CHAPTER 2

The Mathematics of Quantum Information Theory

This chapter puts into mathematical perspective some basic concepts of quantum information theory. (For a physically motivated approach, see Chapter 3.) We discuss the geometry of the set of quantum states, the entanglement vs. separability dichotomy, and introduce completely positive maps and quantum channels. All these concepts will be extensively used in Chapters 8–12.

2.1. On the geometry of the set of quantum states

2.1.1. Pure and mixed states. In this section we take a closer look at the set $\mathrm{D}(\mathcal{H})$ (or simply D) of quantum states on a finite-dimensional complex Hilbert space $\mathcal{H}$. By definition (see Section 0.10), we have

$$\mathrm{D}(\mathcal{H}) = \{\rho \in B_{\mathrm{sa}}(\mathcal{H}) \ : \ \rho \geqslant 0, \operatorname{Tr}\rho = 1\}. \tag{2.1}$$

If $\mathcal{H} = \mathbb{C}^d$, the definition (2.1) simply says that $\mathrm{D}(\mathbb{C}^d)$ is the base of the positive semi-definite cone $\mathcal{PSD}(\mathbb{C}^d)$ defined by the hyperplane $H_1 \subset \mathsf{M}_d^{\mathrm{sa}}$ of trace one Hermitian matrices (cf. (1.22)). The (real) dimension of the set $\mathrm{D}(\mathbb{C}^d)$ equals $d^2 - 1$: it has non-empty interior inside H_1. (This follows from $\mathcal{PSD}(\mathbb{C}^d)$ being a full cone.)

A state $\rho \in \mathrm{D}(\mathcal{H})$ is called *pure* if it has rank 1, i.e., if there is a unit vector $\psi \in \mathcal{H}$ such that

$$\rho = |\psi\rangle\langle\psi|.$$

Note that $|\psi\rangle\langle\psi|$ is the orthogonal projection onto the (complex) line spanned by ψ. We sometimes use the terminology "consider a pure state ψ" (such language is prevalent in physics literature). What we mean is that ψ is a unit vector and we consider the corresponding pure state $|\psi\rangle\langle\psi|$. We use the terminology of *mixed* states when we want to emphasize that we consider the set of all states, not necessarily pure.

Let ψ, χ be unit vectors in $\mathcal{H}$. Then the pure states $|\psi\rangle\langle\psi|$ and $|\chi\rangle\langle\chi|$ coincide if and only if there is a complex number λ with $|\lambda| = 1$ such that $\chi = \lambda\psi$. Therefore the set of pure states identifies with $\mathsf{P}(\mathcal{H})$, the projective space on $\mathcal{H}$. (See Appendix B.2; note that the space $\mathsf{P}(\mathbb{C}^d)$ is more commonly denoted by $\mathbb{CP}^{d-1}$.)

The set $\mathrm{D}(\mathcal{H})$ is a compact convex set, and it is easily checked that the extreme points of $\mathrm{D}(\mathcal{H})$ are exactly the pure states (cf. Proposition 1.9 and Corollary 1.10).

It follows from general convexity theory (Krein–Milman and Carathéodory's theorems) that any state is a convex combination of at most $(\dim\mathcal{H})^2$ pure states. However, using the spectral theorem instead tells us more: any state is a convex combination of at most $\dim\mathcal{H}$ pure states $|\psi_i\rangle\langle\psi_i|$, where (ψ_i) are pairwise orthogonal unit vectors (cf. Exercise 1.45). A fundamental consequence is that whenever we want to maximize a convex function (or minimize a concave function) over the

set $\mathrm{D}(\mathcal{H})$, the extremum is achieved on a pure state, which significantly reduces the dimension of the problem.

As opposed to pure states, which are extremal, the "most central" element in $\mathrm{D}(\mathcal{H})$ is the state $\mathrm{I}/\dim\mathcal{H}$, which is called the *maximally mixed state*, and denoted by ρ_* when there is no ambiguity. We also note that the set of states on $\mathcal{H}$ which are diagonal with respect to a given orthonormal basis $(e_i)_{i\in I}$ naturally identifies with the set of classical states on I.

EXERCISE 2.1. Describe states which belong to the boundary of $\mathrm{D}(\mathcal{H})$.

EXERCISE 2.2 (Every state is an average of pure states). Show that every state $\rho \in \mathrm{D}(\mathbb{C}^d)$ can be written as $\frac{1}{d}(|\psi_1\rangle\langle\psi_1| + \cdots + |\psi_d\rangle\langle\psi_d|)$ for some unit vectors $\psi_1, \ldots, \psi_d$ in $\mathbb{C}^d$.

2.1.2. The Bloch ball $\mathrm{D}(\mathbb{C}^2)$. The situation for $d = 2$ is very special. Let $\rho \in \mathsf{M}_2^{\mathrm{sa}}$, with $\operatorname{Tr}\rho = 1$. Then ρ has two eigenvalues, which can be written as $1/2-\lambda$ and $1/2+\lambda$ for some $\lambda \in \mathbb{R}$. Moreover, $\rho \geqslant 0$ if and only if $|\lambda| \leqslant 1/2$. On the other hand, we have

$$\|\rho - \rho_*\|_{\mathrm{HS}} = \sqrt{2}|\lambda|.$$

Therefore, ρ is a state if and only if $\|\rho - \rho_*\|_{\mathrm{HS}} \leqslant 1/\sqrt{2}$. What we have proved is that, inside the space of trace one self-adjoint operators, the set of states is a Euclidean ball centered at ρ_* and with radius $1/\sqrt{2}$. This ball is called the *Bloch ball* and its boundary is called the *Bloch sphere*. Once we introduce the *Pauli matrices*

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.2}$$

a convenient orthonormal basis (with respect to the Hilbert–Schmidt inner product) in $\mathsf{M}_2^{\mathrm{sa}}$ is

$$\Big(\frac{1}{\sqrt{2}}\,\mathrm{I}, \frac{1}{\sqrt{2}}\sigma_x, \frac{1}{\sqrt{2}}\sigma_y, \frac{1}{\sqrt{2}}\sigma_z\Big). \tag{2.3}$$

A very useful consequence of $\mathrm{D}(\mathbb{C}^2)$ being a ball is the fact—mentioned already in Section 1.2.1—that the cone $\mathcal{PSD}(\mathbb{C}^2)$ is isomorphic (or even isometric in the appropriate sense) to the Lorentz cone $\mathcal{L}_4$. A popular explicit isomorphism, inducing the so-called *spinor map* (see Appendix C), is given by

$$\mathbb{R}^4 \ni \mathbf{x} = (t, x, y, z) \mapsto \begin{bmatrix} t+z & x-iy \\ x+iy & t-z \end{bmatrix} = X \in \mathsf{M}_2^{\mathrm{sa}}. \tag{2.4}$$

The formula for X can be rewritten in terms of the Pauli matrices (2.2) as

$$X = t\,\mathrm{I} + x\sigma_x + y\sigma_y + z\sigma_z, \tag{2.5}$$

and so a convenient expression for it is $X = \mathbf{x}\cdot\sigma$, where σ is a shorthand for $(\mathrm{I}, \sigma_x, \sigma_y, \sigma_z)$, and "$\cdot$" is a "formal dot product." Since $\{\mathrm{I}, \sigma_x, \sigma_y, \sigma_z\}$ is a multiple of the orthonormal basis (2.3) of $\mathsf{M}_2^{\mathrm{sa}}$, it follows that the map given by (2.4) is likewise a multiple of isometry (with respect to the Euclidean metric in the domain and the Hilbert–Schmidt metric in the range). Next, it is readily verified that

$$\frac{1}{2}\operatorname{Tr} X = t, \ \det X = t^2 - x^2 - y^2 - z^2 =: q(\mathbf{x}), \tag{2.6}$$

where q is the quadratic form of the Minkowski spacetime, which confirms that $X \in \mathcal{PSD}(\mathbb{C}^2)$ iff $\mathbf{x} \in \mathcal{L}_4$. The isomorphism $\mathbf{x} \mapsto \mathbf{x}\cdot\sigma$ will be useful in understanding

automorphisms of the cones $\mathcal{L}_4$ and $\mathcal{PSD}(\mathbb{C}^2)$, and when proving Størmer's theorem in Section 2.4.5.

When $d > 2$, the set $\mathrm{D}(\mathbb{C}^d)$ is no longer a ball, but rather the non-commutative analogue of a simplex. Its symmetrization (see Section 4.1.2)

$$\mathrm{D}(\mathbb{C}^d)_{\diamondsuit} = \mathrm{conv}\left(\mathrm{D}(\mathbb{C}^d) \cup -\mathrm{D}(\mathbb{C}^d)\right) = \{A \in \mathsf{M}_d^{\mathrm{sa}} \ : \ \|A\|_1 \leqslant 1\},$$

is $S_1^{d,\mathrm{sa}}$, the unit ball of the self-adjoint part of the 1-Schatten space (see Section 1.3.2).

One way to quantify the fact that the set $\mathrm{D}(\mathbb{C}^d)$ is different from a ball when $d > 2$, is to compute the radius of its inscribed and circumscribed Hilbert–Schmidt balls. The former equals $1/\sqrt{d(d-1)}$ while the latter is $\sqrt{(d-1)/d}$ (the same values as for the set Δ_{d-1} of classical states on $\{1, \ldots, d\}$, and for the same reasons). In other words, if we denote by $B(\rho_*, r)$ the ball centered at ρ_* and with Hilbert–Schmidt radius r inside the hyperplane $H_1 = \{\mathrm{Tr}(\cdot) = 1\} \subset \mathsf{M}_d^{\mathrm{sa}}$, we have

$$B\left(\rho_*, \frac{1}{\sqrt{d(d-1)}}\right) \subset \mathrm{D}(\mathbb{C}^d) \subset B\left(\rho_*, \sqrt{\frac{d-1}{d}}\right) \tag{2.7}$$

and these values—differing by the factor of $d-1$—are the best possible.

Exercise 2.3 (The Bloch sphere is a sphere). Show that the matrix X given by (2.5) has eigenvalues 1 and -1 if and only if $t = 0$ and $x^2 + y^2 + z^2 = 1$.

Exercise 2.4 (Composition rules for Pauli matrices). Verify the composition rules for Pauli matrices. (i) $\sigma_a^2 = \mathrm{I}$ (ii) If a, b, c are all different, then $\sigma_a \sigma_b = i\varepsilon\sigma_c$, where $\varepsilon = \pm 1$ is the sign of the permutation $(x, y, z) \mapsto (a, b, c)$; in particular, if $a \neq b$, then $\sigma_a \sigma_b = -\sigma_b \sigma_a$.

2.1.3. Facial structure.

Proposition 2.1 (Characterization of faces of D). *There is a one-to-one correspondence between nontrivial subspaces of $\mathbb{C}^d$ and proper faces of $\mathrm{D}(\mathbb{C}^d)$. Given a subspace $\{0\} \subsetneq E \subsetneq \mathbb{C}^d$, the corresponding face $\mathrm{D}(E)$ is the set of states whose range is contained in E:*

$$\mathrm{D}(E) = \{\rho \in \mathrm{D}(\mathbb{C}^d) \ : \ \rho(\mathbb{C}^d) \subset E\}.$$

In particular, pure states (extreme points, i.e., minimal, 0-dimensional faces) correspond to the case $\dim E = 1$. In the direction opposed to a pure state $|x\rangle\langle x|$ lies a face which corresponds to all states with a range orthogonal to x; these are maximal proper faces.

Remark 2.2. All faces of $\mathrm{D}(\mathbb{C}^d)$ are exposed (as defined in Exercise 1.5) since $\mathrm{D}(E)$ is the intersection of $\mathrm{D}(\mathbb{C}^d)$ with the hyperplane $\{X \ : \ \mathrm{Tr}(XP_E) = 1\}$.

Proof of Proposition 2.1. Denote by $\mathrm{range}(\rho) = \rho(\mathbb{C}^d)$ the range of a state $\rho \in \mathrm{D}(\mathbb{C}^d)$. We use the following observation: if $\rho, \sigma \in \mathrm{D}(\mathbb{C}^d)$ and $\lambda \in (0, 1)$, then

$$\mathrm{range}(\lambda\rho + (1-\lambda)\sigma) = \mathrm{range}(\rho) + \mathrm{range}(\sigma). \tag{2.8}$$

We first check that, for any nontrivial subspace $E \subset \mathbb{C}^d$, $\mathrm{D}(E)$ is a face of $\mathrm{D}(\mathbb{C}^d)$. For indeed, if $\rho \in \mathrm{D}(E)$ can be written as $\lambda\rho_1 + (1-\lambda)\rho_2$ for $\rho_1, \rho_2 \in \mathrm{D}(\mathbb{C}^d)$ and $\lambda \in (0, 1)$, then (2.8) implies that $\mathrm{range}(\rho_1) \subset E$ and $\mathrm{range}(\rho_2) \subset E$.

Conversely, let $F \subset \mathrm{D}(\mathbb{C}^d)$ be a proper face. Define $E = \bigcup\{\mathrm{range}(\rho) \ : \ \rho \in F\}$. It follows—from (2.8) and from the fact that F is convex—that E is actually a

subspace and that F contains an element ρ such that $\mathrm{range}(\rho) = E$. We now claim that $F = \mathrm{D}(E)$. The direct inclusion is obvious. Conversely, consider $\sigma \in \mathrm{D}(E)$. For $\lambda > 0$ small enough the operator $\tau = \frac{1}{1-\lambda}(\rho - \lambda\sigma)$ is a state. Since $\rho = \lambda\sigma + (1-\lambda)\tau$, we conclude that the segment joining σ and τ is contained in F; in particular $\sigma \in F$. □

EXERCISE 2.5. Show directly (i.e., without appealing to Proposition 2.1) that any *exposed* face of $\mathrm{D}(\mathbb{C}^d)$ has the form $\mathrm{D}(E)$ for some subspace $E \subset \mathbb{C}^d$.

2.1.4. Symmetries. We now describe the symmetries of $\mathrm{D}(\mathbb{C}^d)$. This is closely related to the famous theorem of Wigner that characterizes the isometries of complex projective space as a metric space. Recall (see Appendix B.2) that $[\psi]$ denotes the equivalence class in $\mathsf{P}(\mathbb{C}^d)$ of a unit vector $\psi \in S_{\mathbb{C}^d}$.

THEOREM 2.3 (Wigner's theorem). *Denote by $\mathsf{P}(\mathbb{C}^d)$ the projective space over $\mathbb{C}^d$, equipped with the Fubini–Study metric* (B.5). *A map $f : \mathsf{P}(\mathbb{C}^d) \to \mathsf{P}(\mathbb{C}^d)$ is an isometry if and only if there is a map U on $\mathbb{C}^d$ which is either unitary or anti-unitary such that, for any unit vector ψ,*

$$f([\psi]) = [U(\psi)]. \tag{2.9}$$

A map $U : \mathbb{C}^d \to \mathbb{C}^d$ is anti-unitary if it is the composition of a unitary map with complex conjugation.

PROOF. We outline the proof of Wigner's theorem for $d = 2$. Since the projective space over $\mathbb{C}^2$ identifies with the Bloch sphere, its group of isometries is given by the orthogonal group $\mathsf{O}(3)$, and splits into direct isometries (rotations, or $\mathsf{SO}(3)$) and indirect isometries.

Let f be a direct isometry of the Bloch ball. It has two opposite fixed points $[\varphi_1]$ and $[\varphi_2]$, with $\varphi_1 \perp \varphi_2$, and is a rotation of angle θ in the plane $\{[\frac{1}{\sqrt{2}}(\varphi_1 + e^{i\alpha}\varphi_2)] : \alpha \in \mathbb{R}\}$. One checks that (2.9) is satisfied when U is given by $U(\varphi_1) = \varphi_1$ and $U(\varphi_2) = e^{i\theta}\varphi_2$. Note that U is determined up to a global phase. In particular, if we insist on having $U \in \mathsf{SU}(2)$, we are led to the choice $U(\varphi_1) = e^{-i\theta/2}\varphi_1$ and $U(\varphi_2) = e^{i\theta/2}\varphi_2$ involving the half-angle. (We point out the isomorphism $\mathsf{PSU}(2) \leftrightarrow \mathsf{SO}(3)$, see Exercise B.4.)

The complex conjugation with respect to an orthonormal basis (ψ_1, ψ_2) in $\mathbb{C}^2$ induces on the Bloch ball the reflection R in the plane $\{[\cos\theta\psi_1 + \sin\theta\psi_2] : \theta \in \mathbb{R}\}$. Since any indirect isometry of the Bloch ball is the composition of R with a direct isometry, the result follows.

The case $d > 2$ can be deduced from the $d = 2$ case; we do not include the argument here (see Notes and Remarks). □

When $\mathsf{P}(\mathbb{C}^d)$ is identified with the set of pure states on $\mathbb{C}^d$, the isometries from Theorem 2.3 act as $\rho \mapsto U\rho U^\dagger$ or $\rho \mapsto U\rho^T U^\dagger$ for $U \in \mathsf{U}(d)$. Here ρ^T denotes the transposition of a state ρ with respect to a distinguished basis (since $\rho = \rho^\dagger$, ρ^T is also the complex conjugate of ρ with respect to that basis).

