$ be two positive operators, and define*

$$\widetilde{\mathcal{P}}_{\min} \;:=\; \inf\Big\{\mathrm{Tr}(\Lambda)\;\Big|\;\Lambda \in \mathcal{SA}(\mathcal{H})\,,\; \Lambda \geq U\,,\; \Lambda \geq V\;\Big\}\,. \tag{IV.25}$$

Then

$$\Lambda_0 \;:=\; \frac{1}{2}(U+V) \;+\; \frac{1}{2}|U-V| \;=\; V \;+\; (U-V)_+ \;=\; U \;+\; (V-U)_+ \tag{IV.26}$$

defined by the functional calculus from Definition II.3, is the unique operator $\Lambda_0 \in \mathcal{SA}(\mathcal{H})$ obeying $\Lambda_0 \geq U$ and $\Lambda_0 \geq V$, such that $\widetilde{\mathcal{P}}_{\min} = \mathrm{Tr}(\Lambda_0)$. Moreover,

$$\widetilde{\mathcal{P}}_{\min} \;=\; \mathcal{P}_{\max} \;=\; \sup\Big\{\mathrm{Tr}[UM + V(\mathbf{1}-M)]\;\Big|\;M \in \mathcal{SA}(\mathcal{H})\,,\; 0 \leq M \leq \mathbf{1}\Big\}\,. \tag{IV.27}$$

Proof. Define Λ_0 by (IV.26) and note that $\Lambda_0 = V + (U-V)_+ \geq V$ and $\Lambda_0 = U + (V-U)_+ \geq U$. We introduce the orthogonal projections

$$P_+ \;:=\; \mathbf{1}[U - V \geq 0] \quad \text{and} \quad P_- \;:=\; P_+^\perp \;=\mathbf{1}[U-V<0] \;=\; \mathbf{1}[V-U>0] \tag{IV.28}$$

and oberve that

$$P_+\,\Lambda_0\,P_+ \;=\; P_+\,U\,P_+ \quad \text{and} \quad P_-\,\Lambda_0\,P_- \;=\; P_-\,V\,P_-\,, \tag{IV.29}$$

which implies that

$$\mathcal{F}(U,V) \;\leq\; \mathrm{Tr}(\Lambda_0) \;=\; \mathrm{Tr}(P_+\,U\,P_+) \;+\; \mathrm{Tr}(P_-\,V\,P_-)\,. \tag{IV.30}$$

Next suppose that $\Gamma \in \mathcal{SA}(\mathcal{H})$ obeys $\Gamma \geq U$ and $\Gamma \geq W$ and minizimes $\mathrm{Tr}(\Gamma)$. Then

$$\begin{aligned}\mathcal{F}(U,V) \;&= \mathrm{Tr}(\Gamma) \;=\; \mathrm{Tr}(P_+\,\Gamma\,P_+) \;+\; \mathrm{Tr}(P_-\,\Gamma\,P_-) \\ &= \mathrm{Tr}(\Lambda_0) \;+\; \mathrm{Tr}[P_+\,(\Gamma-U)\,P_+] \;+\; \mathrm{Tr}[P_-\,(\Gamma-V)\,P_-]\,,\end{aligned} \tag{IV.31}$$

which implies that Λ_0 is a minimizer, $\mathcal{F}(U,V) = \mathrm{Tr}(\Lambda_0)$, indeed. Furthermore, it follows from (IV.31) and (IV.29) that

$$P_+\,\Gamma\,P_+ \;=\; P_+\,\Lambda_0\,P_+ \quad \text{and} \quad P_-\,\Gamma\,P_- \;=\; P_-\,\Lambda_0\,P_-\,. \tag{IV.32}$$

Now assume that $\Theta := \Gamma - \Lambda_0 \neq 0$. Then $\Theta = P_+\Theta P_- + P_-\Theta P_+$ and

$$\Gamma - U \;=\; \Lambda_0 - U + \Theta \;=\; (V-U)_+ + \Theta \;=\; P_-(V-U)P_- + P_+\Theta P_- + P_-\Theta P_+\,. \tag{IV.33}$$

Since $\Theta \neq 0$, there exist $\varphi_\pm = P_\pm\varphi_\pm \neq 0$ such that $\langle\varphi_-|\Theta\varphi_+\rangle \neq 0$. For any $\varepsilon > 0$ and $|\sigma| = 1$, we define $\psi_{\varepsilon,\sigma} := \sigma\varphi_+ + \varepsilon\varphi_-$ and observe that, thanks to (IV.33), we have

$$\langle\psi_{\varepsilon,\sigma}|(\Gamma-U)\psi_{\varepsilon,\sigma}\rangle \;=\; 2\varepsilon\,\mathrm{Re}\big\{\sigma\,\langle\varphi_-|\Theta\varphi_+\rangle\big\} \;+\; \varepsilon^2\,\langle\varphi_-|(V-U)\varphi_-\rangle\,. \tag{IV.34}$$

Choosing σ such that $\sigma\,\langle\varphi_-|\Theta\varphi_+\rangle = -|\langle\varphi_-|\Theta\varphi_+\rangle| < 0$, we obtain

$$\langle\psi_{\varepsilon,\sigma}|(\Gamma-U)\psi_{\varepsilon,\sigma}\rangle \;<\; 0\,, \tag{IV.35}$$

for $\varepsilon > 0$ sufficiently small. This contradicts $\Gamma \geq U$. It follows that $\Theta = 0$ and hence the uniqueness of the minimizer Λ_0.

Finally, if $0 \leq M \leq \mathbf{1}$ then

$$\begin{aligned}&\mathrm{Tr}\{UM + V(\mathbf{1}-M)\} \\ &\quad= \mathrm{Tr}\{V\} + \mathrm{Tr}\{(U-V)M\} \;=\; \mathrm{Tr}\{V\} + \mathrm{Tr}\{M^{1/2}(U-V)M^{1/2}\} \\ &\quad\leq \mathrm{Tr}\{V\} + \mathrm{Tr}\{M^{1/2}(U-V)_+M^{1/2}\} \;=\; \mathrm{Tr}\{V\} + \mathrm{Tr}\{(U-V)_+^{1/2}M(U-V)_+^{1/2}\} \\ &\quad\leq \mathrm{Tr}\{V\} + \mathrm{Tr}\{(U-V)_+\} \;=\; \widetilde{\mathcal{P}}_{\min}\,,\end{aligned} \tag{IV.36}$$

which implies that $\mathcal{P}_{\max} \leq \widetilde{\mathcal{P}}_{\min}$. Conversely, if $\hat{M} := \mathbf{1}[U - V \geq 0]$ then

$$\begin{aligned} \mathrm{Tr}\{U\hat{M} + V(\mathbf{1} - \hat{M})\} &= \mathrm{Tr}\{V + (U - V)\hat{M}\} \;=\; \mathrm{Tr}\{V + (U - V)_+\} \\ &= \mathrm{Tr}\{\Lambda_0\} \;=\; \widetilde{\mathcal{P}}_{\min}\,, \end{aligned} \tag{IV.37}$$

hence $\widetilde{\mathcal{P}}_{\min} \leq \mathcal{P}_{\max}$. □

Remarks and Examples. Let $\mathcal{A} = \{0, 1\}$ and again $\Omega = \mathbb{Z}_1^N = \{1, 2, \ldots, N\}$ such that $\mathcal{H} = \ell^2(\Omega) \cong \mathbb{C}^N$ is the Hilbert space of states. Suppose that we are given two density matrices $\rho_0, \rho_1 \in \mathcal{DM}(\mathcal{H})$ that are chosen with probability $\pi_0 \in (0, 1)$ and $\pi_1 = 1 - \pi_0$, respectively. We introduce $W_0 := \pi_0\rho_0 \geq 0$ and $W_1 := \pi_1\rho_1 \geq 0$, as before.