THEOREM 2.4 (Kadison's theorem). *Affine maps preserving globally $\mathrm{D}(\mathbb{C}^d)$ are of the form $\rho \mapsto U\rho U^\dagger$ or $\rho \mapsto U\rho^T U^\dagger$ for $U \in \mathsf{U}(d)$. In particular, they are isometries with respect to the Hilbert–Schmidt distance.*

PROOF. Let Φ be an affine map on $\mathsf{M}_d^{\mathrm{sa}}$ such that $\Phi(\mathrm{D}(\mathbb{C}^d)) = \mathrm{D}(\mathbb{C}^d)$. Then Φ preserves the set of faces of $\mathrm{D}(\mathbb{C}^d)$, which are described in Proposition 2.1. In

particular, Φ preserves the set of minimal faces, which identify with pure states. Therefore Φ induces a bijection on $\mathsf{P}(\mathbb{C}^d)$. We claim that Φ is an isometry with respect to the Fubini–Study distance (B.5), which is equivalent to

$$\operatorname{Tr}\left(\Phi(|\psi\rangle\langle\psi|)\cdot\Phi(|\varphi\rangle\langle\varphi|)\right)=|\langle\psi,\varphi\rangle|^2$$

for $\psi,\varphi\in\mathbb{C}^d$. If $[\psi]=[\varphi]$, this is clear. Otherwise, let $M\subset\mathbb{C}^d$ be the 2-dimensional subspace generated by ψ and φ. By Proposition 2.1, the set $\mathrm{D}(M)$ canonically identifies with a (3-dimensional) face of $\mathrm{D}(\mathbb{C}^d)$. Consequently, $\Phi(\mathrm{D}(M))$ is also a face, which identifies with $\mathrm{D}(M')$ for some 2-dimensional subspace $M'\subset\mathbb{C}^d$. Since $\mathrm{D}(M)$ and $\mathrm{D}(M')$ are Bloch balls, the map Φ restricted to $\mathrm{D}(M)$ must be an isometry (affine maps preserving S^2 are isometries). We may now apply Wigner's theorem: there is $U\in\mathsf{U}(d)$ such that either $\Phi(\rho)=U\rho U^\dagger$ whenever ρ is a pure state, or $\Phi(\rho)=U\rho^TU^\dagger$ for all pure states ρ. Since Φ is affine, one of the two formulas is valid for all $\rho\in\mathrm{D}(\mathbb{C}^d)$. □

Although for $d>2$ the set $\mathrm{D}(\mathbb{C}^d)$ is not centrally symmetric, we may argue that the maximally mixed state ρ_* plays the role of a center. In particular, we have

PROPOSITION 2.5. *Let $\rho\in\mathrm{D}(\mathbb{C}^d)$ be a state which is fixed by all the isometries of $\mathrm{D}(\mathbb{C}^d)$ (with respect to the Hilbert–Schmidt distance). Then $\rho=\rho_*$.*

PROOF. We have $U\rho U^\dagger=\rho$ for every unitary matrix U. Since $\mathsf{U}(d)$ spans M_d as a vector space, ρ commutes with any matrix, therefore it equals $\alpha\,\mathrm{I}$ for some $\alpha\in\mathbb{C}$, and the trace constraint forces $\alpha=1/d$. □

One consequence of Proposition 2.5 is that ρ_* is the centroid of $\mathrm{D}(\mathbb{C}^d)$. Kadison's theorem also implies that D has enough symmetries in the sense of Section 4.2.2 (see Exercise 4.25). Another consequence of Kadison's Theorem 2.4 is a characterization of affine automorphisms of the cone of positive semi-definite matrices, which will be presented in Proposition 2.29.

EXERCISE 2.6. Show that the affine automorphisms of $\mathrm{D}(\mathbb{C}^2)$ form a group which is isomorphic to $\mathsf{O}(3)$.

EXERCISE 2.7. Show that the affine automorphisms of $\mathrm{D}(\mathbb{C}^d)$ form a group which is isomorphic to the semidirect product of $\mathsf{PSU}(d)$ and $\mathbb{Z}_2$ with respect to the action of $\mathbb{Z}_2$ on $\mathsf{PSU}(d)$ induced by the complex conjugation.

EXERCISE 2.8. State and prove the real version of Wigner's theorem.

EXERCISE 2.9. Let ρ be a state which is invariant under transposition with respect to any basis. Show that $\rho=\rho_*$.

2.2. States on multipartite Hilbert spaces

2.2.1. Partial trace. A fundamental concept in quantum information theory is the *partial trace* (for a physically motivated approach, see Section 3.4). Let $\mathcal{H}=\mathcal{H}_1\otimes\mathcal{H}_2$ be a bipartite Hilbert space. The partial trace over $\mathcal{H}_2$ is the map (or the superoperator, see Section 0.9) $\operatorname{Tr}_{\mathcal{H}_2}:B(\mathcal{H}_1)\otimes B(\mathcal{H}_2)\to B(\mathcal{H}_1)$ defined as $\mathrm{Id}_{B(\mathcal{H}_1)}\otimes\operatorname{Tr}$. Its action on product operators is given by

$$\operatorname{Tr}_{\mathcal{H}_2}(A\otimes B)=(\operatorname{Tr}B)A$$

for $A\in B(\mathcal{H}_1)$, $B\in B(\mathcal{H}_2)$. Similarly, the partial trace with respect to $\mathcal{H}_1$ is defined as $\operatorname{Tr}_{\mathcal{H}_1}=\operatorname{Tr}\otimes\mathrm{Id}_{B(\mathcal{H}_2)}$.

In particular, if ρ is a state on $\mathcal{H}_1 \otimes \mathcal{H}_2$, then $\mathrm{Tr}_{\mathcal{H}_1} \rho$ is a state on $\mathcal{H}_2$, and $\mathrm{Tr}_{\mathcal{H}_2}$ is a state on $\mathcal{H}_1$. Note also the formulas $\mathrm{Tr}_{\mathcal{H}_1}(\rho_1 \otimes \rho_2) = \rho_2$ and $\mathrm{Tr}_{\mathcal{H}_2}(\rho_1 \otimes \rho_2) = \rho_1$ for states $\rho_1 \in \mathrm{D}(\mathcal{H}_1)$, $\rho_2 \in \mathrm{D}(\mathcal{H}_2)$.

We sometimes write Tr_1 for $\mathrm{Tr}_{\mathcal{H}_1}$ and Tr_2 for $\mathrm{Tr}_{\mathcal{H}_2}$. The definition of partial trace extends naturally to the multipartite setting: if $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$, then for $1 \leqslant i \leqslant k$ we denote by $\mathrm{Tr}_{\mathcal{H}_i}$ or Tr_i the operation

$$\mathrm{Id}_{B(\mathcal{H}_1)} \otimes \cdots \otimes \mathrm{Id}_{B(\mathcal{H}_{i-1})} \otimes \mathrm{Tr} \otimes \mathrm{Id}_{B(\mathcal{H}_{i+1})} \otimes \cdots \otimes \mathrm{Id}_{B(\mathcal{H}_k)} .$$

2.2.2. Schmidt decomposition. We recall the *singular value decomposition* (SVD) for matrices: any real or complex matrix $A \in \mathsf{M}_{k,d}$ can be decomposed as $A = U\Sigma V^\dagger$, when U and V are unitary matrices of sizes k and d respectively, and $\Sigma = (\Sigma_{ij}) \in \mathsf{M}_{k,d}$ is a "rectangular diagonal" (i.e., such that $\Sigma_{ij} = 0$ whenever $i \neq j$) nonnegative matrix. Moreover, up to permutation, the "diagonal" elements of Σ are uniquely determined by A and are called the *singular values* of A. We often denote the singular values of A by $s_1(A) \geqslant \cdots \geqslant s_{\min(k,d)}(A)$. The singular values of A coincide with the eigenvalues of $(AA^\dagger)^{1/2}$ when $k \leqslant d$, and with the eigenvalues of $(A^\dagger A)^{1/2}$ when $k \geqslant d$. Note that, in any case, $AA^\dagger$ and $A^\dagger A$ share the same nonzero eigenvalues.

An equivalent presentation of the SVD is as follows: there exist orthonormal sequences (u_i) (in $\mathbb{R}^k$ or $\mathbb{C}^k$, depending on the context) and (v_i) (in $\mathbb{R}^d$ or $\mathbb{C}^d$), and a non-increasing sequence of nonnegative scalars (s_i) such that

$$A = \sum_i s_i |u_i\rangle\langle v_i|. \tag{2.10}$$

When translated into the language of tensors (see Section 0.4), the singular value decomposition becomes the *Schmidt decomposition*, which is widely used in quantum information. We note that, besides the bipartite situation, there is no analogue of the Schmidt decomposition in multipartite Hilbert spaces.

Proposition 2.6 (easy). *Let ψ be a vector in a (real or complex) bipartite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, with $d_1 = \dim \mathcal{H}_1$ and $d_2 = \dim \mathcal{H}_2$. Set $d := \min(d_1, d_2)$. Then there exist nonnegative scalars $(\lambda_i)_{1 \leqslant i \leqslant d}$, and orthonormal vectors $(\chi_i)_{1 \leqslant i \leqslant d}$ in $\mathcal{H}_1$ and $(\varphi_i)_{1 \leqslant i \leqslant d}$ in $\mathcal{H}_2$, such that*

$$\psi = \sum_{i=1}^{d} \lambda_i \chi_i \otimes \varphi_i. \tag{2.11}$$

The numbers $(\lambda_1, \ldots, \lambda_d)$ are uniquely determined if we require that $\lambda_1 \geqslant \cdots \geqslant \lambda_d$ and are called the Schmidt coefficients of ψ.

Note that $\lambda_1^2 + \cdots + \lambda_d^2 = |\psi|^2$. We may write $\lambda_i(\psi)$ instead of λ_i to emphasize the dependence on ψ. The largest r such that $\lambda_r(\psi) > 0$ is called the *Schmidt rank* of ψ. If $\psi \in \mathbb{C}^k \otimes \mathbb{C}^d$ is identified with a matrix $M \in \mathsf{M}_{k,d}$ as in Section 0.8, then

$$\mathrm{Tr}_{\mathbb{C}^d} |\psi\rangle\langle\psi| = MM^\dagger. \tag{2.12}$$

Via this identification, Schmidt coefficients of ψ coincide with singular values of M, and the Schmidt rank of ψ coincides with the rank of M. States of Schmidt rank 1 are exactly product vectors. The largest and the smallest Schmidt coefficients of $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ are also given by the variational formulas

$$\lambda_1(\psi) = \max\{|\langle \psi, \chi \otimes \varphi\rangle| \ : \ \chi \in \mathcal{H}_1, \varphi \in \mathcal{H}_2, |\chi| = |\varphi| = 1\}, \tag{2.13}$$

often referred to as the maximal *overlap* with a product vector, and

$$\lambda_d(\psi) = \min_{\chi\in\mathcal{H}_1,|\chi|=1} \max_{\varphi\in\mathcal{H}_2,|\varphi|=1} |\langle\psi, \chi\otimes\varphi\rangle|. \tag{2.14}$$

The above are fully analogous to the (special cases of) Courant–Fischer variational formulas for singular values of a matrix.

2.2.3. A fundamental dichotomy: separability vs. entanglement. We now introduce a fundamental concept: the dichotomy between separability and entanglement for quantum states. Let $\mathcal{H}$ be a **complex** Hilbert space admitting a tensor decomposition

$$\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k. \tag{2.15}$$

Recall that since 1-dimensional factors may be dropped, we may—and usually will—assume that all the factors are of dimension at least 2.

Definition 2.7. A pure state $\rho = |\chi\rangle\langle\chi|$ on $\mathcal{H}$ is said to be *pure separable* if the unit vector χ is a product vector, i.e., if there exist unit vectors $\chi_1, \ldots, \chi_k$ such that $\chi = \chi_1 \otimes \cdots \otimes \chi_k$. In that case,

$$\rho = |\chi_1\rangle\langle\chi_1| \otimes \cdots \otimes |\chi_k\rangle\langle\chi_k|. \tag{2.16}$$

Extending the definition of separability to mixed states requires to consider convex combinations (we study in detail the convex hull operation $A \mapsto \mathrm{conv}(A)$ in Section 1.1.2).

Definition 2.8. A mixed state $\rho = |\chi\rangle\langle\chi|$ on $\mathcal{H}$ is said to be *separable* if it can be written as a convex combination of pure separable states. We denote by $\mathrm{Sep}(\mathcal{H})$ (or simply by Sep) the set of separable states on $\mathcal{H}$. We have

$$\mathrm{Sep}(\mathcal{H}) = \mathrm{conv}\{|\chi_1 \otimes \cdots \otimes \chi_k\rangle\langle\chi_1 \otimes \cdots \otimes \chi_k| \ : \ \chi_1 \in \mathcal{H}_1, \ldots, \chi_k \in \mathcal{H}_k\}. \tag{2.17}$$

States which are not separable are called *entangled*. Since pure states are the extreme points even of the larger set $\mathrm{D}(\mathcal{H})$ (Proposition 2.1), it follows that the pure separable states (i.e., those given by (2.16)) are exactly the extreme points of $\mathrm{Sep}(\mathcal{H})$. Since there are vectors that are not product vectors, the set $\mathrm{Sep}(\mathcal{H})$ is a proper subset of $\mathrm{D}(\mathcal{H})$. A schematic representation of the inclusion $\mathrm{Sep} \subset \mathrm{D}$ and of the corresponding extreme points can be found in Figure 2.1.

An alternative description of the set $\mathrm{Sep}(\mathcal{H})$ is the following: it is the convex hull of product states.

$$\mathrm{Sep}(\mathcal{H}) = \mathrm{conv}\{\rho_1 \otimes \cdots \otimes \rho_k \ : \ \rho_1 \in \mathrm{D}(\mathcal{H}_1), \ldots, \rho_k \in \mathrm{D}(\mathcal{H}_k)\}. \tag{2.18}$$

It is noteworthy that $\mathrm{Sep}(\mathcal{H})$ and $\mathrm{D}(\mathcal{H})$ have the same dimension. This can be seen from the following observation. Let $V_1, \ldots, V_k$ be real or complex vector spaces and, for each i, let $\mathcal{F}_i$ be a family of linear independent vectors in V_i. Then the family

$$\bigotimes \mathcal{F}_i = \{f_1 \otimes \cdots \otimes f_k \ : \ f_i \in \mathcal{F}_i\}$$

is linearly independent in $\bigotimes V_i$. We apply the observation with $V_i = B^{\mathrm{sa}}(\mathcal{H}_i)$ and with $\mathcal{F}_i$ being a basis of $B^{\mathrm{sa}}(\mathcal{H}_i)$ consisting of states. This way, we obtain a family of $(\dim \mathcal{H})^2$ linearly independent product states which are elements of $\mathrm{Sep}(\mathcal{H})$. This shows that $\mathrm{Sep}(\mathcal{H})$ has dimension $(\dim \mathcal{H})^2 - 1$. Note that this argument uses the fact that the field is $\mathbb{C}$: in real quantum mechanics, the set of separable states has empty interior (cf. Section 0.4).

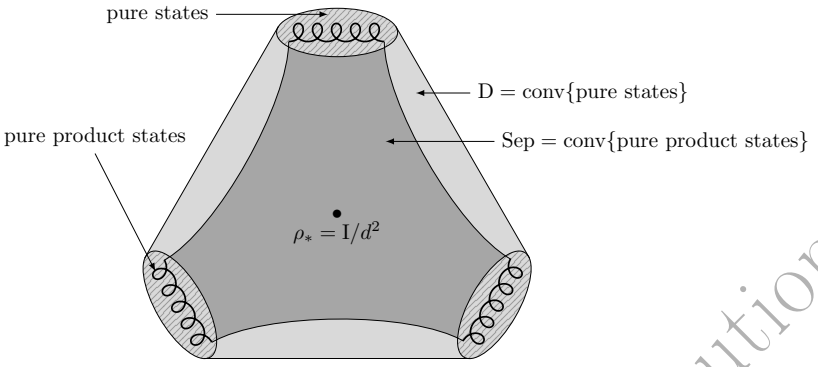

FIGURE 2.1. The sets of states (D) and of separable states (Sep) on $\mathbb{C}^d \otimes \mathbb{C}^d$. Pure product states have measure zero inside the set of pure states; however both convex hulls have the same dimension. The picture does not respect convexity of Sep, but it is supposed to reflect the relative rarity of separability.

A deeper result asserts that, in the bipartite case, not only do Sep and D have the same dimension, they also have the same inradius. This may look surprising since Sep is defined as the convex hull of a very small subset of the set of extreme points of D. This remarkable fact was discovered by Gurvits and Barnum and will be proved later (see Theorem 9.15).

It is often useful to consider the cone

$$\mathcal{SEP}(\mathcal{H}) = \{\lambda\rho \ : \ \lambda \geqslant 0, \ \rho \in \mathrm{Sep}(\mathcal{H})\}$$

of separable operators; we will return to this in Section 2.4.

We emphasize that the notion of separability depends crucially on the tensor decomposition (2.15) of $\mathcal{H}$. As a concrete example, consider a tripartite space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$. There are several different notions of separability on $\mathcal{H}$: separability with respect to the tripartition $\mathcal{H}_1 : \mathcal{H}_2 : \mathcal{H}_3$, and separability with respect to each of the three bipartitions $\mathcal{H}_1 : \mathcal{H}_2 \otimes \mathcal{H}_3$, $\mathcal{H}_2 : \mathcal{H}_1 \otimes \mathcal{H}_3$ and $\mathcal{H}_3 : \mathcal{H}_1 \otimes \mathcal{H}_2$ or combinations thereof. Moreover, some authors introduce the concept of "absolute" properties. For example, a state $\rho \in \mathrm{D}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k)$ is *absolutely separable* if $U\rho U^\dagger$ is separable for any unitary operator U on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$. However, in this book we will focus primarily on the setting in which all partitions are fixed.

Although the extreme points of Sep are very easy to describe (as noted earlier, they are precisely the pure product states), there is no simple description of the facial structure of Sep available (compare with Proposition 2.1, which describes all the faces of D). The complexity of the facial structure of Sep can be related to the fact that deciding whether a state is separable is known to be, in the general setting, NP-hard. This makes calculating some parameters of Sep highly nontrivial; we will run into this problem in Chapter 9 (see, e.g., Theorem 9.6). Finally, in view of the dual formulation of the problem of describing faces of a convex body (see Section 1.1.5, and particularly Proposition 1.5), characterizing maximal faces of Sep is essentially equivalent to describing extreme points of the object dual to Sep (see (2.47)), which are well understood only for very small dimensions. (Appendix C discusses closely related issues.)

EXERCISE 2.10 (The length of separable representations). (i) Using Carathéodory's theorem (see Section 1.1.2), show that any separable state on $\mathbb{C}^d \otimes \mathbb{C}^d$ can be written as the convex combination of at most d^4 pure product states. (ii) Using a dimension-counting argument, prove that there exist separable states on $\mathbb{C}^d \otimes \mathbb{C}^d$ which cannot be written as a convex combination of less than cd^3 pure product states, for some constant $c > 0$.

EXERCISE 2.11 (Edges of Sep). Let $d_1, d_2 \geqslant 2$. Show that $\mathrm{Sep}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ has a face (as defined in Section 1.1.3) which is 1-dimensional.

2.2.4. Some examples of bipartite states. We now present some examples of states on $\mathbb{C}^d \otimes \mathbb{C}^d$ that are widely used in quantum information theory.

2.2.4.1. *Maximally entangled states.* A pure state on $\mathbb{C}^d \otimes \mathbb{C}^d$ is called *maximally entangled* if it has the form $\rho = |\psi\rangle\langle\psi|$ with

$$\psi = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes f_i, \tag{2.19}$$

where $(e_i)_{1 \leqslant i \leqslant d}$ and $(f_i)_{1 \leqslant i \leqslant d}$ are two orthonormal bases in $\mathbb{C}^d$. Such a vector ψ is called a *maximally entangled vector*.

In the special case of $d = 2$, i.e., for systems formed of 2 qubits, the maximally entangled states are called *Bell states*. Many quantum information protocols, such as quantum teleportation, use Bell states as a fundamental resource.

If we identify vectors and matrices as explained in Section 0.8, the set of all maximally entangled vectors on $\mathbb{C}^d \otimes \mathbb{C}^d$ (or, more precisely, on $\overline{\mathbb{C}^d} \otimes \mathbb{C}^d$) identifies with the unitary group $\mathsf{U}(d) \subset \mathsf{M}_d$.

EXERCISE 2.12 (Maximally entangled states and trace duality). Let ψ be the maximally entangled state given by (2.19), with (e_i) and (f_i) both equal to the canonical basis $(|i\rangle)_{1 \leqslant i \leqslant d}$, and let $\rho = |\psi\rangle\langle\psi|$. Show that $\mathrm{Tr}\big(\rho(X \otimes Y)\big) = \frac{1}{d}\,\mathrm{Tr}(XY^T)$ for any $X, Y \in B(\mathbb{C}^d)$.

EXERCISE 2.13 (Maximal entanglement and the distance to Seg). Let ψ be a unit vector in $\mathbb{C}^d \otimes \mathbb{C}^d$ and $\mathrm{Seg} \subset S_{\mathbb{C}^d \otimes \mathbb{C}^d}$ the set of unit product vectors (see (B.6)). Show that $|\psi\rangle\langle\psi|$ is maximally entangled if and only if $\mathrm{dist}(\psi, \mathrm{Seg})$ is maximal. For extensions to the multipartite case, see Section 8.5.

2.2.4.2. *Isotropic states.* Isotropic states are states which are a convex (or affine) combination of the maximally mixed state and a maximally entangled state. They have the form

$$\rho_\beta = \beta|\psi\rangle\langle\psi| + (1 - \beta)\frac{\mathrm{I}}{d^2}, \tag{2.20}$$

where ψ is as in (2.19) and $-\frac{1}{d^2-1} \leqslant \beta \leqslant 1$.

2.2.4.3. *Werner states.* Consider the *flip operator* $F \in B^{\mathrm{sa}}(\mathbb{C}^d \otimes \mathbb{C}^d)$ defined on pure tensors by $F(x \otimes y) = y \otimes x$ and extended by linearity. Its eigenspaces are the *symmetric subspace*

$$\mathrm{Sym}_d = \{\psi \in \mathbb{C}^d \otimes \mathbb{C}^d \ : \ F(\psi) = \psi\}$$

and the *antisymmetric subspace*

$$\mathrm{Asym}_d = \{\psi \in \mathbb{C}^d \otimes \mathbb{C}^d \ : \ F(\psi) = -\psi\}.$$

The corresponding projectors are $P_{\mathrm{Sym}_d} = \frac{1}{2}(\mathrm{I}+F)$ and $P_{\mathrm{Asym}_d} = \frac{1}{2}(\mathrm{I}-F)$. We need to know that the symmetric and antisymmetric subspaces are irreducible for the action $U \mapsto U \otimes U$ of the unitary group.

PROPOSITION 2.9 (see Exercise 2.15). *Let $E \subsetneq \mathbb{C}^d \otimes \mathbb{C}^d$ be a nonzero subspace such that for every $U \in \mathsf{U}(d)$ and $\psi \in E$, we have $(U \otimes U)\psi \in E$. Then either $E = \mathrm{Sym}_d$ or $E = \mathrm{Asym}_d$.*

Note that $\dim \mathrm{Sym}_d = d(d+1)/2$ while $\dim \mathrm{Asym}_d = d(d-1)/2$. The *symmetric* and *antisymmetric states* are defined respectively as

$$\pi_s = \frac{2}{d(d+1)} P_{\mathrm{Sym}_d} \quad \text{and} \quad \pi_a = \frac{2}{d(d-1)} P_{\mathrm{Asym}_d}.$$

For $\lambda \in [0,1]$, consider the state w_λ (called the *Werner state*) obtained as a convex combination of these two projectors

$$w_\lambda = \lambda \pi_s + (1-\lambda)\pi_a. \tag{2.21}$$

Another equivalent expression is

$$w_\lambda = \frac{1}{d^2 - d\alpha}(\mathrm{I} - \alpha F), \tag{2.22}$$

where

$$\alpha = \frac{1 + d(1-2\lambda)}{1 + d - 2\lambda} \in [-1, 1]. \tag{2.23}$$

When $d = 2$, the space Asym_2 has dimension one, and Werner states are then a special case of isotropic states.

EXERCISE 2.14 (Polarization formulas in Sym_d and Asym_d). Prove that $\mathrm{Sym}_d = \mathrm{span}\{x \otimes x \ : \ x \in \mathbb{C}^d\}$ and $\mathrm{Asym}_d = \mathrm{span}\{x \otimes y - y \otimes x \ : \ x, y \in \mathbb{C}^d\}$.

EXERCISE 2.15 (Irreducibility of Sym_d and Asym_d).
Denote by $\mathscr{A} = \mathrm{span}\{U \otimes U \ : \ U \in \mathsf{U}(d)\}$.
(i) Prove that for every subspace $E \subset \mathbb{C}^d$, $P_E \otimes P_E \in \mathscr{A}$.
(ii) Show that for every nonzero vectors $\varphi, \psi \in \mathrm{Sym}_d$, there is $V \in \mathscr{A}$ such that $\langle\varphi|V|\psi\rangle \neq 0$.
(iii) Show that for every nonzero vectors $\varphi, \psi \in \mathrm{Asym}_d$, there is $V \in \mathscr{A}$ such that $\langle\varphi|V|\psi\rangle \neq 0$.
(iv) Deduce Proposition 2.9.

EXERCISE 2.16 (The twirling channel and Werner states).
(i) Show that a state $\rho \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ satisfies $(V \otimes V)\rho(V \otimes V)^\dagger = \rho$ for all $V \in \mathsf{U}(d)$ if and only if it is a Werner state.
(ii) Show that if U is chosen at random with respect to the Haar measure on $\mathsf{U}(\mathbb{C}^d)$, then for any $\rho \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$, $\mathbf{E}(U \otimes U)\rho(U \otimes U)^\dagger = w_\lambda$ with $\lambda = \mathrm{Tr}(\rho P_{\mathrm{Sym}_d})$. (The map $\rho \mapsto \mathbf{E}(U \otimes U)\rho(U \otimes U)^\dagger$ is called the *twirling channel*.)
(iii) Show that if $\psi \in S_{\mathbb{C}^d}$ is chosen uniformly at random, then $\mathbf{E}\,|\psi\otimes\psi\rangle\langle\psi\otimes\psi| = \pi_s$.

2.2.5. Entanglement hierarchies.

2.2.5.1. *k-extendible states.* Consider a bipartite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ and $k \geqslant 2$. For $i \in \{1, \ldots, k\}$, we denote by

$$\mathrm{Tr}_{\text{all but } i} : B(\mathcal{H}_1 \otimes \mathcal{H}_2^{\otimes k}) \to B(\mathcal{H}_1 \otimes \mathcal{H}_2)$$

the partial trace with respect to all copies of $\mathcal{H}_2$, except for the ith. A state $\rho \in \mathrm{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is said to be *k-extendible* (with respect to $\mathcal{H}_2$) if there exists a state $\rho_k \in \mathrm{D}(\mathcal{H}_1 \otimes \mathcal{H}_2^{\otimes k})$ with the property that e

$$\mathrm{Tr}_{\text{all but } i}\, \rho_k = \rho$$

for every $i \in \{1, \ldots, k\}$. The state ρ_k is called a k-extension of ρ. The main result regarding k-extendible states is the following theorem.

THEOREM 2.10 (not proved here). *A quantum state on $\mathcal{H}_1 \otimes \mathcal{H}_2$ is separable if and only if it is k-extendible for every $k \geqslant 2$.*

The "only if" direction is easy (see Exercise 2.17), while the "if" direction relies on the quantum de Finetti theorem and is beyond the scope of this book.

EXERCISE 2.17. For $k \geqslant 2$, denote by k-Ext the set of k-extendible states on $\mathcal{H}_1 \otimes \mathcal{H}_2$. Show that k-Ext is convex and check the inclusions $\mathrm{Sep} \subset l\text{-Ext} \subset k\text{-Ext}$ for $k \leqslant l$.

EXERCISE 2.18 (2-extendibility of pure states). (i) Let $\rho \in \mathrm{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ be a state such that $\mathrm{Tr}_{\mathcal{H}_2} \rho = |\psi\rangle\langle\psi|$ for some $\psi \in \mathcal{H}_1$. Show that $\rho = |\psi\rangle\langle\psi| \otimes \sigma$ for some $\sigma \in \mathrm{D}(\mathcal{H}_2)$. (ii) Let $\chi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ be a unit vector. Show that $|\chi\rangle\langle\chi|$ is 2-extendible if and only if χ is a product vector.

2.2.5.2. *k-entangled states.* A quantum state on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is said to be *k-entangled* if it can be written as a convex combination

$$\sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$$

where each unit vector $\psi_i \in \mathcal{H}_1 \otimes \mathcal{H}_2$ has Schmidt rank at most k. Note that separable states are exactly 1-entangled states.

2.2.6. Partial transposition. Let $\mathcal{H}$ be a complex Hilbert space, and let (e_j) be an orthonormal basis in $\mathcal{H}$. We can identify $B(\mathcal{H})$ with the set of $n \times n$ matrices by associating a matrix (a_{ij}) with the operator

$$\sum_{i,j} a_{ij} |e_i\rangle\langle e_j|.$$

Once the basis is fixed, it makes sense to consider the transposition $T : B(\mathcal{H}) \to B(\mathcal{H})$ with respect to that basis, defined as

$$T\Big(\sum_{i,j} a_{ij} |e_i\rangle\langle e_j|\Big) = \sum_{i,j} a_{ij} |e_j\rangle\langle e_i|.$$

We will sometimes use the alternative notation $A^T = T(A)$. Note that T is *not* canonical and depends on the choice of the basis in $\mathcal{H}$. The standard usage in linear algebra refers to the transposition with respect to the standard basis $(|j\rangle)_{j=1}^{\dim \mathcal{H}}$.

We now define the *partial transposition*: if $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is a bipartite Hilbert space, and if T denotes the transposition on $B(\mathcal{H}_1)$ (with respect to a specified

basis) and Id is the identity operation of $B(\mathcal{H}_2)$, then the partial transposition (or partial transpose) is the operation

$$\Gamma = T \otimes \mathrm{Id} : B(\mathcal{H}_1 \otimes \mathcal{H}_2) \to B(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

The partial transposition of a state $\rho \in \mathrm{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is denoted by $\rho^\Gamma = \Gamma(\rho)$. What we have defined is actually the partial transposition with respect to the first factor. The partial transposition with respect to the second factor is defined by switching the roles of $\mathcal{H}_1$ and $\mathcal{H}_2$.

Partial transposition applies nicely to states represented as block matrices (see Section 0.7): if $\rho \in \mathrm{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ corresponds to the block operator (A_{ij}), with $A_{ij} \in B(\mathcal{H}_2)$, then ρ^Γ corresponds to the block operator (A_{ji}). Similarly, partial transposition of ρ with respect to the second factor corresponds to the block operator (A_{ij}^T). We illustrate this by computing the partial transposition of the (maximally entangled) Bell state: if $\psi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then (assuming transposition is taken with respect to the canonical basis of $\mathbb{C}^2$)

$$|\psi\rangle\langle\psi| = \frac{1}{2}\left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right], \quad |\psi\rangle\langle\psi|^\Gamma = \frac{1}{2}\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right]. \tag{2.24}$$

As for the usual transposition, the partial transposition depends on a choice of basis. However, we have the following result.

PROPOSITION 2.11. *The eigenvalues of the partial transposition of an operator do not depend on a choice of basis.*

PROOF. Let (e_i) and (e'_i) be two orthonormal bases in $\mathcal{H}_1$, and T and T' denote the transpositions with respect to each basis. Let U be the unitary transformation such that $e'_j = U(e_j)$. We claim that, for every operator $X \in B(\mathcal{H}_1)$,

$$T'(X) = V^\dagger T(X) V, \tag{2.25}$$

where $V = UT(U)$. By linearity, it is enough to check (2.25) when $X = |e'_i\rangle\langle e'_j|$, in which case $T'(X) = |e'_j\rangle\langle e'_i|$. On the other hand, since $X = U|e_i\rangle\langle e_j|U^\dagger$, we then have

$$T(X) = T(U^\dagger)|e_j\rangle\langle e_i|T(U) = T(U^\dagger)U^\dagger|e'_j\rangle\langle e'_i|UT(U) = T(U)^\dagger U^\dagger|e'_j\rangle\langle e'_i|UT(U),$$

as claimed. This shows that the partial transpositions with respect to the two bases are conjugated via the unitary transformation $V \otimes \mathrm{I}$, and the claim follows since unitary conjugation preserves the spectrum. □

Partial transposition naturally extends to the multipartite setting: if $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$, then for any $i \in \{1, \ldots, k\}$ we may define the partial transposition with respect to the ith factor as

$$\Gamma_i \coloneqq \mathrm{Id}_{B(\mathcal{H}_1)} \otimes \cdots \otimes \mathrm{Id}_{B(\mathcal{H}_{i-1})} \otimes T \otimes \mathrm{Id}_{B(\mathcal{H}_{i+1})} \otimes \cdots \otimes \mathrm{Id}_{B(\mathcal{H}_k)}.$$

EXERCISE 2.19 (Eigenvalues of the partial transpose of a pure state). Find all eigenvalues of the partial transpose of a pure state in terms of the Schmidt coefficients of that state.

EXERCISE 2.20 (Partial transpose and the flip operator). Let $\psi = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes e_i$ be a maximally entangled state on $\mathbb{C}^d \otimes \mathbb{C}^d$ and assume that partial transposition is computed with respect to the basis (e_i). Show that $|\psi\rangle\langle\psi|^\Gamma = \frac{1}{d} F$ where $F : x \otimes y \mapsto y \otimes x$ is the flip operator.

EXERCISE 2.21. Find an error in the following argument that purports to mimic the proof of Proposition 2.11 to show that the partial transpose of any state is positive.
If $X \in B^{\mathrm{sa}}(\mathcal{H}_1)$, then $T(X)$ (with respect to some fixed basis) has the same spectrum as X and so there is a unitary operator V such that $T(X) = V^\dagger X V$. This shows that the partial transpose with respect to the same basis is given by conjugation by the unitary transformation $V \otimes \mathrm{I}$. Since such conjugation preserves spectra, it follows that the partial transpose of any state is positive.

2.2.7. PPT states.

DEFINITION 2.12. A state $\rho \in \mathrm{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is said to have a *positive partial transpose* (or to be PPT) if the operator ρ^Γ is positive. We denote by $\mathrm{PPT}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, or simply PPT, the set of PPT states (note that this set is convex).

Proposition 2.11 implies that the definition of PPT states is basis-independent. Similarly, we do not need to specify whether we apply the partial transposition to the first or the second factor; one passes from one to the other by applying the full transposition, which is a spectrum-preserving operation.

Let ρ be a state on $\mathcal{H}_1 \otimes \mathcal{H}_2$. Since the partial transposition preserves the trace, we have $\operatorname{Tr} \rho^\Gamma = 1$, and therefore ρ is PPT if and only if ρ^Γ is a state. Geometrically, the set of PPT states can therefore be described as an intersection

$$\mathrm{PPT} = \mathrm{D} \cap \Gamma(\mathrm{D}). \tag{2.26}$$

The map Γ is a linear map which preserves the Hilbert–Schmidt norm, and therefore behaves as an isometry (see Exercise 2.22). This map is not a canonical object and depends on the choice of a basis. However, the intersection $\mathrm{D} \cap \Gamma(\mathrm{D})$ does not depend on the particular basis used.

The next proposition lies at the root of the relevance of the concept of PPT states to quantum information theory.