A resolution $M = \{M_0, M_1\} \subseteq \mathcal{SA}(\mathcal{H})$ of the identity is necessarily of the form $M_1 = \mathbf{1} - M_0$ and hence fully determined by the choice of $0 \leq M_0 \leq \mathbf{1}$. Given M_0, and hence M, we observe that

$$\mathcal{P}(M) \;= \mathrm{Tr}[W_0 M_0] \;+\; \mathrm{Tr}[W_1(\mathbf{1} - M_0)] \;=\; \mathrm{Tr}[W_1] \;+\; \mathrm{Tr}[(W_0 - W_1)M_0]\,. \tag{IV.38}$$

Since $W_0 - W_1 \in \mathcal{SA}(\mathcal{H})$, there is an ONB $\{f_k\}_{k\in\Omega} \subseteq \mathcal{H}$ of eigenvectors of $W_0 - W_1$ with corresponding eigenvalues $\lambda_k \in \mathbb{R}$ such that

$$W_0 - W_1 \;=\; \sum_{k\in\Omega} \lambda_k \, |f_k\rangle\langle f_k| \tag{IV.39}$$

and, therefore,

$$\mathrm{Tr}[(W_0 - W_1)M_0] \;=\; \sum_{k\in\Omega} \lambda_k \, \langle f_k| \, M_0 f_k\rangle \;=\; \sum_{k\in\Omega} (\lambda_k)_+\,, \tag{IV.40}$$

using that $\langle f_k|M_0 f_k\rangle \in [0, 1]$, where the *positive part* $(\cdot)_+ : \mathbb{R} \to \mathbb{R}_0^+$ of a real number is defined by

$$\forall\, \lambda \in \mathbb{R}: \quad (\lambda)_+ \;:=\; \max\{\lambda,\, 0\} \;=\; \lambda\, \mathbf{1}[\lambda > 0] \;=\; \frac{1}{2}|\lambda| + \frac{1}{2}\lambda\,. \tag{IV.41}$$

By the functional calculus as in Definition II.3, we have that

$$\mathrm{Tr}[(W_0 - W_1)M_0] \;\leq\; \mathrm{Tr}[(W_0 - W_1)_+]\,, \tag{IV.42}$$

for any $0 \leq M_0 \leq \mathbf{1}$, where

$$(W_0 - W_1)_+ \;=\; \sum_{k\in\Omega} (\lambda_k)_+ \, |f_k\rangle\langle f_k|\,. \tag{IV.43}$$

Again by the functional calculus as in Definition II.3, we define

$$\hat{M}_0 \;:= \mathbf{1}[W_0 - W_1 > 0] \;=\; \sum_{k\in\Omega} \mathbf{1}[\lambda_k > 0] \, |f_k\rangle\langle f_k|\,. \tag{IV.44}$$

Then $0 \leq \hat{M}_0 \leq \mathbf{1}$ and

$$\mathrm{Tr}[(W_0 - W_1)\hat{M}_0] \;=\; \mathrm{Tr}[(W_0 - W_1)_+]\,, \tag{IV.45}$$

which implies that $\hat{M} = \{\hat{M}_0, \mathbf{1} - \hat{M}_0\} \subseteq \mathcal{SA}(\mathcal{H})$ is a (sharp) resolution of the identity which maximizes the average probability of making a correct prediction,

$$\begin{aligned}
\mathcal{P}(\hat{M}) \;&= \mathrm{Tr}[W_1 + (W_0 - W_1)_+] \;=\; \mathrm{Tr}\big(W_1 + \tfrac{1}{2}|W_0 - W_1| + \tfrac{1}{2}(W_0 - W_1)\big) \\
&= \frac{1}{2}\mathrm{Tr}\big(W_0 + W_1\big) \;+\; \frac{1}{2}\mathrm{Tr}\big(|W_0 - W_1|\big) \\
&= \frac{1}{2}\big[\pi_0\,\mathrm{Tr}(\rho_0) \;+\; \pi_1\,\mathrm{Tr}(\rho_1)\big] \;+\; \frac{1}{2}\mathrm{Tr}\big(|\pi_0\rho_0 - \pi_1\rho_1|\big) \\
&= \frac{1}{2} \;+\; \frac{1}{2}\|\pi_0\rho_0 - \pi_1\rho_1\|_{\mathcal{L}^1(\mathcal{H})}\,.
\end{aligned} \tag{IV.46}$$

Now, we generalize Theorem IV.2 from $d = 2$ to general $d \in \mathbb{N}$. In this general case, the characterization of the optimal resolution of identity is, however, somewhat implicit.

Theorem IV.3. *Let $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ be a Hilbert space and $\mathcal{A}$ a finite set with at least two elements. Further suppose that $\{\rho_a\}_{a\in\mathcal{A}} \in \mathcal{DM}(\mathcal{H})$ is a finite collection of density matrices on $\mathcal{H}$ and $\pi : \mathcal{A} \to (0,1)$ is a probability distribution, such that π_b is the probability that a random density matrix $\rho \in \{\rho_a\}_{a\in\mathcal{A}}$ assumes the value ρ_b and define $W_a := \pi_a\rho_a$, for all $a \in \mathcal{A}$, and*

$$\widetilde{\mathcal{P}}_{\min} \;:=\; \inf\Big\{\mathrm{Tr}(\Lambda)\;\Big|\;\forall\, a \in \mathcal{A}:\; \Lambda \geq W_a\Big\}\,. \tag{IV.47}$$

(i) If $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ is a resolution of the identity with maximal average probability of making a correct decision, $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$. Then there exists $\Lambda = \Lambda^* \in \mathcal{B}(\mathcal{H})$ such that

$$\forall\, a \in \mathcal{A}: \qquad \big(\Lambda - W_a\big)\hat{M}_a \;=\; 0\,, \tag{IV.48}$$

$$\forall\, a \in \mathcal{A}: \qquad \Lambda \;\geq\; W_a\,. \tag{IV.49}$$

(ii) Conversely, if a resolution of the identity $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ and an operator $\Lambda = \Lambda^* \in \mathcal{B}(\mathcal{H})$ fulfill (IV.48) *and* (IV.49)*, then $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$.*

(iii) There is a unique $\widehat{\Lambda} \in \mathcal{SA}(\mathcal{H})$ obeying $\widehat{\Lambda} \geq W_a$, for all $a \in \mathcal{A}$, such that

$$\mathcal{P}_{\max} \;=\; \widetilde{\mathcal{P}}_{\min} \;=\; \mathrm{Tr}(\widehat{\Lambda})\,. \tag{IV.50}$$