PROPOSITION 2.13 (Peres–Horodecki criterion). *Let ρ be a state on $\mathcal{H}_1 \otimes \mathcal{H}_2$. If ρ is separable, then ρ is PPT. In other words, we have the inclusion*

$$\mathrm{Sep}(\mathcal{H}_1 \otimes \mathcal{H}_2) \subset \mathrm{PPT}(\mathcal{H}_1 \otimes \mathcal{H}_2). \tag{2.27}$$

PROOF. Since the set PPT is convex, it suffices to show that the extreme points of $\mathrm{Sep}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ are PPT. The extreme points of $\mathrm{Sep}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ are pure product states, i.e., states of the form

$$\rho = |\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2| = |\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|$$

for unit vectors $\psi_1 \in \mathcal{H}_1, \psi_2 \in \mathcal{H}_2$. The partial transpose of such a state is

$$\rho^\Gamma = |\psi_1\rangle\langle\psi_1|^T \otimes |\psi_2\rangle\langle\psi_2| = |\overline{\psi_1}\rangle\langle\overline{\psi_1}| \otimes |\psi_2\rangle\langle\psi_2|,$$

where $\overline{\psi_1}$ is the vector obtained by applying the complex conjugation to each coordinate of ψ_1. It follows that ρ^Γ is positive, hence ρ is PPT. □

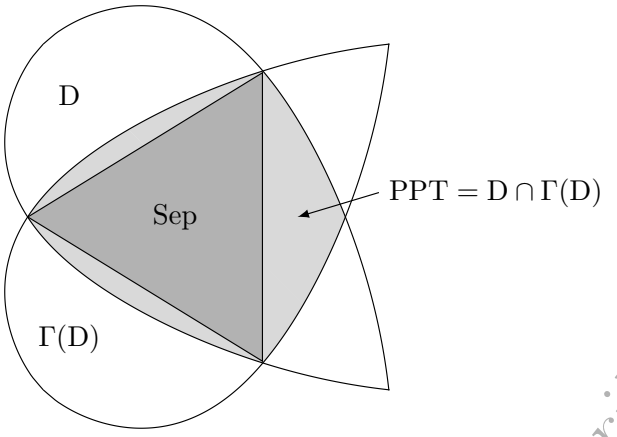

FIGURE 2.2. An illustration of the inclusion Sep $\subset$ PPT $=$ D $\cap$ Γ(D). The inclusion is strict if and only if $\dim \mathcal{H}_1 \dim \mathcal{H}_2 > 6$, see Theorem 2.15. The set Sep is not a polytope, but the set of its extreme points is much "thinner" than those of D and of PPT if the dimension is large.

The Peres–Horodecki criterion (or the PPT criterion) is shown in action in (2.24), where it certifies non-separability of the Bell state: the partial transpose $|\psi\rangle\langle\psi|^\Gamma$ is clearly non-positive. However, positivity of ρ^Γ is, in general, only a necessary condition for separability of ρ as, without additional assumptions, the inclusion (2.27) is strict. Still, there are two important cases where PPT states are guaranteed to be separable: pure states and states in low dimensions, specifically in $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$.

LEMMA 2.14. *A pure state is PPT if and only if it is separable.*

PROOF. Let $\rho = |\psi\rangle\langle\psi|$ be a pure state, and let $\psi = \sum \lambda_i \chi_i \otimes \psi_i$ be a Schmidt decomposition. If we compute the partial transposition with respect to a basis including (χ_i), we obtain

$$\rho^\Gamma = \sum_{i,j} \lambda_i \lambda_j |\chi_i \otimes \psi_j\rangle\langle\chi_j \otimes \psi_i|. \tag{2.28}$$

Suppose there exist two non-zero Schmidt coefficients (say, λ_i and λ_j with $i \neq j$). Then one checks from (2.28) that the restriction of ρ^Γ to $\operatorname{span}\{\chi_i \otimes \psi_j, \chi_j \otimes \psi_i\}$ is not positive. It follows that ρ is PPT if and only if only one Schmidt coefficient of ψ is nonzero, which means that ψ is a product vector and, consequently, ρ is separable. (See Exercise 2.19 for a complete description of the spectrum of ρ^Γ.) $\square$

THEOREM 2.15 (Størmer–Woronowicz theorem, see Section 2.4.5 for the $2 \otimes 2$ case, the $2 \otimes 3$ case is not proved here). *If $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^2$ or $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^3$, then every PPT state on $\mathcal{H}$ is separable.*

Examples of entangled PPT states are known for any other (nontrivial) pairs of dimensions.

Besides pure and low-dimensional states, another family of states for which separability and the PPT property are equivalent are the Werner states. We have

PROPOSITION 2.16 (Separability of Werner states). *For $\lambda \in [0,1]$, let w_λ be the Werner state on $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$ as defined in* (2.21)*. The following are equivalent*
(i) w_λ is separable,
(ii) w_λ is PPT,
(iii) $\operatorname{Tr} w_\lambda F \geqslant 0$,
(iv) $\lambda \geqslant 1/2$.

PROOF. The equivalence (iii) $\iff$ (iv) is a straightforward calculation (we have $\operatorname{Tr} w_\lambda F = 2\lambda - 1$). To show that (ii) $\iff$ (iv), we compute the partial transpose of Werner states in the form (2.22) to obtain (see also Exercise 2.20)

$$w_\lambda^\Gamma = \frac{1}{d^2 - d\alpha}\big(\mathrm{I} - \alpha d |x\rangle\langle x|\big),$$

where x is the maximally entangled vector in the canonical basis $(|i\rangle)_{1\leqslant i\leqslant d}$. It follows that $w_\lambda^\Gamma \geqslant 0 \iff \alpha \leqslant 1/d \iff \lambda \geqslant 1/2$ (see (2.23) for the second equivalence). It remains to prove that (iv) implies (i); since Sep is convex, it is enough to establish that w_1 and $w_{1/2}$ are separable. The separability of $w_1 = \pi_s$ is clear from part (iii) of Exercise 2.16. To show that $w_{1/2}$ is separable, we proceed as follows. For $j \neq k$ and a complex number ξ with modulus one, denote $v^\pm = |j\rangle \pm \xi |k\rangle$. Next, think of ξ as a random variable uniformly distributed on the unit circle. The operator $\mathbf{E}\, |v^+\rangle\langle v^+| \otimes |v^-\rangle\langle v^-|$ belongs to the separable cone $\mathcal{SEP}$. We compute

$$\mathbf{E}\, |v^+v^-\rangle\langle v^+v^-| = |jj\rangle\langle jj| + |kk\rangle\langle kk| + |jk\rangle\langle jk| + |kj\rangle\langle kj| - |jk\rangle\langle kj| - |kj\rangle\langle jk|,$$

where we omitted the symbols $\otimes$ to reduce the clutter. Summing over $j \neq k$, we obtain that

$$A := 2d \sum_j |j\rangle\langle j| \otimes |j\rangle\langle j| + 2 \sum_{j\neq k} |j\rangle\langle j| \otimes |k\rangle\langle k| - 2F \in \mathcal{SEP}.$$

The separability of $w_{1/2}$ follows now from the identity

$$w_{1/2} = \frac{1}{d(d^2-1)}(d\mathrm{I} - F) = \frac{1}{d(d^2-1)}\Big(\frac{A}{2} + (d-1)\sum_{j\neq k} |j\rangle\langle j| \otimes |k\rangle\langle k|\Big),$$

where the first equality is just (2.22) (note that $\lambda = 1/2$ implies $\alpha = 1/d$ by (2.23)). □

EXERCISE 2.22 (Partial transposition as a reflection). Find a subspace $E \subset B^{\mathrm{sa}}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that $\Gamma = 2P_E - \mathrm{Id}$, where P_E denotes the orthogonal projection onto E. Geometrically, Γ identifies with the reflection with respect to E.

EXERCISE 2.23 (Separability of isotropic states). For $-\frac{1}{d^2-1} \leqslant \beta \leqslant 1$, let $\rho_\beta \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ be the isotropic state as defined in (2.20). Show that ρ_β is separable if and only if $\beta \leqslant \frac{1}{d+1}$.

EXERCISE 2.24 (The realignment criterion). The *realignment* $A^R \in B(\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}, \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1})$ of an operator $A \in B(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ is defined as follows: the map $A \mapsto A^R$ is $\mathbb{C}$-linear, and $|ij\rangle\langle kl|^R = |ik\rangle\langle jl|$.
(i) Let $\rho \in \mathrm{D}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ be a separable state. Show that $\|\rho^R\|_1 \leqslant 1$. (The trace norm $\|\cdot\|_1$ is defined in Section 1.3.2).
(ii) Let $\rho \in \mathrm{D}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ be a pure entangled state. Show that $\|\rho^R\|_1 > 1$.
The condition $\|\rho^R\|_1 \leqslant 1$ is usually called the *realignment criterion*. Just as for

the PPT criterion, this is a necessary (but generally not sufficient) condition for separability.

2.2.8. Local unitaries and symmetries of Sep**.** Let us state an analogue of Kadison's theorem (Theorem 2.4), which characterizes affine maps preserving the set Sep. This can be seen as a motivation for the study of partial transposition.

THEOREM 2.17 (not proved here). *Let $\mathcal{H} = \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_k}$ be a multipartite Hilbert space. An affine map $\Phi : B^{\mathrm{sa}}(\mathcal{H}) \to B^{\mathrm{sa}}(\mathcal{H})$ satisfies $\Phi(\mathrm{Sep}) = \mathrm{Sep}$ if and only if it can be written as the composition of maps of the following forms:*

(i) local unitaries

$$\rho \mapsto (U_1 \otimes \cdots \otimes U_k)\rho(U_1 \otimes \cdots \otimes U_k)^\dagger$$

for $U_i \in \mathsf{U}(d_i)$,

(ii) partial transpositions

$$\rho_1 \otimes \cdots \otimes \rho_i \otimes \cdots \otimes \rho_k \mapsto \rho_1 \otimes \cdots \otimes \rho_i^T \otimes \cdots \otimes \rho_k,$$

for some $i \in \{1, \ldots, d\}$,

(iii) swaps

$$\rho_1 \otimes \cdots \otimes \rho_i \otimes \cdots \otimes \rho_j \otimes \cdots \otimes \rho_k \mapsto \rho_1 \otimes \cdots \otimes \rho_j \otimes \cdots \otimes \rho_i \otimes \cdots \otimes \rho_k,$$

for some $i < j$ such that $d_i = d_j$.
All these maps are also isometries with respect to the Hilbert–Schmidt distance.

Although $\mathrm{Sep}(\mathcal{H})$ has a much smaller group of isometries than $\mathrm{D}(\mathcal{H})$, the conclusion of Proposition 2.5 still holds for Sep: the only fixed point is ρ_*. This implies for example that ρ_* is the centroid of Sep.

PROPOSITION 2.18. *Consider $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$, and let $A \in B^{\mathrm{sa}}(\mathcal{H})$ be an operator which is invariant under local unitaries, i.e., such that*

$$A = (U_1 \otimes \cdots \otimes U_k)A(U_1 \otimes \cdots \otimes U_k)^\dagger$$

for any unitary matrices U_i on $\mathcal{H}_i$. Then A is a multiple of identity. In particular, if A is a state, then $A = \rho_*$.

PROOF. We use the following elementary fact: an operator $A_j \in B(\mathcal{H}_j)$ which commutes with any unitary operator actually commutes with any operator and is therefore a multiple of identity. We can write A as a linear combination of product operators

$$A = \sum_i c_i A_1^{(i)} \otimes \cdots \otimes A_k^{(i)},$$

where $A_j^{(i)} \in B^{\mathrm{sa}}(\mathcal{H}_j)$. Let $U = U_1 \otimes \cdots \otimes U_k$, where (U_j) are random unitary matrices, independent and Haar-distributed on the corresponding unitary groups. By the translation-invariance of the Haar measure (see Appendix B.3), the operator $\mathbf{E}\, U_j A_j^{(i)} U_j^\dagger$ commutes with any unitary operator on $\mathcal{H}_j$ and therefore (by the preceding fact) equals $\alpha_{i,j}\, \mathrm{I}_{\mathcal{H}_j}$ for some $\alpha_{i,j} \in \mathbb{R}$. By independence, it follows that

$$\begin{aligned} \mathbf{E}\, UAU^\dagger &= \sum_i c_i\, \mathbf{E}\left(U_1 A_1^{(i)} U_1^\dagger \otimes \cdots \otimes U_k A_k^{(i)} U_k^\dagger\right) \\ &= \sum_i c_i (\mathbf{E}\, U_1 A_1^{(i)} U_1^\dagger) \otimes \cdots \otimes (\mathbf{E}\, U_k A_k^{(i)} U_k^\dagger) \end{aligned}$$

$$= \left(\sum_i c_i \prod_{j=1}^{k} \alpha_{i,j} \right) \mathrm{I}_{\mathcal{H}} .$$

Since $UAU^\dagger = A$, the conclusion follows. □

However, the group of local unitaries does not act irreducibly: there are non-trivial invariant subspaces which are described by the following lemma.

LEMMA 2.19 (not proved here). *Let $\mathcal{H} = \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_k}$ be a multipartite Hilbert space, and*

$$\mathsf{G} = \{U_1 \otimes \cdots \otimes U_k \ : \ U_i \in \mathsf{U}(d_i)\}$$

be the group of local unitaries. For $1 \leqslant i \leqslant k$, write $\mathsf{M}_{d_i}^{\mathrm{sa}} = V_i^1 \oplus V_i^2$, where V_i^1 denotes the hyperplane of trace zero Hermitian matrices, and $V_i^2 = \mathbb{R}\,\mathrm{I}$.

A subspace $E \subset B^{\mathrm{sa}}(\mathcal{H})$ is invariant under G if and only if it can be decomposed as a direct sum of subspaces of the form

$$V_{i_1}^{\alpha_1} \otimes \cdots \otimes V_{i_k}^{\alpha_k}$$

for some choice $(\alpha_1, \ldots, \alpha_k) \in \{1, 2\}^k$.

2.3. Superoperators and quantum channels

We now turn our attention to maps acting between spaces of operators, whence the name *superoperators*. Other terms that will be used to describe these objects are *quantum maps* and *quantum operations*. The crucial observation is that with any such map one can naturally associate usual operators acting on larger Hilbert spaces.

2.3.1. The Choi and Jamiołkowski isomorphisms. As usual, let $\mathcal{H}_1$ and $\mathcal{H}_2$ denote complex (finite-dimensional) Hilbert spaces. Recall (see Sections 0.4 and 0.8) the canonical isomorphisms $(\mathcal{H}_1 \otimes \mathcal{H}_2)^* \leftrightarrow \mathcal{H}_1^* \otimes \mathcal{H}_2^*$ and

$$\mathcal{H}_1^* \otimes \mathcal{H}_2 \leftrightarrow B(\mathcal{H}_1, \mathcal{H}_2). \tag{2.29}$$

It follows that there is a canonical isomorphism

$$B(\mathcal{H}_1, \mathcal{H}_2)^* \leftrightarrow B(\mathcal{H}_2, \mathcal{H}_1).$$

This isomorphism can be seen more concretely via trace duality: a map $S \in B(\mathcal{H}_2, \mathcal{H}_1)$ is identified with the linear form on $B(\mathcal{H}_1, \mathcal{H}_2)$ defined by $T \mapsto \operatorname{Tr} ST$.

By iterating (2.29), we deduce that there is a canonical isomorphism

$$J : B(B(\mathcal{H}_1), B(\mathcal{H}_2)) \longrightarrow B(\mathcal{H}_2 \otimes \mathcal{H}_1)$$

(both spaces being canonically isomorphic to $\mathcal{H}_1 \otimes \mathcal{H}_1^* \otimes \mathcal{H}_2 \otimes \mathcal{H}_2^*$), which is called the *Jamiołkowski isomorphism*. A concrete representation of the Jamiołkowski isomorphism is as follows: fix any basis (e_i) in $\mathcal{H}_1$ and denote by E_{ij} the operator $|e_i\rangle\langle e_j| \in B(\mathcal{H}_1)$. Then J is described as

$$\begin{array}{rccc} J : & B(B(\mathcal{H}_1), B(\mathcal{H}_2)) & \longrightarrow & B(\mathcal{H}_2 \otimes \mathcal{H}_1) \\ & \Phi & \longmapsto & \displaystyle\sum_{i,j} \Phi(E_{ij}) \otimes E_{ji}. \end{array} \tag{2.30}$$

It turns out that there is another related isomorphism, called the *Choi isomorphism*, which is often more useful. Once a basis in $\mathcal{H}_1$ is fixed, the Choi isomorphism is the $\mathbb{C}$-linear bijective map

$$\begin{array}{rccc} C: & B(B(\mathcal{H}_1), B(\mathcal{H}_2)) & \longrightarrow & B(\mathcal{H}_2 \otimes \mathcal{H}_1) \\ & \Phi & \longmapsto & \sum_{i,j} \Phi(E_{ij}) \otimes E_{ij}. \end{array} \tag{2.31}$$

We call $C(\Phi)$ the *Choi matrix* of Φ. Note that the Choi isomorphism is basis-dependent, whereas the Jamiołkowski isomorphism is not. The relation between the isomorphisms J and C is given by the partial transposition: if Γ denotes the partial transposition on $\mathcal{H}_2 \otimes \mathcal{H}_1$ with respect to $\mathcal{H}_1$, then $C = \Gamma \circ J$.

Here is a simple lemma which identifies the elements in $B(B(\mathcal{H}_1), B(\mathcal{H}_2))$ that correspond to rank 1 operators under the Choi isomorphism.

LEMMA 2.20. *Given $A, B \in B(\mathcal{H}_1, \mathcal{H}_2)$, consider the map $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ defined by*

$$\Phi(X) = AXB^\dagger$$

for $X \in B(\mathcal{H}_1)$. Then $C(\Phi) = |a\rangle\langle b|$, where $a = \mathrm{vec}(A)$ and $b = \mathrm{vec}(B)$ are the vectors in $\mathcal{H}_2 \otimes \mathcal{H}_1$ associated to the operators A and B (see Section 0.8). Note also that A has rank 1 if and only if a is a product vector.