Proof. We first introduce

$$\mathfrak{L}(W) \;:=\Big\{\Lambda \in \mathcal{SA}(\mathcal{H})\;\Big|\;\forall\, a \in \mathcal{A}:\quad \Lambda \geq W_a\Big\} \tag{IV.51}$$

and define

$$\begin{aligned}\mathcal{F}(M,\Lambda) \;&:=\; \sum_{a\in\mathcal{A}} \mathrm{Tr}\big[W_a\, M_a\big] \;-\; \mathrm{Tr}\Big[\Lambda\Big(\sum_{a\in\mathcal{A}} M_a - \mathbf{1}\Big)\Big] \\ &=\; \mathrm{Tr}[\Lambda] \;-\; \sum_{a\in\mathcal{A}} \mathrm{Tr}\big[(\Lambda - W_a)\, M_a\big]\,,\end{aligned} \tag{IV.52}$$

for $M \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}}$ and $\Lambda \in \mathcal{SA}(\mathcal{H})$. Note that, for all $\Lambda \in \mathfrak{L}(W)$,

$$\widetilde{\mathcal{P}}(\Lambda) \;:=\; \sup_{\chi\in\mathcal{SA}(\mathcal{H})^{\mathcal{A}}} \mathcal{F}(\chi^2,\Lambda) \;=\; \max_{\chi\in\mathcal{SA}(\mathcal{H})^{\mathcal{A}}} \mathcal{F}(\chi^2,\Lambda) \;=\; \mathcal{F}(0,\Lambda) \;=\; \mathrm{Tr}[\Lambda]\,, \tag{IV.53}$$

writing $(\chi^2)_a := \chi_a^2$. Conversely, for all $\Lambda \in \mathcal{SA}(\mathcal{H}) \setminus \mathfrak{L}(W)$, there is an $\tilde{a} \in \mathcal{A}$ and $\varphi \in \mathcal{H} \setminus \{0\}$ such that $W_{\tilde{a}} - \Lambda \geq |\varphi\rangle\langle\varphi|$. Then, choosing $\chi_a = 0$ except $\chi_{\tilde{a}}$, which is chosen as $\chi_{\tilde{a}} := \mu|\varphi\rangle\langle\varphi|$, we obtain that

$$\widetilde{\mathcal{P}}(\Lambda) \;\geq\; \sup_{\mu\in\mathbb{R}} \big\{\mu^2\, \|\varphi\|^4\big\} \;=\; \infty\,. \tag{IV.54}$$

So, if we define $\widetilde{\mathcal{P}} : \mathcal{SA}(\mathcal{H}) \to \mathbb{R} \cup \{\infty\}$, with $\infty > x$, for any $x \in \mathbb{R}$, it follows that

$$\widetilde{\mathcal{P}}_{\min} \;=\; \min_{\Lambda\in\mathcal{SA}(\mathcal{H})} \{\widetilde{\mathcal{P}}(\Lambda)\} \;=\; \min_{\Lambda\in\mathfrak{L}(W)} \{\widetilde{\mathcal{P}}(\Lambda)\}\,. \tag{IV.55}$$

(i): Let $\hat{\chi} \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}}$ be such that $\hat{M} = \hat{\chi}^2 \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ is a maximizer of $\mathcal{P}$, i.e.,

$$\begin{aligned}\mathcal{P}(\hat{\chi}^2) \;&=\; \max_{M\in\mathfrak{M}_{\mathcal{A}}(\mathcal{H})} \{\mathcal{P}(M)\} \\ &=\; \max\left\{\mathcal{P}(M) \;\middle|\; M = (\chi_a^2)_{a\in\mathcal{A}}\,,\; \forall\, a\in\mathcal{A} : \chi_a \in \mathcal{SA}(\mathcal{H})\,,\; \sum_{a\in\mathcal{A}} \chi_a^2 = \mathbf{1}\right\}.\end{aligned} \tag{IV.56}$$

The theory of extrema of multivariate functions under constraints implies that there is a family of Lagrange mutlipliers which we can arrange as real and imaginary parts of the matrix entries of a self-adjoint matrix $\Lambda \in \mathcal{SA}(\mathcal{H})$ such that $\mathcal{SA}(\mathcal{H})^{\mathcal{A}} \ni \chi \mapsto \mathcal{F}(\chi^2,\Lambda) \in \mathbb{R}$ is stationary at $\hat{\chi}$. Moreover, by results from convex analysis we may even assume that $\hat{\chi}$ is a maximizer of $\mathcal{SA}(\mathcal{H})^{\mathcal{A}} \ni \chi \mapsto \mathcal{F}(\chi^2,\Lambda) \in \mathbb{R}$. Then, for all $\varepsilon > 0$ and all $\theta = (\theta_a)_{a\in\mathcal{A}} \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}}$,

$$\begin{aligned}0 \;&\leq \mathcal{F}\big[\hat{\chi}^2,\Lambda\big] \;-\; \mathcal{F}\big[(\hat{\chi}+\varepsilon\theta)^2,\Lambda\big] \\ &= \varepsilon \sum_{a\in\mathcal{A}} \mathrm{Tr}\Big\{\big[(\Lambda - W_a)\hat{\chi}_a + \hat{\chi}_a(\Lambda - W_a)\big]\theta_a\Big\} \;+\; \varepsilon^2 \sum_{a\in\mathcal{A}} \mathrm{Tr}\big\{\theta_a(\Lambda - W_a)\theta_a\big\}\,.\end{aligned} \tag{IV.57}$$

Since θ can be chosen arbitrarily, taking the limit $\varepsilon \to$ yields

$$\forall\, a \in \mathcal{A}: \qquad (\Lambda - W_a)\hat{\chi}_a + \hat{\chi}_a(\Lambda - W_a) \;=\; 0\,. \tag{IV.58}$$

From this we obtain for all $a \in \mathcal{A}$ that $(\Lambda - W_a)\hat{\chi}_a = -\hat{\chi}_a(\Lambda - W_a)$, which implies $(\Lambda - W_a)^2\hat{\chi}_a = \hat{\chi}_a(\Lambda - W_a)^2$ and, hence, for all $r > 0$ that

$$\left[(\Lambda - W_a)^2 + r^2\right]^{-1} \hat{\chi}_a \;=\; \hat{\chi}_a \left[(\Lambda - W_a)^2 + r^2\right]^{-1}. \tag{IV.59}$$

Using $\sqrt{A} = \frac{A}{\pi}\int_0^\infty (A + r^2)^{-1}\, dr$, we obtain

$$|\Lambda - W_a|\,\hat{\chi}_a \;=\; \sqrt{(\Lambda - W_a)^2}\,\hat{\chi}_a \;=\; \hat{\chi}_a\,\sqrt{(\Lambda - W_a)^2} \;=\; \hat{\chi}_a\,|\Lambda - W_a|\,, \tag{IV.60}$$

and finally

$$\begin{aligned}(\Lambda - W_a)_\pm\,\hat{\chi}_a \;&= \tfrac{1}{2}|\Lambda - W_a|\,\hat{\chi}_a \;\pm\; \tfrac{1}{2}(\Lambda - W_a)\,\hat{\chi}_a \\ &= \hat{\chi}_a\,\tfrac{1}{2}|\Lambda - W_a| \;\mp\; \tfrac{1}{2}\hat{\chi}_a\,(\Lambda - W_a) \;=\; \hat{\chi}_a\,(\Lambda - W_a)_\mp\,.\end{aligned} \tag{IV.61}$$

On the other hand, inserting (IV.58) into (IV.57), we further obtain that

$$0 \;\leq\; \varepsilon^2 \sum_{a\in\mathcal{A}} \mathrm{Tr}\big\{\theta_a(\Lambda - W_a)\theta_a\big\}\,. \tag{IV.62}$$

Since $\theta_a \in \mathcal{SA}(\mathcal{H})$ is arbitrary, this implies that $\Lambda \geq W_a$, for all $a \in \mathcal{A}$, i.e., that

$$\Lambda \;\in\; \mathfrak{L}(W)\,. \tag{IV.63}$$

Moreover, $\Lambda \geq W_a$ is equivalent to $(\Lambda - W_a)_- = 0$, which together with (IV.61) yields

$$\forall\, a \in \mathcal{A}: \qquad (\Lambda - W_a)\,M_a \;=\; (\Lambda - W_a)_+\,M_a \;=\; \hat{\chi}_a\,(\Lambda - W_a)_-\,\hat{\chi}_a \;=\; 0\,. \tag{IV.64}$$

This completes the proof of *(i)*.

(ii): Let $\Lambda \in \mathfrak{L}(W)$ and $M = \{M_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ be a resolution of the identity. Then

$$\mathcal{P}(M) \;=\; \sum_{a\in\mathcal{A}} \mathrm{Tr}[W_a\,M_a] \;=\; \mathrm{Tr}(\Lambda) \;-\; \sum_{a\in\mathcal{A}} \mathrm{Tr}[(\Lambda - W_a)\,M_a] \;\leq\; \mathrm{Tr}(\Lambda) \;=\; \widetilde{\mathcal{P}}(\Lambda)\,. \tag{IV.65}$$

It follows that

$$\mathcal{P}_{\max} \;=\; \max_{M\in\mathfrak{M}_{\mathcal{A}}(\mathcal{H})} \mathcal{P}(\hat{M}) \;\leq\; \min_{\Lambda\in\mathfrak{L}(W)} \widetilde{\mathcal{P}}(\Lambda) \;=\; \widetilde{\mathcal{P}}_{\min}\,. \tag{IV.66}$$

If $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ additionally fulfills (IV.48) then

$$\mathcal{P}(\hat{M}) \;=\; \mathrm{Tr}(\Lambda) \;-\; \sum_{a\in\mathcal{A}} \mathrm{Tr}[(\Lambda - W_a)\,M_a] \;=\; \mathrm{Tr}(\Lambda) \;=\; \widetilde{\mathcal{P}}(\Lambda)\,. \tag{IV.67}$$

and hence $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$ and $\widetilde{\mathcal{P}}(\Lambda) = \widetilde{\mathcal{P}}_{\min}$.

(iii): is obvious from what has been proven so far except the uniqueness of the minimizer $\widehat{\Lambda} \in \mathfrak{L}(W)$ of $\widetilde{\mathcal{P}}_(\Lambda)$, which we omit here. □

Remarks and Examples. We exemplify Theorem IV.3 on a single qubit, i.e., $\mathcal{H} = \mathbb{C}^2$ and we assume that $\mathcal{A} = \{1,2,3\}$. We are given $\pi_1, \pi_2, \pi_3 \in (0,1)$ such that $\pi_1 + \pi_2 + \pi_3 = 1$ and $\vec{v}_1, \vec{v}_2, \vec{v}_3 \in \overline{B(0,1)} \subseteq \mathbb{R}^3$ that determine three density matrices $\rho_1, \rho_2, \rho_3 \in \mathcal{DM}(\mathcal{H})$ and operators $W_a = \pi_a \rho_a$ by

$$\rho_a \;=\; \frac{1}{2}\Big(\mathbf{1} \,+\, \vec{v}_a \cdot \vec{\sigma}\Big)\,, \qquad W_a \;=\; \frac{\pi_a}{2}\Big(\mathbf{1} \,+\, \vec{v}_a \cdot \vec{\sigma}\Big)\,. \tag{IV.68}$$

We assume that $\Lambda \in \mathcal{SA}(\mathcal{H})$ is positive and hence determined by $r > 0$ and $\vec{z} \in \overline{B(0,r)}$ as

$$\Lambda \;=\; \frac{r}{2}\,\mathbf{1} \,+\, \vec{z} \cdot \vec{\sigma}\,. \tag{IV.69}$$

We observe that, for $a \in \mathcal{A}$,

$$\Lambda - W_a \;=\; \frac{r - \pi_a}{2}\,\mathbf{1} \,+\, \left(\frac{\vec{z} - \pi_a \vec{v}_a}{2}\right) \cdot \vec{\sigma}\,, \tag{IV.70}$$

so, if $\Lambda - W_a \geq 0$ then necessarily $r > \pi_a$ and $r - \pi_a \geq |\vec{z} - \pi_a \vec{v}_a|$. The latter condition is equivalent to

$$(r - \pi_a)^2 \;\geq\; |\vec{z}|^2 + \pi_a^2 |\vec{v}_a|^2 - 2\pi_a \vec{z} \cdot \vec{v}_a\,. \tag{IV.71}$$

Now we concretely choose $\pi_1 = \pi_2 = \pi_3 = \frac{1}{3}$ and

$$\vec{v}_a \;:=\; \begin{pmatrix} \sin(\frac{4\pi}{3}a) \\ 0 \\ \cos(\frac{4\pi}{3}a) \end{pmatrix}\,, \;\text{i.e.,}\; \vec{v}_1 \;:=\; \begin{pmatrix} \frac{1}{2}\sqrt{3} \\ 0 \\ -\frac{1}{2} \end{pmatrix}\,, \;\vec{v}_2 \;:=\; \begin{pmatrix} -\frac{1}{2}\sqrt{3} \\ 0 \\ -\frac{1}{2} \end{pmatrix}\,, \;\vec{v}_3 \;:=\; \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\,, \tag{IV.72}$$

which implies that $|\vec{v}_1| = |\vec{v}_2| = |\vec{v}_3| = 1$ and simplifies the three conditions (IV.71) to a single one,

$$\big(r - \tfrac{1}{3}\big)^2 \;\geq\; \tfrac{1}{9} + \max_{a \in \mathcal{A}} \Big\{ |\vec{z}|^2 - \tfrac{2}{3}\vec{z} \cdot \vec{v}_a \Big\}\,. \tag{IV.73}$$

Writing $\vec{z} = (z_1, z_2, z_3)^t$, we observe that

$$\begin{aligned}
&\max_{a \in \mathcal{A}} \Big\{ |\vec{z}|^2 - \tfrac{2}{3}\vec{z} \cdot \vec{v}_a \Big\} \\
&\quad= \max \Big\{ z_1^2 + z_2^2 + z_3^2 - \tfrac{1}{\sqrt{3}} z_1 + \tfrac{1}{3} z_3\,,\;\; z_1^2 + z_2^2 + z_3^2 + \tfrac{1}{\sqrt{3}} z_1 + \tfrac{1}{3} z_3\,, \\
&\qquad\qquad z_1^2 + z_2^2 + z_3^2 - \tfrac{2}{3} z_3 \Big\} \\
&\quad= \max \Big\{ z_1^2 + z_2^2 + z_3^2 + \tfrac{1}{\sqrt{3}} |z_1| + \tfrac{1}{3} z_3\,,\;\; z_1^2 + z_2^2 + z_3^2 - \tfrac{2}{3} z_3 \Big\} \\
&\quad\geq z_1^2 + z_2^2 + z_3^2 + \tfrac{1}{3}|z_3|\,.
\end{aligned} \tag{IV.74}$$