PROOF. By $\mathbb{C}$-linearity it is enough to consider $A = |\psi\rangle\langle e_j|$ and $B = |\chi\rangle\langle e_i|$ for some $\psi, \chi \in \mathcal{H}_2$ and some basis vectors $e_i, e_j \in \mathcal{H}_1$. A simple computation shows that then $C(\Phi) = |\psi\rangle\langle\chi| \otimes E_{ij}$, while $a = \psi \otimes e_j$ and $b = \chi \otimes e_i$, and the Lemma follows. □

Finally, let us mention a connection with the notion of realignment defined in Exercise 2.24. If $\Phi : B(\mathbb{C}^{d_1}) \to B(\mathbb{C}^{d_2})$ is a superoperator, the matrix of Φ with respect to the bases $(E_{ij})_{1 \leqslant i,j \leqslant d_1}$ and $(E_{kl})_{1 \leqslant k,l \leqslant d_2}$ is given by the realigned Choi matrix $C(\Phi)^R$.

2.3.2. Positive and completely positive maps. A map $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is called *self-adjointness-preserving* if $\Phi(B^{\mathrm{sa}}(\mathcal{H}_1)) \subset B^{\mathrm{sa}}(\mathcal{H}_2)$. It is easily checked that the following are equivalent:

(1) Φ is self-adjointness-preserving,
(2) $\Phi(X^\dagger) = (\Phi(X))^\dagger$ for any $X \in B(\mathcal{H}_1)$,
(3) $J(\Phi) \in B^{\mathrm{sa}}(\mathcal{H}_2 \otimes \mathcal{H}_1)$,
(4) $C(\Phi) \in B^{\mathrm{sa}}(\mathcal{H}_2 \otimes \mathcal{H}_1)$.

An elegant way to rewrite the definition (2.31) of Choi's matrix is as follows.

$$C(\Phi) = \left(\Phi \otimes \mathrm{Id}_{B(\mathcal{H}_1)}\right)(|\chi\rangle\langle\chi|), \tag{2.32}$$

where $\chi = \sum_i e_i \otimes e_i \in \mathcal{H}_1 \otimes \mathcal{H}_1$ is (a multiple of) a maximally entangled vector. (Recall that we fixed a basis (e_i) in $\mathcal{H}_1$ when defining the Choi isomorphism.) We also note that there is a one-to-one correspondence between

(a) self-adjointness-preserving $\mathbb{C}$-linear maps $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ and
(b) $\mathbb{R}$-linear maps $\Psi : B^{\mathrm{sa}}(\mathcal{H}_1) \to B^{\mathrm{sa}}(\mathcal{H}_2)$.

The correspondence is straightforward: Ψ is obtained from Φ by restriction, whereas Φ is obtained from Ψ by complexification (see Section 0.5).

In the sequel we will occasionally refer to maps of the form $\Phi \otimes \mathrm{Id}_{B(\mathcal{H}_1)}$ as *extensions* of Φ (not to be confused with k-extensions of *states* defined in Section 2.2.5.1). As an example, the partial transposition Γ is an extension of the transposition T.

Throughout this section, we consider a self-adjointness-preserving linear map $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$. The *adjoint* of Φ is the unique map $\Phi^* : B(\mathcal{H}_2) \to B(\mathcal{H}_1)$ such that

$$\mathrm{Tr}(X\Phi(Y)) = \mathrm{Tr}(\Phi^*(X)Y)$$

for any $X \in B(\mathcal{H}_2)$ and $Y \in B(\mathcal{H}_1)$. Note that Φ^* is automatically self-adjointness-preserving if Φ is.

The map Φ is said to be *positivity preserving*—shortened to *positive* when this does not lead to ambiguity—if the image of every positive operator is a positive operator. The map Φ is said to be *n-positive* if $\Phi \otimes \mathrm{Id} : B^{\mathrm{sa}}(\mathcal{H}_1 \otimes \mathbb{C}^n) \to B^{\mathrm{sa}}(\mathcal{H}_2 \otimes \mathbb{C}^n)$ is positive. (Note that n-positivity formally implies k-positivity for any $k < n$.) Finally, the map Φ is said to be *completely positive* if it is n-positive for every integer n. (However, only $n = \min(\dim \mathcal{H}_1, \dim \mathcal{H}_2)$ needs to be checked, see Exercise 2.28.) We denote by $\boldsymbol{CP}(\mathcal{H}_1, \mathcal{H}_2)$ the set of completely positive maps from $B(\mathcal{H}_1)$ to $B(\mathcal{H}_2)$. It is immediate from the definition that $\boldsymbol{CP}(\mathcal{H}_1, \mathcal{H}_2)$ is a convex cone; more about this aspect of the theory in Section 2.4.

The transposition is an example of a map which is positive but not 2-positive; this can be seen, e.g., from (2.24) in Section 2.2.6 or from Exercise 2.32. Here is an important structure theorem concerning completely positive maps.

THEOREM 2.21 (Choi's theorem). *Let $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ be self-adjointness-preserving. The following are equivalent:*

(1) the map Φ is completely positive,
(2) the Choi matrix $C(\Phi)$ is positive semi-definite,
(3) there exist finitely many operators $A_1, \ldots, A_N \in B(\mathcal{H}_1, \mathcal{H}_2)$ such that, for any $X \in B(\mathcal{H}_1)$,

$$\Phi(X) = \sum_{i=1}^{N} A_i X A_i^\dagger. \tag{2.33}$$

A decomposition of Φ in the form (2.33) is called a *Kraus decomposition* of Φ. The smallest integer N such that a Kraus decomposition is possible is called the *Kraus rank* of Φ. As will be clear from the proof, the Kraus rank of Φ is the same as the rank of $C(\Phi)$ in the usual (linear algebra) sense. In particular, it will follow that the Kraus rank of $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is at most $\dim \mathcal{H}_1 \dim \mathcal{H}_2$.

PROOF. It is easily checked that (3) implies (1). The implication (1) $\Rightarrow$ (2) follows from the representation (2.32) of the Choi matrix. We now prove (2) $\Rightarrow$ (3). By the spectral theorem, there exist vectors $a_i \in \mathcal{H}_1 \otimes \mathcal{H}_2$ such that

$$C(\Phi) = \sum_i |a_i\rangle\langle a_i|. \tag{2.34}$$

By Lemma 2.20, $|a_i\rangle\langle a_i|$ is the Choi matrix of the map $X \mapsto A_i X A_i^\dagger$, where $A_i \in B(\mathcal{H}_1, \mathcal{H}_2)$ is associated to a_i via the relation $a_i = \mathrm{vec}(A_i)$. A representation of type (3) follows now from the linearity of the Choi isomorphism. □

There is a simple relation between Kraus decompositions of a completely positive map and of its adjoint: if Φ is given by (2.33), then for any $Y \in B(\mathcal{H}_2)$,

$$\Phi^*(Y) = \sum_{i=1}^{N} A_i^\dagger Y A_i. \tag{2.35}$$

It is clear from the above analysis that Φ^* is completely positive if and only if Φ is. It is also readily checked that Φ^* is positivity-preserving if and only if Φ is; this and related properties are explored in Exercises 2.25–2.33, and discussed in a more general setting in Section 2.4.

EXERCISE 2.25. Let $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ be self-adjointness-preserving. Show that Φ^* is positive if and only if Φ is positive, and that for any n, Φ^* is n-positive if and only if Φ is n-positive.

EXERCISE 2.26. Show that if Φ and Ψ are completely positive, so are $\Phi \otimes \Psi$ and $\Phi \circ \Psi$ (the composition, assuming it is defined).

EXERCISE 2.27. Show that any self-adjointness-preserving map $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is the difference of two completely positive maps.

EXERCISE 2.28. Show that the assertions of Theorem 2.21 are also equivalent to the fact that Φ is n-positive, with $n = \min(\dim \mathcal{H}_1, \dim \mathcal{H}_2)$.

EXERCISE 2.29. Let $k < n$ be integers. Show that the map $\Phi : \mathsf{M}_n \to \mathsf{M}_n$ defined by $\Phi(X) = k \operatorname{Tr}(X) \mathrm{I} - X$ is k-positive but not $(k+1)$-positive.

2.3.3. Quantum channels and Stinespring representation. Consider a self-adjointness-preserving map $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$. We say that Φ is *unital* if $\Phi(\mathrm{I}_{\mathcal{H}_1}) = \mathrm{I}_{\mathcal{H}_2}$. We say that Φ is *trace-preserving* if $\operatorname{Tr} \Phi(X) = \operatorname{Tr} X$ for any $X \in B(\mathcal{H}_1)$. It is easily checked that these properties are dual to each other:

$$\Phi \text{ is unital} \iff \Phi^* \text{ is trace-preserving.} \tag{2.36}$$

We now introduce a fundamental concept in quantum information theory:

DEFINITION 2.22. A *quantum channel* $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is a completely positive and trace-preserving map.

The reasons why we require quantum channels to be positivity- and trace-preserving are clear: since Φ is supposed to represent some physically possible process, we want states to be mapped to states. (The motivation behind the *complete* positivity condition is more subtle; we attempt to explain it in Section 3.5.) A channel that is additionally unital (i.e., if both Φ and Φ^* are channels) is called *doubly stochastic* or *bistochastic*. Clearly, such channels exist only if $\dim \mathcal{H}_1 = \dim \mathcal{H}_2$. (However, see Proposition 2.32 for a notion that makes sense also when $\dim \mathcal{H}_1 \neq \dim \mathcal{H}_2$.)

REMARK 2.23. It follows immediately from the relation (2.33) that the condition $\sum_{i=1}^N A_i A_i^\dagger = \mathrm{I}_{\mathcal{H}_2}$ is equivalent to $\Phi\big(\mathrm{I}_{\mathcal{H}_1}\big) = \mathrm{I}_{\mathcal{H}_2}$, i.e., to Φ being unital. It is less obvious, but easily checked, that $\sum_{i=1}^N A_i^\dagger A_i = \mathrm{I}_{\mathcal{H}_1}$ is equivalent to Φ being trace-preserving. Indeed, if the condition holds, then, for any $\xi \in \mathcal{H}_1$,

$$\operatorname{Tr}(|\xi\rangle\langle\xi|) = \operatorname{Tr}\Big(\sum_{i=1}^N A_i^\dagger A_i |\xi\rangle\langle\xi|\Big) = \operatorname{Tr}\Big(\sum_{i=1}^N A_i |\xi\rangle\langle\xi| A_i^\dagger\Big).$$

In other words, $\operatorname{Tr}\Phi(X) = \operatorname{Tr} X$ if $X = |\xi\rangle\langle\xi|$ and hence, by linearity, for any $X \in B^{\mathrm{sa}}(\mathcal{H}_1)$. Furthermore, the argument is clearly reversible, so we have equivalence.

We now state the Stinespring representation theorem, which plays a fundamental role in understanding the structure of quantum maps.

THEOREM 2.24 (Stinespring theorem). *Let $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ be a completely positive map. Then there exist a finite-dimensional Hilbert space $\mathcal{H}_3$ and an embedding $V : \mathcal{H}_1 \to \mathcal{H}_2 \otimes \mathcal{H}_3$ such that, for any $X \in B(\mathcal{H}_1)$,*

$$\Phi(X) = \operatorname{Tr}_{\mathcal{H}_3} VXV^\dagger. \tag{2.37}$$

Moreover, Φ is a quantum channel if and only if V is an isometry. Conversely, for any isometric embedding V, the map Φ defined via (2.37) is a quantum channel.

The proof shows that the smallest possible dimension for $\mathcal{H}_3$ equals the Kraus rank of Φ; in particular we can require that $\dim(\mathcal{H}_3) \leqslant \dim(\mathcal{H}_1)\dim(\mathcal{H}_2)$.

PROOF. Start from a Kraus decomposition (2.33) for Φ. Set $\mathcal{H}_3 := \mathbb{C}^N$, and let $(|i\rangle)_{1\leqslant i\leqslant N}$ be its canonical basis. Define V by the formula

$$V|\psi\rangle = \sum_{i=1}^N A_i|\psi\rangle \otimes |i\rangle \quad \text{for } \psi \in \mathcal{H}_1. \tag{2.38}$$

We claim that, for any $X \in B(\mathcal{H}_1)$,

$$VXV^\dagger = \sum_{i,j=1}^N A_i X A_j^\dagger \otimes |i\rangle\langle j|.$$

As in Remark 2.23, this follows by linearity from the special case $X = |\psi\rangle\langle\psi|$. This implies the identity (2.37). We also see from (2.38) that $V^\dagger V = \sum_{i=1}^N A_i^\dagger A_i$. By Remark 2.23 it follows that Φ is a quantum channel if and only if $V^\dagger V = \mathrm{I}_{\mathcal{H}_1}$, which is equivalent to V being an isometry. Finally, the last assertion is straightforward: complete positivity follows from (the easy direction of) Choi's Theorem 2.21 and the trace preserving property is immediate. □

When $\mathcal{H}_1 = \mathcal{H}_2$, the Stinespring theorem can be reformulated as follows: any quantum channel can be lifted to a unitary transformation using some ancillary Hilbert space.

THEOREM 2.25. *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ be a quantum channel. Then there exist a finite-dimensional Hilbert space $\mathcal{H}'$, a unit vector $\psi \in \mathcal{H}'$ and a unitary transformation U on $\mathcal{H} \otimes \mathcal{H}'$ such that, for any X in $B(\mathcal{H})$,*

$$\Phi(X) = \operatorname{Tr}_{\mathcal{H}'} U(X \otimes |\psi\rangle\langle\psi|)U^\dagger. \tag{2.39}$$

PROOF. Let $V : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}'$ be given by Theorem 2.24 (with $\mathcal{H}' = \mathcal{H}_3$). Choose any vector $\psi \in \mathcal{H}'$. The map $\varphi \otimes \psi \mapsto V(\varphi)$ (defined on the subspace $\mathcal{H} \otimes \psi \subset \mathcal{H} \otimes \mathcal{H}'$) is an isometry, and therefore can be extended to a unitary U on $\mathcal{H} \otimes \mathcal{H}'$. One checks easily that (2.39) holds. □

We mention in passing that a popular way to quantify how different two quantum channels are is the *diamond norm*. For a self-adjointness-preserving map $\Phi : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$, define

$$\|\Phi\|_\diamond = \sup_{k\in\mathbb{N}} \sup_{\rho\in \mathrm{D}(\mathbb{C}^k)} \|(\Phi \otimes \mathrm{I}_{B(\mathbb{C}^k)})(\rho)\|_1.$$

EXERCISE 2.30. Show that any positive unital map $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ is a contraction with respect to the operator norm $\|\cdot\|_\infty$.

EXERCISE 2.31. Show that any positive trace-preserving map $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ is a contraction with respect to the trace norm $\|\cdot\|_1$ (cf. Proposition 8.4).

EXERCISE 2.32. (i) Let $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ be a trace preserving map. Show that Φ is k-positive if and only if $\Phi \otimes \mathrm{Id} : B^{\mathrm{sa}}(\mathbb{C}^m \otimes \mathbb{C}^k) \to B^{\mathrm{sa}}(\mathbb{C}^n \otimes \mathbb{C}^k)$ is a contraction with respect to the trace norm $\|\cdot\|_1$. (ii) Let $T : \mathsf{M}_n \to \mathsf{M}_n$ be the transposition map. Calculate the norm of $T \otimes \mathrm{Id}$ considered as a map on $\big(B^{\mathrm{sa}}(\mathbb{C}^m \otimes \mathbb{C}^2), \|\cdot\|_1\big)$ and give an example of an operator on which that norm is attained. (iii) Same question for the operator norm $\|\cdot\|_\infty$.

EXERCISE 2.33. Show that any positive, unital, and trace-preserving map $\Phi : \mathsf{M}_n^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ is rank non-decreasing, i.e., $\operatorname{rank} \Phi(\rho) \geqslant \operatorname{rank} \rho$ for any $\rho \in \mathrm{D}(\mathbb{C}^n)$.

2.3.4. Some examples of channels. In this section we list some important classes and examples of quantum channels or, more generally, of superoperators. (Sometimes it is convenient to drop the trace-preserving constraint.)

2.3.4.1. *Unitary channels. Unitary channels* are the completely positive isometries of the set of states identified in Theorem 2.4, i.e., the maps that are of the form $\rho \mapsto U\rho U^\dagger$ for some $U \in \mathsf{U}(d)$.

2.3.4.2. *Mixed-unitary channels.* A *mixed-unitary channel* $\Phi : B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ is a channel which is a convex combination of unitary channels, i.e., is of the form

$$\Phi(\rho) = \sum_{i=1}^{N} \lambda_i U_i \rho U_i^\dagger, \tag{2.40}$$

where (λ_i) is a convex combination and $U_i \in \mathsf{U}(\mathbb{C}^d)$. Such channels are automatically unital. A remarkable fact is that the converse is true when $d = 2$.

PROPOSITION 2.26 (see Exercise 2.34). *Let $\Phi : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ be a unital quantum channel. Then Φ is mixed-unitary.*

EXERCISE 2.34 (Proof of Proposition 2.26). (i) Argue that it is enough to prove Proposition 2.26 for channels which are diagonal with respect to the basis of Pauli matrices (2.2).
(ii) Given real numbers a, b, c, check that the superoperator

$$\frac{1}{2}\big(|\,\mathrm{I}\rangle\langle\mathrm{I}\,| + a|\sigma_x\rangle\langle\sigma_x| + b|\sigma_y\rangle\langle\sigma_y| + c|\sigma_z\rangle\langle\sigma_z|\big)$$

is completely positive if and only if $(a+b)^2 \leqslant (1+c)^2$ and $(a-b)^2 \leqslant (1-c)^2$.
(iii) Rewrite the conditions from part (ii) as a system of four linear inequalities and conclude the proof.

EXERCISE 2.35. Show that any mixed-unitary channel $\Phi : B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ can be expressed as in (2.40) with $N \leqslant d^4 - 2d^2 + 2$. Note that the argument from Exercise 2.34 gives $N \leqslant 4$ (which is optimal) for $d = 2$.

2.3.4.3. *Depolarizing and dephasing channels.* The *completely depolarizing* (or *completely randomizing*) *channel* is the channel $R : B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ defined as $R(X) = \operatorname{Tr} X \frac{\mathrm{I}}{d}$. It maps every state to the maximally mixed state. The completely dephasing channel is the channel $D : B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ that maps any operator to its diagonal part (with respect to a fixed basis).