This, however, implies that $\vec{z} = \vec{0}$ is the best possible choice for $\vec{z}$ because it imposes the least constraint on r in (IV.73). In turn, if $\vec{z} = \vec{0}$ then the smallest $r > \frac{1}{3}$ fulfilling (IV.73) is $r = \frac{2}{3}$. As $\mathrm{Tr}(\Lambda) = r$, it follows that the optimal choice for Λ is

$$\Lambda \;=\; \frac{1}{3}\,\mathbf{1} \qquad \text{and} \qquad \widetilde{\mathcal{P}}_{\min} \;=\; \mathrm{Tr}(\Lambda) \;=\; \frac{2}{3}\,. \tag{IV.75}$$

V. Sharp Resolutions of the Identity, Purification, and Entanglement

V.1. Naimark's Dilation

Our first topic is resolutions of the identity. If $M = (M_a)_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ is a resolution of the identity on a Hilbert space $\mathcal{H}$ then the operators M_a are positive and add to the identity on $\mathcal{H}$. *Sharp* resolution of the identity posses the addtional property, that each member M_a is an orthogonal projection, $M_a = M_a^2$. Naimark's theorem below states that, conversely, any resolution of the identity can be realized as a sharp one, provided the Hilbert space $\mathcal{H}$ is embedded in a larger Hilbert space $\mathcal{K}$ by a suitable isometry $V \in \mathcal{B}(\mathcal{H};\mathcal{K})$.

To formulate the precise statement, we recall that the adjoint $V^* \in \mathcal{B}(\mathcal{K};\mathcal{H})$ of $V \in \mathcal{B}(\mathcal{H};\mathcal{K})$ is the unique operator obeying

$$\forall\, \varphi \in \mathcal{K},\ \psi \in \mathcal{H}: \qquad \langle V^*\varphi \,|\, \psi\rangle_{\mathcal{H}} \;=\; \langle \varphi \,|\, V\psi\rangle_{\mathcal{K}} \tag{V.1}$$

and that a linear operator V from $\mathcal{H}$ to $\mathcal{K}$ is an **isometry**, if $V^*V = \mathbf{1}_{\mathcal{H}}$, i.e.,

$$\forall\, \psi, \psi' \in \mathcal{H}: \qquad \langle V\psi \,|\, V\psi\rangle_{\mathcal{K}} \;=\; \langle \psi \,|\, \psi\rangle_{\mathcal{H}}\,, \tag{V.2}$$

which, by polarization, is equivalent to

$$\forall\, \psi \in \mathcal{H}: \qquad \|V\psi\|_{\mathcal{K}} \;=\; \|\psi\|_{\mathcal{H}}\,. \tag{V.3}$$

Note that $U \in \mathcal{B}(\mathcal{H};\mathcal{K})$ is unitary if, and only if, both $U \in \mathcal{B}(\mathcal{H};\mathcal{K})$ and $U^* \in \mathcal{B}(\mathcal{K};\mathcal{H})$ are isometries. If $\mathcal{H}$ and $\mathcal{K}$ are finite dimensional and $\dim(\mathcal{H}) < \dim(\mathcal{K})$, then no unitary operators from $\mathcal{H} \to \mathcal{K}$ exist, but isometries do.

Theorem V.1 (Naimark)**.** *Let $\mathcal{H}$ be a Hilbert space, $\mathcal{A}$ a finite set of measurement outcomes, $m := |\mathcal{A}| \in \mathbb{N}$, and a resolution $M = (M_a)_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ of the identity on $\mathcal{H}$. Then there exists a Hilbert space $\mathcal{K}$ of dimension $\dim(\mathcal{K}) \le m\cdot\dim(\mathcal{H})$, an isometry $V \in \mathcal{B}(\mathcal{H};\mathcal{K})$, and a sharp resolution $E = (E_a)_{a\in\mathcal{A}} = (E_a^2)_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{K})$ of the identity on $\mathcal{K}$ such that*

$$\forall\, a \in \mathcal{A}: \qquad M_a \;=\; V^*\, E_a\, V\,. \tag{V.4}$$

Proof. We may w.l.o.g. assume that $\mathcal{A} = \mathbb{Z}_1^m$. We first note that $\big(\mathcal{H}^m\,,\langle\cdot|\cdot\rangle_{\mathcal{H}^m}\big)$ is a Hilbert space of dimension $\dim(\mathcal{H}^m) = m\cdot\dim(\mathcal{H})$ with the scalar product

$$\left\langle \begin{pmatrix}\varphi_1\\ \vdots\\ \varphi_m\end{pmatrix} \,\middle|\, \begin{pmatrix}\psi_1\\ \vdots\\ \psi_m\end{pmatrix} \right\rangle_{\mathcal{H}^m} \;=\; \langle\varphi_1|\psi_1\rangle + \ldots + \langle\varphi_m|\psi_m\rangle\,. \tag{V.5}$$

We define block diagonal linear operators $\underline{M}, \underline{\widetilde{E}}_1, \ldots, \underline{\widetilde{E}}_m \in \mathcal{B}(\mathcal{H}^m)$ on the complex Hilbert space $\mathcal{H}^m$ by

$$\underline{M} \;=\; \begin{pmatrix} M_1 & 0 & \cdots & 0\\ 0 & M_2 & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & M_m\end{pmatrix} \tag{V.6}$$

and

$$\underline{\widetilde{E}}_1 \;=\; \begin{pmatrix} \mathbf{1}_{\mathcal{H}} & 0 & \cdots & 0\\ 0 & 0 & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & 0\end{pmatrix}, \ldots, \underline{\widetilde{E}}_m \;=\; \begin{pmatrix} 0 & 0 & \cdots & 0\\ 0 & 0 & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & \mathbf{1}_{\mathcal{H}}\end{pmatrix}. \tag{V.7}$$

Equivalently,

$$\underline{M}\big[(\psi_a)_{a=1}^m\big] \;:=\; (M_a\psi_a)_{a=1}^m \quad\text{and}\quad \underline{\widetilde{E}}_b\big[(\psi_a)_{a=1}^m\big] \;:=\; (\delta_{b,a}\psi_a)_{a=1}^m\,, \tag{V.8}$$

for all $b\in\mathbb{Z}_1^m$. Clearly, $\underline{\widetilde{E}}_b = \underline{\widetilde{E}}_b^* = \underline{\widetilde{E}}_b^2$ and $\sum_{b=1}^m \underline{\widetilde{E}}_b = \mathbf{1}_{\mathcal{H}^m}$. In other words, $\underline{\widetilde{E}} = (\underline{\widetilde{E}}_b)_{b=1}^m$ is a sharp resolution of the identity. Furthermore, we equip $\mathcal{H}^m$ with the quadratic form

$$\Big\langle (\varphi_a)_{a=1}^m \,\Big|\, (\psi_a)_{a=1}^m \Big\rangle_{\underline{M}} \;:=\; \Big\langle (\varphi_a)_{a=1}^m \,\Big|\, \underline{M}\,(\psi_a)_{a=1}^m \Big\rangle_{\mathcal{H}^m} \;=\; \sum_{a=1}^m \langle\varphi_a \mid M_a\psi_a\rangle_{\mathcal{H}}\,. \tag{V.9}$$

We observe that $\langle\cdot|\cdot\rangle_{\underline{M}}$ is not positive definite, but only positive semidefinite, on $\mathcal{H}^m$. That is,

$$\mathcal{N}(\underline{M}) \;:=\; \Big\{\Psi\in\mathcal{H}^m \,\Big|\, \langle\Psi|\Psi\rangle_{\underline{M}} \;=\; 0\Big\} \;\subseteq\; \mathcal{H}^m \tag{V.10}$$

may possibly be nontrivial, $\mathcal{N}(\underline{M}) \neq \{\underline{0}\}$. Introducing

$$\mathrm{Ker}(\underline{M}) \;=\; \big\{\Psi\in\mathcal{H}^m \,\big|\, \underline{M}\Psi = 0\big\} \;=\; \big\{(\psi_a)_{a=1}^m\in\mathcal{H}^m \,\big|\, \forall\, a\in\mathcal{A}:\;\; M_a\psi_a = 0\big\}\,, \tag{V.11}$$

we observe that $\Psi\in\mathrm{Ker}(\underline{M})$ implies that $\langle\Psi|\Psi\rangle_{\underline{M}} = \langle\Psi|\underline{M}\Psi\rangle_{\mathcal{H}^m} = \langle\Psi|\underline{0}\rangle_{\mathcal{H}^m} = 0$ and hence $\Psi\in\mathcal{N}(\underline{M})$. Conversely, if $\Psi = (\psi_a)_{a=1}^m \in \mathcal{N}(\underline{M})$ then

$$0 \;=\; \langle\Psi|\underline{M}\Psi\rangle_{\mathcal{H}^m} \;=\; \sum_{a=1}^m \langle\psi_a|M_a\psi_a\rangle_{\mathcal{H}} \;=\; \sum_{a=1}^m \big\|\sqrt{M_a}\,\psi_a\big\|_{\mathcal{H}}^2\,, \tag{V.12}$$

hence $\sqrt{M_a}\psi_a = 0$ and also $M_a\psi_a = \sqrt{M_a}\,[\sqrt{M_a}\,\psi_a] = 0$, for all $a \in \mathbb{Z}_1^m$, which implies that $\Psi \in \mathrm{Ker}(\underline{M})$. It follows that

$$\mathcal{N}(\underline{M}) \;=\; \mathrm{Ker}(\underline{M})\,. \tag{V.13}$$

Now, let $\Psi = (\psi_a)_{a=1}^m \in \mathrm{Ker}(\underline{M})$, i.e., $M_a\psi_a = 0$, for all $a \in \mathbb{Z}_1^m$. So, if $b \in \mathbb{Z}_1^m$ then $\underline{\widetilde{E}}_b\Psi = (\delta_{b,a}\psi_a)_{a=1}^m$ and $\underline{M}\,\underline{\widetilde{E}}_b\Psi = (\delta_{b,a}M_a\psi_a)_{a=1}^m = \underline{0}$. It follows that $\underline{\widetilde{E}}_1, \underline{\widetilde{E}}_2, \ldots, \underline{\widetilde{E}}_m$ all leave $\mathrm{Ker}(\underline{M})$ invariant.

We define $\underline{P} \in \mathcal{B}(\mathcal{H}^m)$ to be the orthogonal projection onto the orthogonal complement

$$\mathcal{K} \;:=\; \mathrm{Ran}[\underline{P}] \;=\; \big[\mathrm{Ker}(\underline{M})\big]^{\perp} \;\subseteq\; \mathcal{H}^m \tag{V.14}$$

of $\mathrm{Ker}(\underline{M}) \subseteq \mathcal{H}$. If $\Psi \in \mathcal{K} \setminus \{\underline{0}\}$ then $\langle\!\langle \Psi|\Psi\rangle\!\rangle > 0$. Consequently $\big(\mathcal{K},\, \langle\!\langle\cdot|\cdot\rangle\!\rangle\big)$ is a complex Hilbert space. Moreover,

$$\underline{M} \;=\; \underline{P}\,\underline{M} \;=\; \underline{M}\,\underline{P} \;=\; \underline{P}\,\underline{M}\,\underline{P} \quad\text{and}\quad \underline{\widetilde{E}}_b\,\underline{M} \;=\; \underline{M}\,\underline{\widetilde{E}}_b \;=\; \underline{\widetilde{E}}_b\,\underline{M}\,\underline{\widetilde{E}}_b\,, \tag{V.15}$$

for all $b \in \mathbb{Z}_1^m$.

Next, we define $J \in \mathcal{B}(\mathcal{H}; \mathcal{H}^m)$ by $(J\psi)_a := \psi$, i.e.,

$$J\psi \;:=\; \begin{pmatrix} \psi \\ \vdots \\ \psi \end{pmatrix}\,, \quad \text{and then} \quad V \;:=\; \underline{P}\,J \;\in\; \mathcal{B}(\mathcal{H}; \mathcal{K})\,. \tag{V.16}$$

For $\psi \in \mathcal{H}$, we observe that,

$$\begin{aligned} \langle\!\langle V\psi|\, V\psi\rangle\!\rangle \;&= \big\langle (\psi)_{a=1}^m \,\big|\, \underline{P}\,\underline{M}\,\underline{P}(\psi)_{a=1}^m \big\rangle_{\mathcal{H}^m} \;=\; \big\langle (\psi)_{a=1}^m \,\big|\, \underline{M}(\psi)_{a=1}^m \big\rangle_{\mathcal{H}^m} \\ &= \sum_{a=1}^m \langle \psi \,|\, M_a\psi\rangle_{\mathcal{H}} \;=\; \langle\psi|\psi\rangle_{\mathcal{H}}\,, \end{aligned} \tag{V.17}$$

thanks to (V.15) and the fact that M is a resolution of the identity. Eq. (V.17) proves that $V \in \mathcal{B}(\mathcal{H}; \mathcal{K})$ is an isometry.

Moreover, defining $E_b := \underline{P\widetilde{E}_b P} \in \mathcal{B}(\mathcal{K})$ and using (V.15), we obtain for all $\varphi, psi \in \mathcal{H}$ and all $b \in \mathbb{Z}_1^m$ that

$$\begin{aligned} \langle\!\langle V\varphi|\, E_b\, V\psi\rangle\!\rangle \;&= \big\langle (\varphi)_{a=1}^m \,\big|\, \underline{P}\,\underline{M}\,\underline{P}\,\underline{\widetilde{E}}_b\,\underline{P}(\psi)_{a=1}^m \big\rangle_{\mathcal{H}^m} \;=\; \big\langle (\varphi)_{a=1}^m \,\big|\, \underline{M}\,(\delta_{b,a}\psi)_{a=1}^m \big\rangle_{\mathcal{H}^m} \\ &= \big\langle (\varphi)_{a=1}^m \,\big|\, (\delta_{b,a}\, M_b\psi)_{a=1}^m \big\rangle_{\mathcal{H}^m} \;=\; \langle\psi|M_b\psi\rangle_{\mathcal{H}}\,, \end{aligned} \tag{V.18}$$

which implies

$$\forall\, a \in \mathbb{Z}_1^m : \qquad M_a \;=\; V^*\, E_a\, V\,. \tag{V.19}$$

Finally, $\sum_{a=1}^m E_a = \underline{P}\sum_{a=1}^m \underline{\widetilde{E}}_a = \underline{P} = \mathbf{1}_{\mathcal{K}}$, and

$$E_a^2 \;=\; \underline{P\widetilde{E}_a^{\,2}P} \;=\; \underline{P\widetilde{E}_a P} \;=\; E_a \;=\; E_a^*\,, \tag{V.20}$$

for all $a \in \mathbb{Z}_1^m$, so $E = (E_a)_{a\in\mathbb{Z}_1^m} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{K})$ is an orthogonal resolution of the identity. □

V.2. Purification

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces and $\mathcal{H}_{12} := \mathcal{H}_1 \otimes \mathcal{H}_2$ their tensor product. Given a normalized vector $\Psi_{12} \in \mathcal{H}_{12}$, we observe that $\rho_{12} = |\Psi_{12}\rangle\langle\Psi_{12}| \in \mathcal{DM}(\mathcal{H}_{12})$ is a pure density matrix, i.e., an orthogonal projection of rank one.