EXERCISE 2.36 (Depolarizing channels and isotropic states). The family of depolarizing channels is defined as $R_\lambda = \lambda \mathrm{I} + (1-\lambda)R$ for $-\frac{1}{d^2-1} \leqslant \lambda \leqslant 1$. Check that the Choi matrix of Φ_λ is $d\rho_\lambda$, where ρ_λ is the isotropic state defined in (2.20).

EXERCISE 2.37. Show that the completely depolarizing and completely dephasing channels are mixed-unitaries (see also Exercise 8.6).

2.3.4.4. *POVMs, quantum-classical channels.* A *POVM* (Positive Operator-Valued Measure) on $\mathcal{H}$ is a finite family of positive operators $(M_i)_{1\leqslant i\leqslant N}$ with the property that $\sum M_i = \mathrm{I}$. Given a POVM, we can associate to it a quantum channel (called sometimes a quantum-classical or q-c channel) $\Phi : B(\mathcal{H}) \to B(\mathbb{C}^N)$ defined as

$$\Phi(\rho) = \sum_{i=1}^{N} |i\rangle\langle i| \operatorname{Tr}(M_i \rho). \tag{2.41}$$

The dual concept is the notion of a classical-quantum or c-q channel $\Psi : B(\mathbb{C}^N) \to B(\mathcal{H})$. This is a channel of the form

$$\Psi(\rho) = \sum_{i=1}^{N} \rho_i \langle i|\rho|i\rangle,$$

where (ρ_i) are states on $\mathcal{H}$.

EXERCISE 2.38 (Duality between c-q and q-c channels). Let Φ be a q-c channel of the form (2.41). Under what condition on (M_i) is Φ unital? When this condition is satisfied, show that the dual map Φ^* is a c-q channel.

2.3.4.5. *Entanglement-breaking maps.* A map $\Phi \in \boldsymbol{CP}(\mathcal{H}^{in}, \mathcal{H}^{out})$ is said to be *entanglement-breaking* if, for any integer d and for any positive operator $X \in B^{\mathrm{sa}}(\mathcal{H}^{in} \otimes \mathbb{C}^d)$, the operator $(\Phi \otimes \mathrm{Id}_{\mathsf{M}_d})(X)$ belongs to the cone $\mathcal{SEP}(\mathcal{H}^{out} \otimes \mathbb{C}^d)$ of separable operators. Here are equivalent descriptions of entanglement-breaking maps:

LEMMA 2.27 (Characterization of entanglement-breaking maps, see Exercise 2.39). *Let $\Phi : B(\mathcal{H}^{in}) \to B(\mathcal{H}^{out})$ be completely positive. The following are equivalent:*
(i) Φ is entanglement-breaking,
(ii) the Choi matrix $C(\Phi)$ lies in the separable cone $\mathcal{SEP}(\mathcal{H}^{out} \otimes \mathcal{H}^{in})$,
(iii) there is a Kraus decomposition of Φ (2.33) where all the Kraus operators A_i have rank 1.

Entanglement-breaking quantum channels are sometimes called *q-c-q channels*. This reflects the fact that a quantum channel Φ is entanglement-breaking if and only if it can be written as the composition of a q-c channel with a c-q channel.

EXERCISE 2.39. Prove Lemma 2.27.

EXERCISE 2.40 (Once broken, always broken). Let Φ, Ψ be two completely positive maps, with one of them being entanglement-breaking. Show that $(\Phi \otimes \Psi)(X) \in \mathcal{SEP}$ for any positive operator X.

2.3.4.6. *PPT-inducing maps.* A map $\Phi \in \boldsymbol{CP}(\mathcal{H}^{in}, \mathcal{H}^{out})$ is said to be *PPT-inducing* if for any integer d and any positive operator $X \in B^{\mathrm{sa}}(\mathcal{H}^{in} \otimes \mathbb{C}^d)$, the operator $(\Phi \otimes \mathrm{Id}_{\mathsf{M}_d})(X)$ has positive partial transpose.

LEMMA 2.28 (Characterization of PPT-inducing maps, see Exercise 2.41). *A completely positive map Φ is PPT-inducing if and only if $J(\Phi) = C(\Phi)^\Gamma$ is positive semi-definite.*

EXERCISE 2.41. Prove Lemma 2.28.

2.3.4.7. *Schur channels.* Given matrices $A, B \in \mathsf{M}_d$, their Schur product $A \odot B$ is defined as the entrywise product: $(A \odot B)_{ij} = A_{ij}B_{ij}$. Given $A \in \mathsf{M}_d$, the map $\Theta_A : \mathsf{M}_d \to \mathsf{M}_d$ defined as $\Theta_A(X) = A \odot X$ is called a Schur multiplier. When A is positive with $A_{ii} = 1$ for all i, the map Θ_A is a quantum channel called a *Schur channel*.

EXERCISE 2.42 (Positivity of Schur multipliers). Let $A \in \mathsf{M}_d$. Show that the following are equivalent:
(i) A is positive semi-definite,
(ii) Θ_A is positive,
(iii) Θ_A is completely positive.

EXERCISE 2.43 (Kraus decompositions of Schur channels). Let $\Phi : \mathsf{M}_d \to \mathsf{M}_d$ be a quantum channel. Show that Φ is a Schur channel if and only if it admits a Kraus decomposition (2.33) where A_i are diagonal operators.

2.3.4.8. *Separable and LOCC superoperators.* We now assume that $\mathcal{H}^{in}$ and $\mathcal{H}^{out}$ are bipartite spaces, say $\mathcal{H}^{in} = \mathcal{H}_1^{in} \otimes \mathcal{H}_2^{in}$ and $\mathcal{H}^{out} = \mathcal{H}_1^{out} \otimes \mathcal{H}_2^{out}$. A map $\Phi \in \boldsymbol{CP}(\mathcal{H}^{in}, \mathcal{H}^{out})$ is called *separable* if it admits a Kraus decomposition involving product operators, i.e., if there exist operators $A_i^{(1)} : \mathcal{H}_1^{in} \to \mathcal{H}_1^{out}$ and $A_i^{(2)} : \mathcal{H}_2^{in} \to \mathcal{H}_2^{out}$ such that for any $X \in B(\mathcal{H}^{in})$,

$$\Phi(X) = \sum_{i=1}^{N} (A_i^{(1)} \otimes A_i^{(2)}) X (A_i^{(1)} \otimes A_i^{(2)})^\dagger.$$

A widely used class is the class of LOCC channels (LOCC standing for "Local Operations and Classical Communication"). Without defining this class, we simply note that any LOCC channel is separable, and that any convex combination of product channels (of the form $\Phi_1 \otimes \Phi_2$) is an LOCC channel. (Note that these notions *are not* all equivalent, see Exercise 2.44.) More properties of this class will be presented in Section 12.2.

EXERCISE 2.44. Consider the following operators on $\mathbb{C}^2 \otimes \mathbb{C}^2$

$$A_1 = |0\rangle\langle 0| \otimes |0\rangle\langle 0|, A_2 = |0\rangle\langle 0| \otimes |0\rangle\langle 1|, A_3 = |1\rangle\langle 1| \otimes |1\rangle\langle 1|, A_4 = |1\rangle\langle 1| \otimes |1\rangle\langle 0|.$$

Show that the channel on $B(\mathbb{C}^2 \otimes \mathbb{C}^2)$ defined as $\Phi(X) = \sum_{i=1}^4 A_i X A_i^\dagger$ is a separable channel which cannot be written as a convex combination of product channels.

2.3.4.9. *Direct sums.* Let $\Phi_1 : B(\mathcal{H}_1^{in}) \to B(\mathcal{H}_1^{out})$ and $\Phi_2 : B(\mathcal{H}_2^{in}) \to B(\mathcal{H}_2^{out})$ be two quantum channels. Their *direct sum*

$$\Phi_1 \oplus \Phi_2 : B(\mathcal{H}_1^{in} \oplus \mathcal{H}_2^{in}) \to B(\mathcal{H}_1^{out} \oplus \mathcal{H}_2^{out})$$

is the quantum channel defined by its action on block operators as

$$(\Phi_1 \oplus \Phi_2)\left(\begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}\right) = \begin{bmatrix} \Phi_1(X_{11}) & 0 \\ 0 & \Phi_2(X_{22}) \end{bmatrix}. \tag{2.42}$$

EXERCISE 2.45. Describe the Kraus operators of $\Phi_1 \oplus \Phi_2$ in terms of the Kraus operators of Φ_1 and Φ_2.

2.4. Cones of QIT

In this section we will review some of the cones used commonly in quantum information theory. We will distinguish between cones of operators and cones of superoperators, and emphasize the distinction by using two different fonts: $\mathcal{C}$ denotes a generic cone of operators and $\boldsymbol{C}$ a generic cone of superoperators.

2.4.1. Cones of operators. We start by describing some cones of operators and by identifying their bases and their dual cones (Table 2.1). We work in a Hilbert space $\mathcal{H}$ and the corresponding space $B^{\mathrm{sa}}(\mathcal{H})$ of self-adjoint operators. The vector e chosen to define the base in (1.22) is the maximally mixed state. Here and in what follows, we assume that separability and the PPT property are defined with respect to a fixed bipartition $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. However, most considerations extend to multipartite variants and settings allowing flexibility in the choice of the partition. In order lighten the notation, we often write $\mathcal{PSD}$ and $\mathcal{SEP}$ instead of $\mathcal{PSD}(\mathcal{H})$ and $\mathcal{SEP}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ unless this may cause ambiguity.

TABLE 2.1. List of cones of operators. All cones live in $B^{\mathrm{sa}}(\mathcal{H})$, the space of self-adjoint operators on a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ with dimension $n = \dim \mathcal{H}$. The base is taken with respect to the distinguished vector $e = \mathrm{I}/n$. The cones $\mathcal{C}$ are listed in the decreasing order (with respect to inclusion) from top to bottom and, consequently, the dual cones $\mathcal{C}^*$ are in the increasing order from top to bottom. Most inclusions/duality relations are straightforward and/or were pointed out earlier in this chapter; the remaining few are clarified in this subsection.

Cone of operators $\mathcal{C}$		base $\mathcal{C}^{\mathrm{b}}$	dual cone $\mathcal{C}^*$
Block-positive	$\mathcal{BP}$	BP	$\mathcal{SEP}$
Decomposable	co-$\mathcal{PSD} + \mathcal{PSD}$	$\mathrm{conv}(\mathrm{D} \cup \Gamma(\mathrm{D}))$	$\mathcal{PPT}$
Positive	$\mathcal{PSD}$	D	$\mathcal{PSD}$
Pos. partial transpose	$\mathcal{PPT}$	PPT	co-$\mathcal{PSD} + \mathcal{PSD}$
Separable	$\mathcal{SEP}$	Sep	$\mathcal{BP}$

In the same way that $\mathcal{PSD}$ is associated with its base D, the set of separable states Sep gives rise to the separable cone $\mathcal{SEP}$, and the set PPT of states with positive partial transpose leads to the $\mathcal{PPT}$ cone. Another example is the cone of k-entangled matrices (cf. Section 2.2.5). In general, whenever a definition of a set of matrices involves linear matrix inequalities and a trace constraint, dropping that constraint gives us a cone. When the original set of matrices is compact, the resulting cone is pointed, with the hyperplane of trace zero matrices isolating 0 as an exposed point (cf. Corollary 1.8). All the cones cataloged in this section have this property and are in fact nondegenerate.

One more convenient concept is that of co-$\mathcal{PSD}$ matrices

$$\text{co-}\mathcal{PSD} := \Gamma(\mathcal{PSD}) = \{\rho \in \mathsf{M}_n^{\text{sa}} : \rho^\Gamma \in \mathcal{PSD}\} \tag{2.43}$$

where Γ is the partial transpose defined in Section 2.2.6. It allows a compact description of the cone dual to $\mathcal{PPT}$: since $\mathcal{PPT} = \text{co-}\mathcal{PSD} \cap \mathcal{PSD}$, it follows from (1.20) (see also Exercise (1.36)) that

$$\mathcal{PPT}^* = \text{co-}\mathcal{PSD} + \mathcal{PSD}, \tag{2.44}$$

the cone of *decomposable* matrices. Note that, except in trivial cases, this cone is strictly larger than $\mathcal{PSD}$ and so its base contains matrices that are not states.

To conclude the review of the standard cones, we will identify the cone $\mathcal{SEP}^*$. To that end, it is convenient to think of operators on a composite Hilbert space $\mathbb{C}^m \otimes \mathbb{C}^n$ as *block matrices* $M = (M_{jk})_{j,k=1}^m$, where $M_{jk} \in \mathsf{M}_n$ (see Section 0.7). Since the extreme rays of $\mathcal{SEP}$ are generated by pure separable states $|\xi\otimes\eta\rangle\langle\xi\otimes\eta|$ (see Section 2.2.3), we have

$$M \in \mathcal{SEP}^* \iff \forall \xi \in \mathbb{C}^m,\ \forall \eta \in \mathbb{C}^n,\ \operatorname{Tr}\big(M|\xi\otimes\eta\rangle\langle\xi\otimes\eta|\big) \geqslant 0 \tag{2.45}$$

$$\iff \forall \xi \in \mathbb{C}^m,\ \sum_{j,k=1}^m \xi_j\overline{\xi_k} M_{jk} \in \mathcal{PSD}(\mathbb{C}^n). \tag{2.46}$$

The condition in (2.46) is usually referred to as $M = (M_{jk})$ being *block-positive*. (We note that the definition treats m and n symmetrically, even though this not apparent in (2.46).) In other words, the dual to the cone of separable matrices is that of block-positive matrices, denoted by $\mathcal{BP}$. As a consequence, the polar of Sep can be identified: we obtain from Lemma 1.6 that

$$\text{Sep}^\circ = -d^2\text{BP}, \tag{2.47}$$

where BP denotes the set of block-positive matrices with unit trace and the minus sign stands for the point reflection with respect to the appropriately normalized identity matrix.

2.4.2. Cones of superoperators. We next turn our attention to the classes of superoperators considered in Section 2.3.2. We consider superoperators acting from $B^{\text{sa}}(\mathcal{H})$ to $B^{\text{sa}}(\mathcal{K})$ and denote the corresponding cones as $\boldsymbol{C}(\mathcal{H},\mathcal{K})$, or as $\boldsymbol{C}(\mathcal{H})$ when $\mathcal{H} = \mathcal{K}$, or simply as $\boldsymbol{C}$ when there is no ambiguity. The cones we consider most frequently are gathered in Table 2.2. (See Exercise 2.48 for a discussion of identification and duality relations for k-positive superoperators and k-entangled states.)

In the language of cones, a positivity-preserving superoperator $\Phi : B^{\text{sa}}(\mathcal{H}) \to B^{\text{sa}}(\mathcal{K})$ may be defined via the condition $\Phi\big(\mathcal{PSD}(\mathcal{H})\big) \subset \mathcal{PSD}(\mathcal{K})$. It is readily seen that the set of positivity-preserving maps is itself a cone (which we will denote by $\boldsymbol{P}(\mathcal{H},\mathcal{K})$) in the space $B\big(B^{\text{sa}}(\mathcal{H}), B^{\text{sa}}(\mathcal{K})\big)$.

As was noted in Section 2.3.2, $\Phi \in \boldsymbol{P}(\mathcal{H},\mathcal{K})$ iff $\Phi^* \in \boldsymbol{P}(\mathcal{K},\mathcal{H})$. As we shall see, it would be erroneous to take this to mean that $\boldsymbol{P}$ is self-dual. Instead, this is a special case of a very general elementary fact: *If V_1, V_2 are vector spaces, if $\mathcal{C}_1 \subset V_1$, $\mathcal{C}_2 \subset V_2$ are closed convex cones, and if $\Phi : V_1 \to V_2$ is linear, then $\Phi(\mathcal{C}_1) \subset \mathcal{C}_2$ iff $\Phi^*(\mathcal{C}_2^*) \subset \mathcal{C}_1^*$.*

The most important cone of superoperators is arguably that of completely positive maps, denoted by $\boldsymbol{CP}$. By Choi's Theorem 2.21, $\Phi \in \boldsymbol{CP}$ iff the Choi matrix $C(\Phi)$ is positive semi-definite. In other words, $\boldsymbol{CP}\big(\mathbb{C}^m,\mathbb{C}^n\big)$ is isomorphic to

TABLE 2.2. Cones of superoperators. To each cone $\boldsymbol{C}$ from the first (double) column we associate a cone $\mathcal{C}$ which consists of Choi matrices of elements from $\boldsymbol{C}$. They are connected by the relation $\Phi \in \boldsymbol{C} \iff C(\Phi) \in \mathcal{C}$. We note that $\boldsymbol{C}$ is a subset of $B(B^{\mathrm{sa}}(\mathcal{H}), B^{\mathrm{sa}}(\mathcal{K}))$ while $\mathcal{C}$ is a subset of $B^{\mathrm{sa}}(\mathcal{K} \otimes \mathcal{H})$. The cones $\boldsymbol{C}$ and $\mathcal{C}$ are in decreasing order from top to bottom and the dual cones $\mathcal{C}^*$ and $\boldsymbol{C}^*$ are in increasing order from top to bottom.