We have seen in previous chapter that taking the partial trace does not preserve this property, and the density matrices $\rho_1 = \mathrm{Tr}_2[\rho_{12}] \in \mathcal{DM}(\mathcal{H}_1)$ and $\rho_2 = \mathrm{Tr}_1[\rho_{12}] \in \mathcal{DM}(\mathcal{H}_2)$ are not pure, in general. The question, which conditions on ρ_1 and ρ_2 necessarily hold in case that these derive from a pure state and which are sufficient to guarantee this comes up naturally.

In preparation for an answer we recall that, given a complex vector space V, its *dual* $V^* := \mathcal{B}(V;\mathbb{C})$ is the complex vector space of bounded linear maps from V to $\mathbb{C}$. A basic fact from linear algebra is that $(\mathbb{C}^d)^*$ can be naturally identified with $\mathbb{C}^d$.

Another case in which the dual can naturally be identified with the vector space itself is the one of Hilbert spaces: If $\mathcal{H}$ is a complex Hilbert space then, according to the *Riesz representation theorem*,

$$\mathcal{I} : \mathcal{H} \to \mathcal{H}^*, \quad \psi \mapsto \langle\psi|\cdot\rangle \tag{V.21}$$

is an antilinear bijection, which in physics is usually denoted as $\mathcal{I}\big(|\psi\rangle\big) = \langle\psi|$. The antilinearity of $\mathcal{I}$ results from the antilinearity of the scalar product in its left entry: Since $\langle\varphi + \alpha\psi|\, x\rangle = \langle\varphi|\, x\rangle + \overline{\alpha}\langle\psi|\, x\rangle$, for all $x \in \mathcal{H}$, we have

$$\mathcal{I}(\varphi + \alpha\psi) \;=\; \mathcal{I}(\varphi) \;+\; \overline{\alpha}\,\mathcal{I}(\psi)\,. \tag{V.22}$$

To avoid antilinear maps we compose $\mathcal{I}$ with an *antiunitary involution*. A map $\mathsf{j} : \mathcal{H} \to \mathcal{H}$ is an antiunitary involution if $\mathsf{j}^2 = \mathbf{1}_{\mathcal{H}}$ and $\langle\mathsf{j}\varphi|\mathsf{j}\psi\rangle = \langle\psi|\varphi\rangle$. Note that antiunitary involutions are antilinear. Given an antiunitary involution j on $\mathcal{H}$, the bijection $\mathcal{I}\circ\mathsf{j} : \mathcal{H} \to \mathcal{H}^*$, $|\psi\rangle \mapsto \langle\mathsf{j}\psi|$ is *linear* and, in fact, a Hilbert space isomorphism.

Similarly, given two complex Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ and an antiunitary involution $\mathsf{j}_2 : \mathcal{H}_2 \to \mathcal{H}_2$, we define an isomorphism by (the linear and continuous extension of)

$$\mathcal{J}_{12} : \mathcal{H}_1 \otimes \mathcal{H}_2 \;\to\; \mathcal{L}^2(\mathcal{H}_2;\mathcal{H}_1)\,, \quad \psi_1 \otimes \psi_2 \mapsto |\psi_1\rangle\langle\,\mathsf{j}_2\psi_2|\,. \tag{V.23}$$

The isomorphism $\mathcal{J}_{12}$ plays an important role in the analysis of the partial trace. A first sign of this it the following theorem.

Theorem V.2 (Schmidt Decomposition)**.** *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces of finite dimensions $d_1 := \dim(\mathcal{H}_1), d_2 := \dim(\mathcal{H}_2) \in \mathbb{N}$ and $\mathcal{H}_{12} := \mathcal{H}_1 \otimes \mathcal{H}_2$ their tensor product. Assume that $\Psi_{12} \in \mathcal{H}_{12}$ is a normalized vector and define by $\rho_{12} = |\Psi_{12}\rangle\langle\Psi_{12}| \in \mathcal{DM}(\mathcal{H}_{12})$ the corresponding pure density matrix on $\mathcal{H}_{12}$ and $\rho_1 = \mathrm{Tr}_2[\rho_{12}] \in \mathcal{DM}(\mathcal{H}_1)$ and $\rho_2 = \mathrm{Tr}_1[\rho_{12}] \in \mathcal{DM}(\mathcal{H}_2)$ its partial traces. Then the strictly positive eigenvalues of ρ_1 and ρ_2 agree and have the same multiplicites.*

Proof. Let $\{f_i\}_{i=1}^{d_1} \subseteq \mathcal{H}_1$ and $\{g_j\}_{j=1}^{d_2} \subseteq \mathcal{H}_2$ be ONB of eigenvectors of ρ_1 and ρ_2 with corresponding eigenvalues μ_i and λ_j, i.e.,

$$\rho_1 \;=\; \sum_{i=1}^{d_1} \mu_i |f_i\rangle\langle f_i| \quad \text{and} \quad \rho_2 \;=\; \sum_{j=1}^{d_2} \lambda_j |g_j\rangle\langle g_j| \,. \tag{V.24}$$

Then $\{f_i \otimes g_j | \, (i,j) \in \mathbb{Z}_1^{d_1} \times \mathbb{Z}_1^{d_2}\} \subseteq \mathcal{H}_1 \otimes \mathcal{H}_2$ is an ONB, too, and there exists complex numbers $A := (a_{i,j})_{(i,j)\in\mathbb{Z}_1^{d_1}\times\mathbb{Z}_1^{d_2}} \in \mathbb{C}^{d_1\times d_2}$ such that

$$\Psi_{12} \;=\; \sum_{i=1}^{d_1}\sum_{j=1}^{d_2} a_{i,j}\,(f_i \otimes g_j) \,. \tag{V.25}$$

Viewing A as a complex $d_1 \times d_2$ matrix, we observe that

$$1 \;=\; \|\Psi_{12}\|^2 \;=\; \sum_{i=1}^{d_1}\sum_{j=1}^{d_2} |a_{i,j}|^2 \;=\; \mathrm{Tr}_{\mathbb{C}^{d_2}}\big[A^*A\big] \;=\; \mathrm{Tr}_{\mathbb{C}^{d_1}}\big[A\,A^*\big] \,. \tag{V.26}$$

Furthermore,

$$\langle f_i|\,\rho_1\,f_k\rangle_{\mathcal{H}_1} \;=\; \sum_{j=1}^{d_2}\langle f_i\otimes g_j|\,\rho_{12}\,f_k\otimes g_j\rangle_{\mathcal{H}_{12}} \;=\; \sum_{j=1}^{d_2} a_{i,j}\,\overline{a_{i,j}} \;=\; (A\,A^*)_{i,k} \,, \tag{V.27}$$

for all $i, k \in \mathbb{Z}_1^{d_1}$, and

$$\langle g_j|\,\rho_2\,g_\ell\rangle_{\mathcal{H}_1} \;=\; \sum_{i=1}^{d_1}\langle f_i\otimes g_j|\,\rho_{12}\,f_i\otimes g_\ell\rangle_{\mathcal{H}_{12}} \;=\; \sum_{j=1}^{d_2} a_{i,j}\,\overline{a_{i,\ell}} \;=\; (A^*A)_{j,\ell} \,, \tag{V.28}$$

for all $j, \ell \in \mathbb{Z}_1^{d_2}$. By (V.24),

$$(A\,A^*)_{i,k} \;=\; \delta_{i,k}\,\mu_i \quad \text{and} \quad (A^*A)_{j,\ell} \;=\; \delta_{j,\ell}\,\lambda_j \,, \tag{V.29}$$

i.e., the canonical bases $\{e_i^{(1)}\}_{i=1}^{d_1} \subseteq \mathbb{C}^{d_1}$ and $\{e_j^{(2)}\}_{j=1}^{d_2} \subseteq \mathbb{C}^{d_2}$ are ONB of eigenvectors of $A\,A^* \in \mathbb{C}^{d_1\times d_1}$ and $A^*A \in \mathbb{C}^{d_2\times d_2}$, respectively.

From here, the assertion is obtained from well-known statements of linear algebra, whose proof we sketch here nevertheless. Fix a positive eigenvalue $\eta > 0$ of A^*A of multiplicity $1 \leq n \leq d_2$ and an ONB $\{\psi_1, \ldots, \psi_n\} \subseteq \mathbb{C}^{d_2}$ of eigenvectors of the corresponding spectral subspace of A^*A, i.e., $A^*A\psi_j = \eta\psi_j$, and set $\varphi_j := \eta^{-1/2}A\psi_j \in \mathbb{C}^{d_1}$, for all $j \in \mathbb{Z}_1^n$. Then each φ_j is an eigenvector of $A\,A^*$ corresponding to the eigenvalue η because

$$A\,A^*\varphi_j \;=\; \eta^{-1/2}\,A\,A^*A\psi_j \;=\; \eta^{1/2}\,A\psi_j \;=\; \eta\,\varphi_j \,. \tag{V.30}$$

Moreover,

$$\langle\varphi_j|\varphi_\ell\rangle_{\mathbb{C}^{d_2}} \;=\; \eta^{-1}\,\langle\psi_j|\,A^*A\psi_\ell\rangle_{\mathbb{C}^{d_2}} \;=\; \delta_{j,\ell} \,, \tag{V.31}$$

and $\{\varphi_1, \ldots, \varphi_n\} \subseteq \mathbb{C}^{d_1}$ is orthonormal, too. It follows that $d_1 \geq n$ and that η is an eigenvalue of $A\,A^*$ of multplicity $m \in \mathbb{Z}_n^{d_1}$.

The same argument, with A replaced by A^*, yields that, if $\eta > 0$ is an eigenvalue of $A\,A^*$ of multiplicity m, then $d_2 \geq m$, and η is also an eigenvalue of multiplicity $n \in \mathbb{Z}_m^{d_2}$ of A^*A.

Hence, the rank of A^*A and $A\,A^*$ is equal (regardless of whether $d_1 = d_2$ or not), A^*A and $A\,A^*$ have the same strictly positive eigenvalues, and each of these are of the same multiplicity. □

The following Corollary is, in some sense, the converse statement of Theorem V.2

Corollary V.3 (Purification)**.** *Let $\mathcal{H}_1$ be a Hilbert space of dimension $d_1 \in \mathbb{N} \cup \{\infty\}$ and $\rho_1 \in \mathcal{DM}(\mathcal{H}_1)$ a density matrix on $\mathcal{H}_1$. Then, for any Hilbert space $\mathcal{H}_2$ of dimension $d_2 \geq \mathrm{rk}(\rho_1)$ there exists a normalized vector $\Psi_{12} \in \mathcal{H}_{12} := \mathcal{H}_1 \otimes \mathcal{H}_2$ such that $\rho_1 = \mathrm{Tr}_2\big(|\Psi_{12}\rangle\langle\Psi_{12}|\big)$ is the partial trace of the pure state $|\Psi_{12}\rangle\langle\Psi_{12}| \in \mathcal{DM}(\mathcal{H}_{12})$.*

Proof. Let $r := \mathrm{rk}(\rho_1)$ be the rank of ρ_1 and $\{f_i\}_{i=1}^r \subseteq \mathcal{H}_1$ be an ONB of eigenvectors of $\mathrm{Ran}[\rho_1]$ with corresponding eigenvalues $\mu_i > 0$, i.e.,

$$\rho \;=\; \sum_{i=1}^{r} \mu_i \, |f_i\rangle\langle f_i| \,. \tag{V.32}$$

By assumption, $d_2 \geq r$ and there exists an orthonormal subset $\{g_j\}_{j=1}^r \subseteq \mathcal{H}_2$. Then the subset $\{f_i \otimes g_j |\, (i,j) \in \mathbb{Z}_1^r \times \mathbb{Z}_1^r\} \subseteq \mathcal{H}_{12}$ is orthonormal, too. Defining

$$\Psi \;:=\; \sum_{i=1}^{r} \sqrt{\mu_i}\, f_i \otimes g_i \;\in\; \mathcal{H}_{12} \,, \tag{V.33}$$

we observe that Ψ is normalized,

$$\|\Psi\|^2 \;=\; \sum_{i,j=1}^{r} \sqrt{\mu_i\,\mu_j}\, \langle f_i \otimes g_i | f_j \otimes g_j \rangle \;=\; \sum_{i=1}^{r} \mu_i \;=\; 1 \,, \tag{V.34}$$

and that its partial trace w.r.t the second tensor factor is ρ_1, indeed, as for all $k, \ell \in \mathbb{Z}_1^d$, we have that

$$\begin{aligned} \langle f_k | \rho_1 \, f_\ell \rangle \;&=\; \sum_{m=1}^{r} \langle f_k \otimes g_m | \Psi \rangle \, \langle \Psi | f_\ell \otimes g_m \rangle \\ &=\; \sum_{i,j,m=1}^{r} \sqrt{\mu_i\,\mu_j}\, \langle f_k \otimes g_m | f_j \otimes g_j \rangle \langle f_i \otimes g_i | f_\ell \otimes g_m \rangle \\ &=\; \sum_{i,j,m=1}^{r} \sqrt{\mu_i\,\mu_j}\, \delta_{k,j}\, \delta_{m,j}\, \delta_{i,\ell}\, \delta_{i,m} \;=\; \delta_{k,\ell}\, \mu_k \,. \end{aligned} \tag{V.35}$$

□

Next we introduce the notion of entanglement of a density matrix which is in close relation to its purity, as we demonstrate right after.

Definition V.4. Let $\big(\mathcal{H}_1, \langle\cdot|\cdot\rangle_1\big)$ and $\big(\mathcal{H}_2, \langle\cdot|\cdot\rangle_2\big)$ be two Hilbert spaces, and assume that $\rho_{12} \in \mathcal{DM}(\mathcal{H}_{12})$ is a density matrix. If there exist $\rho_1 \in \mathcal{DM}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{DM}(\mathcal{H}_2)$ such that $\rho_{12} = \rho_1 \otimes \rho_2$, then ρ_{12} is called **not entangled**. Conversely, if $\rho_{12} \neq \rho_1 \otimes \rho_2$, for any pair of density matrices $\rho_1 \in \mathcal{DM}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{DM}(\mathcal{H}_2)$, then ρ_{12} is called **entangled**.