Cone of superoperators $\boldsymbol{C}$		$\mathcal{C}$	$\mathcal{C}^*$	$\boldsymbol{C}^*$
Positivity-preserving	$\boldsymbol{P}$	$\mathcal{BP}$	$\mathcal{SEP}$	$\boldsymbol{EB}$
Decomposable	$\boldsymbol{DEC}$	co-$\mathcal{PSD} + \mathcal{PSD}$	$\mathcal{PPT}$	$\boldsymbol{PPT}$
Completely positive	$\boldsymbol{CP}$	$\mathcal{PSD}$	$\mathcal{PSD}$	$\boldsymbol{CP}$
PPT-inducing	$\boldsymbol{PPT}$	$\mathcal{PPT}$	co-$\mathcal{PSD} + \mathcal{PSD}$	$\boldsymbol{DEC}$
Entanglement-breaking	$\boldsymbol{EB}$	$\mathcal{SEP}$	$\mathcal{BP}$	$\boldsymbol{P}$

$\mathcal{PSD}(\mathbb{C}^n \otimes \mathbb{C}^m)$. This means that—with proper identifications, see Exercise 2.47—the cone $\boldsymbol{CP}$ is self-dual. Choi's correspondence $\Phi \mapsto C(\Phi)$ relates similarly the cone $\boldsymbol{EB}(\mathbb{C}^m, \mathbb{C}^n)$ of entanglement-breaking maps from $\mathsf{M}_m^{\mathrm{sa}}$ to $\mathsf{M}_n^{\mathrm{sa}}$ to $\mathcal{SEP}\big(\mathbb{C}^n \otimes \mathbb{C}^m\big)$, as well as the cone $\boldsymbol{PPT}(\mathbb{C}^m, \mathbb{C}^n)$ of PPT-inducing maps to $\mathcal{PPT}(\mathbb{C}^n \otimes \mathbb{C}^m)$.

A map $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ is said to be *co-completely positive* if $C(\Phi) \in$ co-$\mathcal{PSD}$. Similarly, one says that Φ is *decomposable* if it can be represented as a sum of a completely positive map and a co-completely positive map. It follows that the correspondence $\Phi \mapsto C(\Phi)$ relates the cone $\boldsymbol{DEC}(\mathbb{C}^n, \mathbb{C}^m)$ of decomposable maps to the cone of decomposable matrices.

Interestingly, $\mathcal{SEP}(\mathbb{C}^n \otimes \mathbb{C}^m)^*$ identifies with $\boldsymbol{P}(\mathbb{C}^m, \mathbb{C}^n)$. This last identification is in fact easy to see directly from (2.45)–(2.46). Indeed, $C(\Phi) = (M_{jk})$ means that $M_{jk} = \Phi(|e_j\rangle\langle e_k|)$ and hence if $\xi = (\xi_j)_{j=1}^m \in \mathbb{C}^m$, then $\Phi(|\xi\rangle\langle\xi|) = \sum_{j,k=1}^m \xi_j \overline{\xi_k} M_{jk}$. Consequently,

$$\begin{aligned} C(\Phi) \in \mathcal{SEP}(\mathbb{C}^n \otimes \mathbb{C}^m)^* &\iff \Phi(|\xi\rangle\langle\xi|) \in \mathcal{PSD}(\mathbb{C}^n) \ \text{ for } \ \xi \in \mathbb{C}^m \\ &\iff \Phi \in \boldsymbol{P}, \end{aligned}$$

which is the claimed identification. The first equivalence is simply (2.45)–(2.46) for the choice $M = C(\Phi)$, whereas the second one reflects the fact that the property of "preserving positivity" needs to be checked only on the extreme rays of the $\mathcal{PSD}$ cone, i.e., on operators of the form $|\xi\rangle\langle\xi|$. (See Section 1.2.2 and particularly Corollary 1.10.)

EXERCISE 2.46 (Composition rules for maps). Show that a composition of two co-completely positive maps is completely positive. Similarly, show that a composition of a co-completely positive map and a completely positive map is co-completely positive.

EXERCISE 2.47 (The completely positive cone is self-dual). Show that

$$\boldsymbol{CP}(\mathbb{C}^n, \mathbb{C}^m) = \{\Psi \in B(\mathsf{M}_n^{\mathrm{sa}}, \mathsf{M}_m^{\mathrm{sa}}) \ : \ \mathbf{Tr}(\Psi \circ \Phi) \geqslant 0 \ \ \forall \Phi \in \boldsymbol{CP}(\mathbb{C}^m, \mathbb{C}^n)\},$$

where $\mathbf{Tr}$ denotes the trace on $B(\mathsf{M}_n^{\mathrm{sa}})$.

EXERCISE 2.48 (k-positive superoperators and k-entangled states). Let $1 \leqslant k \leqslant \min(m, n)$ and $\Phi : \mathsf{M}_n \to \mathsf{M}_m$ be self-adjointness-preserving. Show that the

following are equivalent
(1) Φ is k-positive,
(2) for every $x \in \mathbb{C}^m \otimes \mathbb{C}^n$ with Schmidt rank at most k, we have $\langle x|C(\Phi)|x\rangle \geqslant 0$,
(3) for every $A \in \mathsf{M}_{k,m}$ and $B \in \mathsf{M}_{k,n}$, the operator $(A\otimes B)^\dagger C(\Phi)(A\otimes B)$ is positive.
In words, the cone of Choi matrices of k-positive superoperators is dual to the cone generated by the set of k-entangled states (as defined in Section 2.2.5).

2.4.3. Symmetries of the $\mathcal{PSD}$ cone. The results of Sections 2.1.4 allow us to deduce a description of the groups of affine automorphisms of some of the cones cataloged in the present section. The argument is based on the following two simple observations: first, since affine automorphisms preserve facial structure, and since 0 is the only extreme point of all the cones considered above, any affine automorphism must be linear. Next, if $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ is such that $A = \Phi(\mathrm{I})$ is positive definite, then Ψ defined by $\Psi(\rho) = A^{-1/2}\Phi(\rho)A^{-1/2}$ is unital, and its adjoint, Ψ^*, is trace-preserving (see (2.36)). This often allows to reduce the analysis of general maps to that of unital or trace-preserving maps. As an example of such reduction we will prove the following statement.

Proposition 2.29 (Characterization of automorphisms of the $\mathcal{PSD}$ cone). *Let $\Phi : \mathsf{M}_n^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ be an affine map which satisfies $\Phi(\mathcal{PSD}(\mathbb{C}^n)) = \mathcal{PSD}(\mathbb{C}^n)$. Then Φ is a linear automorphism of $\mathcal{PSD}(\mathbb{C}^n)$ and is of one of two possible forms: $\Phi(\rho) = V\rho V^\dagger$ or $\Phi(\rho) = V\rho^T V^\dagger$, for some $V \in \mathsf{GL}(n,\mathbb{C})$. In the first case Φ is completely positive, whereas in the second case Φ is co-completely positive.*

Proof. Since $\operatorname{rank}\Phi \geqslant \dim \mathcal{PSD}(\mathbb{C}^n) = \dim \mathsf{M}_n^{\mathrm{sa}}$, it follows that Φ is surjective and hence injective, so it is indeed an automorphism of $\mathcal{PSD}(\mathbb{C}^n)$ (and, consequently, so is Φ^{-1}). By the earlier remark, Φ must be linear. Since the adjoint of a positive map is positive (see Section 2.3.2), it follows that Φ^* and $(\Phi^*)^{-1} = (\Phi^{-1})^*$ are positive. Hence they are both automorphisms of $\mathcal{PSD}(\mathbb{C}^n)$. Let $A = \Phi^*(\mathrm{I}) \in \mathcal{PSD}(\mathbb{C}^n)$. We claim that A belongs to the interior of $\mathcal{PSD}(\mathbb{C}^n)$ and, consequently, is positive definite (and invertible). This follows from topological considerations, but can also be deduced from Proposition 1.4: if $A = \Phi^*(\mathrm{I})$ lay on the boundary of $\mathcal{PSD}(\mathbb{C}^n)$, we would have $A \in F$ for some face of $\mathcal{PSD}(\mathbb{C}^n)$, which would imply $\Phi^*(\mathcal{PSD}(\mathbb{C}^n)) \subset F$, contradicting injectivity of Φ^*. Having established the claim, we set $\Psi(\sigma) = A^{-1/2}\Phi^*(\sigma)A^{-1/2}$, so that Ψ is a unital automorphism of $\mathcal{PSD}(\mathbb{C}^n)$. Consequently, Ψ^* is a trace-preserving automorphism of $\mathcal{PSD}(\mathbb{C}^n)$, which is only possible if $\Psi^*(\mathrm{D}) = \mathrm{D}$. It now follows from Kadison's Theorem 2.4 that, for some $U \in \mathsf{U}(n)$, either (i) $\Psi^*(\tau) = U\tau U^\dagger$ or (ii) $\Psi^*(\tau) = U\tau^T U^\dagger$ (for all $\tau \in \mathsf{M}_n^{\mathrm{sa}}$). The rest of the argument is just bookkeeping. First, the definition of Ψ—and that of an adjoint map—imply that Ψ^* is given by the formula $\Psi^*(\tau) = \Phi(A^{-1/2}\tau A^{-1/2})$. In case (i), this shows that $\Phi(A^{-1/2}\tau A^{-1/2}) = U\tau U^\dagger$ or, substituting $\rho = A^{-1/2}\tau A^{-1/2}$, $\Phi(\rho) = UA^{1/2}\rho A^{1/2}U^\dagger = V\rho V^\dagger$, where $V = UA^{1/2}$, as needed. The fact that Φ is then completely positive is the easy implication of Choi's Theorem 2.21. Case (ii) is handled in the same way. □

We have an immediate

Corollary 2.30. *Completely positive automorphisms of the cone $\mathcal{PSD}(\mathbb{C}^n)$, all of which are of the form $\Phi_V(\rho) = V\rho V^\dagger$ for some $V \in \mathsf{GL}(n,\mathbb{C})$, act transitively on the interior of that cone.*

For future reference, we state here a slightly more general form of the principle that is implicit in the proof of Proposition 2.29.

LEMMA 2.31. *If $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ is a positivity-preserving linear map such that $A = \Phi(\mathrm{I})$ is positive definite, then $\tilde{\Phi}$ defined by $\tilde{\Phi}(\rho) = A^{-1/2}\Phi(\rho)A^{-1/2}$ is unital and positivity-preserving. Similarly, if Ψ is a positivity-preserving linear map such that $\Psi(\rho) \neq 0$ for $\rho \in \mathcal{PSD}(\mathbb{C}^m)\backslash\{0\}$, then $\tilde{\Psi}(\rho) = \Psi(B^{-1/2}\rho B^{-1/2})$ is trace-preserving and positivity-preserving, where $B = \Psi^*(\mathrm{I})$ (necessarily positive definite).*

We emphasize that the map Φ in Lemma 2.31 is not assumed to be an automorphism of the $\mathcal{PSD}$ cone (as was the case in Proposition 2.29), only positivity-preserving. Moreover, we also allow the dimensions in the domain and in the range to be different. Finally, recall that, by Lemma 1.7, the properties "$\Phi(\mathrm{I})$ is positive definite" and "$\Psi(\rho) \neq 0$ for $\rho \in \mathcal{PSD}(\mathbb{C}^m)\backslash\{0\}$" are dual to each other.

In view of the above result, it is natural to wonder when a positivity-preserving map is equivalent, in the sense of Lemma 2.31, to a map which is *both* unital and trace-preserving. (Of course if the dimensions in the domain and in the range are different, this is only possible if we use the normalized trace or, alternatively, if we ask that the maximally mixed state be mapped to the maximally mixed state.) It turns out that this can be ensured if just a little more regularity is assumed. (See Exercise 2.52 for examples exploring the necessity of the stronger hypothesis.) We have

PROPOSITION 2.32 (Sinkhorn's normal form for positive maps). *Let $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ be a linear map which belongs to the interior of $\boldsymbol{P}$, the cone of positivity-preserving maps. Then there exist positive operators $A \in \mathcal{PSD}(\mathbb{C}^n)$ and $B \in \mathcal{PSD}(\mathbb{C}^m)$ such that the map $\tilde{\Phi}(\rho) = A\Phi(B\rho B)A$ is trace-preserving and maps the maximally mixed state to the maximally mixed state (and is necessarily positivity-preserving).*

PROOF. Let us first focus on the case $m = n$. Given positive definite A, B, let $\tilde{\Phi}$ be given by the formula from the Proposition. Then

$$\tilde{\Phi} \text{ is unital } \Leftrightarrow A\Phi(B^2)A = \mathrm{I} \Leftrightarrow \Phi(B^2) = A^{-2} \Leftrightarrow \Phi(B^2)^{-1} = A^2. \tag{2.48}$$

We next note that, in the notation of Corollary 2.30, $\tilde{\Phi} = \Phi_A \circ \Phi \circ \Phi_B$ and so $\tilde{\Phi}^* = \Phi_B \circ \Phi^* \circ \Phi_A$ (this uses the identity $\Phi_M^* = \Phi_M$, valid when M is self-adjoint). Accordingly, by (2.36),

$$\tilde{\Phi} \text{ is trace-preserving } \Leftrightarrow \tilde{\Phi}^* \text{ is unital } \Leftrightarrow B\Phi^*(A^2)B = \mathrm{I} \Leftrightarrow \Phi^*(A^2) = B^{-2}. \tag{2.49}$$

Solving the last equation in (2.49) for B^2 and substituting it in (2.48) we are led to a system of equations

$$B^2 = \Phi^*(A^2)^{-1} \quad \text{and} \quad \Phi\big(\Phi^*(A^2)^{-1}\big)^{-1} = A^2. \tag{2.50}$$

The second equation in (2.50) says that $S = A^2$ is a fixed point of the function

$$S \mapsto f(S) := \Phi\big(\Phi^*(S)^{-1}\big)^{-1}. \tag{2.51}$$

Conversely, if S is a positive definite fixed point of f, then $A = S^{1/2}$ and $B = \Phi^*(A^2)^{-1/2}$ (i.e., B defined so that the first equation in (2.50) holds) satisfy (2.48) and (2.49) and yield $\tilde{\Phi}$ that is unital and trace-preserving. (The hypothesis "Φ

belongs to the interior of $\boldsymbol{P}$" guarantees that all the inverses and negative powers above make sense, and that f is well-defined and continuous on $\mathcal{PSD}\backslash\{0\}$, see Exercises 2.50 and 2.51.)

To find a fixed point of f we want to use Brouwer's fixed-point theorem, which requires a (continuous) function that is a self-map of a compact convex set. One way to arrive at such setting is to consider $f_1 : \mathrm{D}(\mathbb{C}^n) \to \mathrm{D}(\mathbb{C}^n)$ defined by

$$f_1(\sigma) = \frac{f(\sigma)}{\operatorname{Tr} f(\sigma)}. \tag{2.52}$$

It then follows that there is $\sigma_0 \in D(\mathbb{C}^n)$ such that $f_1(\sigma_0) = \sigma_0$ and hence $f(\sigma_0) = t\sigma_0$, where $t = \operatorname{Tr} f(\sigma_0) > 0$. The final step is to note that if we choose, as before, $A = \sigma_0^{1/2}$ and $B = \Phi^*(A^2)^{-1/2}$, then the corresponding $\tilde{\Phi}$ is trace-preserving and satisfies $\tilde{\Phi}(\mathrm{I}) = t^{-1}\,\mathrm{I}$. If $m = n$, this is only possible if $t = 1$. In other words, σ_0 is a fixed point of f that we needed in order to conclude the argument. In the general case, the same argument yields $t = n/m$, which translates to $\tilde{\Phi}(\mathrm{I}/m) = \mathrm{I}/n$, again as needed. □

Exercise 2.49. Show that $\Phi \in \boldsymbol{P}(\mathbb{C}^n)$ is an automorphism of $\mathcal{PSD}(\mathbb{C}^n)$ if an only if it is rank-preserving.

Exercise 2.50 (Descriptions of the interior of the positive cone). Show that Φ belongs to the interior of $\boldsymbol{P}(\mathbb{C}^n)$ iff Φ maps $\mathcal{PSD}(\mathbb{C}^n)\backslash\{0\}$ to the interior of $\mathcal{PSD}(\mathbb{C}^n)$ iff there exists $\delta > 0$ such that $\Phi(\rho) \geqslant \delta(\operatorname{Tr}\rho)\,\mathrm{I}$ for all $\rho \in \mathcal{PSD}$.

Exercise 2.51 (Interior of the positive cone is self-dual). Show that Φ verifies $\Phi(\rho) \geqslant \delta(\operatorname{Tr}\rho)\,\mathrm{I}$ (for all $\rho \in \mathcal{PSD}$) iff Φ^* does.

Exercise 2.52 (Discussion of the necessity of the hypothesis of Proposition 2.32). Give examples of $\Phi, \Psi \in \boldsymbol{P}(\mathbb{C}^2)$ such that (a) $\Phi(\mathrm{I})$ and $\Phi^*(\mathrm{I})$ are positive definite, but Φ is not equivalent (in the sense of Proposition 2.32) to a unital, trace-preserving map, and (b) Ψ is unital and trace-preserving, but $\Psi \in \partial\boldsymbol{P}$.

Exercise 2.53 (Rank nondecreasing and Sinkhorn's normal form). Give an example of map $\Phi \in \boldsymbol{P}(\mathbb{C}^2, \mathbb{C}^2)$ which is rank nondecreasing (i.e., verifies $\operatorname{rank}\Phi(\rho) \geqslant \operatorname{rank}\rho$ for any $\rho \in \mathrm{D}(\mathbb{C}^2)$), but which does not satisfy the conclusion of Proposition 2.32.

2.4.4. Entanglement witnesses. The formalism of cones and their duality allows us to conveniently discuss the concept of *entanglement witnesses*. We start with the following simple observation, which is a direct consequence of the identifications of the dual cone $\mathcal{SEP}^*$ as $\mathcal{BP}$ (see Table 2.1 in Section 2.4), and of the corresponding cone of superoperators as $\boldsymbol{P}$ (Table 2.2).

Proposition 2.33 (Entanglement witnesses, take #1). *Let $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$ and let ρ be a state on $\mathcal{H}$. Then the following conditions are equivalent:*
(i) ρ is entangled,
(ii) there exists $\sigma \in \mathcal{SEP}(\mathcal{H})^* = \mathcal{BP}$ such that $\langle\sigma, \rho\rangle_{\mathrm{HS}} = \operatorname{Tr}(\sigma\rho) < 0$,
(iii) there exists a positivity-preserving linear map $\Psi : \mathsf{M}_n^{\mathrm{sa}} \to \mathsf{M}_m^{\mathrm{sa}}$ such that $\operatorname{Tr}(C(\Psi)\rho) < 0$.

The next result is a simple corollary of the above observation, but it goes well beyond a straightforward reformulation.

THEOREM 2.34 (Horodecki's entanglement witness theorem). *Let $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$ and let ρ be a state on $\mathcal{H}$. Then ρ is entangled iff there exists a positivity-preserving map $\Phi : \mathsf{M}_m^{\mathrm{sa}} \to \mathsf{M}_n^{\mathrm{sa}}$ such that the operator $(\Phi \otimes \mathrm{Id}_{\mathsf{M}_n^{\mathrm{sa}}})\rho$ is not positive semi-definite.*

In the setting of Proposition 2.33 and Theorem 2.34, the operator σ or the map Φ are said to witness the entanglement present in ρ, hence the term "entanglement witnesses."

PROOF OF THEOREM 2.34. The sufficiency is obvious: if $\rho = \tau \otimes \tau'$ is a product state and Φ is positivity-preserving, then $(\Phi \otimes \mathrm{Id})\rho = \Phi(\tau) \otimes \tau'$, which is clearly positive; the case of convex combinations of product states easily follows. To show necessity, let $\Psi : \mathsf{M}_n^{\mathrm{sa}} \to \mathsf{M}_m^{\mathrm{sa}}$ be the positivity-preserving map given by Proposition 2.33. If $\chi \in \mathbb{C}^n \otimes \mathbb{C}^n$ is the maximally entangled vector as in (2.32), then

$$\begin{aligned} 0 &> \mathrm{Tr}(C(\Psi)\rho) = \langle C(\Psi), \rho \rangle_{\mathrm{HS}} = \langle (\Psi \otimes \mathrm{Id}_{\mathsf{M}_n^{\mathrm{sa}}})|\chi\rangle\langle\chi|, \rho \rangle_{\mathrm{HS}} \\ &= \langle |\chi\rangle\langle\chi|, (\Psi^* \otimes \mathrm{Id}_{\mathsf{M}_n^{\mathrm{sa}}})\rho \rangle_{\mathrm{HS}} = \langle \chi | (\Psi^* \otimes \mathrm{Id}_{\mathsf{M}_n^{\mathrm{sa}}})\rho | \chi \rangle, \end{aligned}$$

which implies that $\big(\Psi^* \otimes \mathrm{Id}_{\mathsf{M}_n^{\mathrm{sa}}}\big)\rho$ is not positive. Given that Ψ^* is positivity-preserving if and only if Ψ is (see Section 2.3.2), the choice of $\Phi = \Psi^*$ works as needed. □

REMARK 2.35. It follows from general considerations that the entanglement witnesses σ, Φ may be required to satisfy various additional properties. First, one may include a normalizing condition such as $\mathrm{Tr}\,\sigma = 1$ or $\mathrm{Tr}\,\Phi(\mathrm{I}) = 1$, which reduces the search for a witness to a convex compact set. Next, since linear functions (restricted to compact sets) attain extreme values on extreme points, one may insist that σ or Φ belong to an extreme ray of the respective cone (or even, by a density argument, to an exposed ray; cf. Exercise 1.5). Finally, another acceptable normalizing condition is to require that Φ be unital or trace-preserving. To see that Φ can be assumed unital, we note first that by a density argument the operator $\Phi(\mathrm{I})$ may be assumed to be positive definite, in which case Lemma 2.31 applies. The case of the trace-preserving restriction is slightly more involved and requires increasing the dimension of the range of Φ. We relegate the details of the arguments to Exercises 2.54 and 2.55.

EXERCISE 2.54 (Unital witnesses suffice). Show that in Theorem 2.34 one can require that Φ be unital.

EXERCISE 2.55 (Trace-preserving witnesses suffice). Show that in Theorem 2.34 one can require that Φ be trace-preserving, at the cost of allowing the range of Φ to be $\mathsf{M}_{m+n}^{\mathrm{sa}}$.

EXERCISE 2.56 (Optimal entanglement witnesses). We work in the Hilbert space $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$. For $\sigma \in \mathcal{BP}$, we denote by $\mathrm{E}(\sigma) = \{\rho \in \mathrm{D} \ : \ \mathrm{Tr}(\rho\sigma) < 0\}$ the set of states detected to be entangled by σ. We say that σ is an optimal entanglement witness if $\mathrm{E}(\sigma)$ is maximal (i.e., whenever $\mathrm{E}(\sigma) \subset \mathrm{E}(\tau)$ for $\tau \in \mathcal{BP}$, then $\mathrm{E}(\sigma) = \mathrm{E}(\tau)$). Use the S-lemma (Lemma C.4) to show that if σ lies on an extreme ray of $\mathcal{BP}$ and $\sigma \notin \mathcal{PSD}$, then σ is an optimal entanglement witness.

2.4.5. Proofs of Størmer's theorem. In this section we will present two rather different proofs of the $\mathbb{C}^2 \otimes \mathbb{C}^2$ case of Theorem 2.15, which we state here in a slightly more general form. (See Notes and Remarks for comments regarding the $\mathbb{C}^2 \otimes \mathbb{C}^3$ case.)

THEOREM 2.36 (Størmer's theorem). *If $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, then the separable cone $\mathcal{SEP}(\mathcal{H})$ and the cone $\mathcal{PPT}(\mathcal{H})$ coincide. Equivalently, $\boldsymbol{P}(\mathbb{C}^2) = \boldsymbol{DEC}(\mathbb{C}^2)$.*

The equivalence of the two assertions of the Theorem follows from Choi's correspondence and duality (see Section 2.4 and particularly Table 2.2). We will focus on the second assertion. Since the inclusion $\boldsymbol{DEC}(\mathcal{H}) \subset \boldsymbol{P}(\mathcal{H})$ always holds, we only need to establish that every positivity-preserving map on $\mathsf{M}_2^{\mathrm{sa}}$ is decomposable.

In a nutshell, the first proof depends on noticing that Proposition 2.32 effectively reduces the general case to that of unital, trace-preserving maps, which in turn follows easily from *very* classical facts. The second proof handles first the maps generating extreme rays of $\boldsymbol{P}(\mathbb{C}^2)$, and concludes via the Krein–Milman theorem. Here are the details.

PROOF # 1 OF THEOREM 2.36. The crucial observation is that it suffices to show that the interior of $\boldsymbol{P}(\mathbb{C}^2)$ is contained in $\boldsymbol{DEC}(\mathbb{C}^2)$. The needed inclusion $\boldsymbol{P}(\mathbb{C}^2) \subset \boldsymbol{DEC}(\mathbb{C}^2)$ follows then from both cones being closed, and being the closures of their interiors.

To that end, suppose that Φ belongs to the interior of $\boldsymbol{P}(\mathbb{C}^2)$. Proposition 2.32 implies then that there exist positive operators $A, B \in \mathsf{M}_2^{\mathrm{sa}}$ and a positivity-preserving, unital and trace-preserving map $\tilde{\Phi} : \mathsf{M}_2^{\mathrm{sa}} \to \mathsf{M}_2^{\mathrm{sa}}$ such that $\Phi(\rho) = A^{-1}\tilde{\Phi}\big(B^{-1}\rho B^{-1}\big)A^{-1}$ for all $\rho \in \mathsf{M}_2^{\mathrm{sa}}$. In other words, $\Phi = \Phi_{A^{-1}} \circ \tilde{\Phi} \circ \Phi_{B^{-1}}$, where $\Phi_M(\rho) := M\rho M^\dagger$. Since every Φ_M is completely positive, the composition rules for completely positive and co-completely positive maps (see Exercises 2.26 and 2.46) show that the problem reduces to establishing decomposability of $\tilde{\Phi}$.

Up to now, the argument worked in any dimension; presently, we will exploit the special features of dimension 2. Since $\tilde{\Phi}$ is an affine self-map of the Bloch ball that preserves the center, it may be thought of as a linear map $R \in B(\mathbb{R}^3)$ with $\|R\|_\infty \leqslant 1$. Such maps are convex combinations of elements of $\mathsf{O}(3)$ (cf. Exercises 1.44 and 1.45), which in turn correspond to maps of the form (i) $\rho \mapsto U\rho U^\dagger$ or (ii) $\rho \mapsto U\rho^T U^\dagger$ for some $U \in \mathsf{U}(2)$ (depending on whether the said element of $\mathsf{O}(3)$ belongs to $\mathsf{SO}(3)$ or not). This is a very special and elementary case of Kadison's Theorem 2.4, and was explained in the proof of Wigner's Theorem 2.3 (see also Exercise B.4 for the isomorphism $\mathsf{PSU}(2) \leftrightarrow \mathsf{SO}(3)$). It remains to recall that the maps of form (i) are completely positive and those of form (ii) are co-completely positive. □

REMARK 2.37. The above argument, when combined with the result from Exercise 1.45, shows that every $\Phi \in \boldsymbol{P}(\mathbb{C}^2)$ can be represented as $\Phi = \sum_j \Phi_{A_j} + \sum_k \Phi_{B_k} \circ T$ so that the total number of terms does not exceed 4.

PROOF # 2 OF THEOREM 2.36. Again, we will prove the inclusion $\boldsymbol{P}(\mathbb{C}^2) \subset \boldsymbol{DEC}(\mathbb{C}^2)$. Since $\boldsymbol{P}(\mathbb{C}^2)$ is convex and nondegenerate, it is enough to verify that its extreme rays consist of decomposable maps (see the comment following Proposition 1.9). The following characterization of such extreme rays comes in handy.

PROPOSITION 2.38 (see Appendix C). *Let $\Phi : \mathsf{M}_2^{\mathrm{sa}} \to \mathsf{M}_2^{\mathrm{sa}}$ be a map which generates an extreme ray of $\boldsymbol{P}(\mathbb{C}^2)$. Then either Φ is an automorphism of $\mathcal{PSD}(\mathbb{C}^2)$, in which case it is described by Proposition 2.29, or Φ is of rank one, in which case it is of the form $\Phi(\rho) = \mathrm{Tr}(\rho|\varphi\rangle\langle\varphi|)|\psi\rangle\langle\psi| = |\psi\rangle\langle\varphi|\rho|\varphi\rangle\langle\psi|$ for some $\varphi, \psi \in \mathbb{C}^2\backslash\{0\}$.*

Proposition 2.38 is a special case of the characterization of the extreme rays of the maps preserving the Lorentz cone $\mathcal{L}_n$ (remember that the cone $\mathcal{PSD}(\mathbb{C}^2)$

is isomorphic to the Lorentz cone $\mathcal{L}_4$) that will be proved in Appendix C. The proof is based on the so-called S-lemma, a well-known fact from control theory and quadratic/semi-definite programming.

Once we assume the above Proposition, concluding the proof is easy. Indeed, if Φ is an automorphism of $\mathcal{PSD}(\mathbb{C}^2)$, then, by Proposition 2.29, it is either completely positive or co-completely positive, so *a fortiori* decomposable. On the other had, if Φ is of rank one and $\Phi(\rho) = |\psi\rangle\langle\varphi|\rho|\varphi\rangle\langle\psi|$, then Φ is clearly completely positive with Kraus rank one and the single Kraus operator $A = |\psi\rangle\langle\varphi|$ (see Choi's Theorem 2.21; actually, since A is itself of rank one, it follows that $C(\Phi)$ is in fact separable and hence that Φ entanglement-breaking, see Lemmas 2.20 and 2.27). □

Notes and Remarks

Classical references for the mathematical aspects of quantum information theory are [**NC00, Hol12, Wil17**]. We also recommend [**Wat**].

Section 2.1. A general reference for the geometry of quantum states is the book [**BŻ06**]. Wigner's theorem appears in [**Wig59**] and Kadison's theorem in [**Kad65**] in a broader context. Elementary proofs can be found in [**Hun72, Sim76**] and recent generalizations in [**SCM16, Stø16**].

Section 2.2. The definition of separability for mixed states was introduced in [**Wer89**]. The NP-hardness of deciding whether a state is separable was shown in [**Gur03**]. The argument sketched in Exercise 2.10 about the number of product vectors needed to represent any separable state is from [**CĐ13**].

Werner states were introduced in [**VW01**], where the question of their separability (Proposition 2.16) is also discussed.

Theorem 2.10 was proved in [**DPS04**]. For more information about k-extendibility and the symmetric subspace (also in the multipartite setting) we refer to the survey [**Har13**]. An early reference for k-entangled states is [**TH00**]. See Notes and Remarks on Chapter 9 for quantitative results about the hierarchies defined in Section 2.2.5.

The observation that non-PPT states are entangled (Peres–Horodecki criterion, Proposition 2.13) goes back to [**Per96**], see also [**HHH96**].

It was observed in [**HHH96**] that Theorem 2.15 is a consequence of results by Størmer [**Stø63**] and Woronowicz [**Wor76**]. See Notes and Remarks on Section 2.4 for more information.

For examples of PPT entangled states in $\mathbb{C}^3 \otimes \mathbb{C}^3$ or $\mathbb{C}^2 \otimes \mathbb{C}^4$, see [**Hor97**]; an early result going in the same direction can be found in [**Cho75b**]. Less *ad hoc* examples (in higher dimensions) are presented, e.g., in [**BDM$^+$99**]. A geometric (non-constructive) argument is given in Chapter 9 (see Propositions 9.18 and 9.20; this approach works if the dimension is sufficiently large).

The realignment criterion to detect entanglement (also called cross-norm criterion) presented in Exercise 2.24 is from [**CW03, Rud05**]. It is neither weaker nor stronger than the PPT criterion. For more separability criteria, see the survey [**HHHH09**].

Theorem 2.17 was proved in [**AS10**] in the bipartite case and in [**FLPS11**] in the general case.

The geometry of the set of absolutely separable states is poorly understood. By definition, whether a state ρ is absolutely separable depends only on its spectrum.

An explicit description is known for $\mathbb{C}^2 \otimes \mathbb{C}^2$: a state ρ with eigenvalues $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3 \geqslant \lambda_4$ is absolutely separable if and only if $\lambda_1 \leqslant \lambda_3 + 2\sqrt{\lambda_2 \lambda_4}$ [**VADM01**].

Similarly to absolute separability, one may say that a state $\rho \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is absolutely PPT if $U\rho U^\dagger$ is PPT for any unitary U on $\mathcal{H}_1 \otimes \mathcal{H}_2$. An intriguing open problem is whether every absolutely PPT state is absolutely separable; see [**AJR15**].

Lemma 2.19 can be proved via elementary representation theory; see, e.g., Appendix C in [**ASY14**].

Section 2.3. The Jamiołkowski isomorphism can be traced to [**Jam72**]. Choi's and Jamiołkowski's isomorphisms are seldom distinguished in the literature; a discussion of the difference between the two appears in [**LS13**].

Choi's Theorem 2.21 as stated was proved in [**Cho75a**], which also contains a description of extreme completely positive unital maps. Closely related statements (including variants of Stinespring's Theorem 2.24) varying by the level of abstractness were arrived at (largely) independently by various authors, see, e.g., [**Sti55, Kra71, Kra83**].

Proposition 2.26 is from [**LS93**] and the argument from Exercise 2.34 is based on more general results from [**RSW02**] which give various descriptions of all quantum channels between qubits and of extreme points of the set of such channels.

For elementary properties of the diamond norm, see Section 3.3.4 in [**Wat**] (where it is studied under the name *completely bounded trace norm*). Entanglement-breaking channels were studied in detail in [**HSR03**].

The example from Exercise 2.29 is from [**Tom85**]. Exercise 2.44 is from [**Wat**], to which we also refer for a discussion of the class of LOCC channels.

Section 2.4. Proposition 2.29 is a folklore result which appears explicitly in [**Sch65**]. Many similar results involve classification of "linear preservers", i.e., linear maps on M_d which preserve some property of matrices. Here is a typical statement due to Frobenius: a linear map $\Phi : \mathsf{M}_d \to \mathsf{M}_d$ satisfies the equation $\det \Phi(X) = \det X$ if and only if it has the from $X \mapsto AXB$ or $A \mapsto AX^TB$ for $A, B \in \mathsf{M}_d$ with $\det(AB) = 1$. For a survey on linear preserver problems, see [**LT92**].

The result from Proposition 2.32 and its derivation from Brouwer's fixed-point theorem appear in [**Ide13, Ide16, AS15**]. A similar statement (proved via an iterative construction) appeared in [**Gur03**] for positive maps Φ which are "rank non-decreasing" (however, not all such maps satisfy the conclusion of Proposition 2.32, see Exercise 2.53). The validity of Proposition 2.32 for completely positive maps is simpler and well known, see for example [**GGHE08**] and its references. The original Sinkhorn's theorem (for matrices, or for maps preserving the positive orthant in $\mathbb{R}^n$) goes back to [**Sin64**]; see [**Ide16**] for an extensive survey of related topics.

Theorem 2.34 is from [**HHH96**]. The concept of optimal entanglement witness which appears in Exercise 2.56 was investigated in [**LKCH00**].

Størmer's Theorem 2.36 was initially proved in [**Stø63**]; the original formulation involved the second of the two statements. The first proof presented here seems to be new and was a byproduct of the work on this book [**AS15**]. The scheme behind the second proof was apparently folklore for some time; it was documented in [**MO15**]. The novelty of its current presentation, if any, consists in streamlining of the proof of Proposition 2.38. (For more background information on Proposition

2.38, see Appendix C.) Other proofs (of either of the two versions given in Theorem 2.36) appeared in [**KCKL00, VDD01, LMO06, KVSW09, Stø13**]. A recent study of positivity-preserving maps on M_3 can be found in [**MO16**]. While [**MO16**] is focused on the unital trace-preserving case, it is likely that (particularly when combined with our Proposition 2.32) it may provide a clear picture of the more general setting. In particular, it may lead to a simple and transparent proof of the $\mathbb{C}^2 \otimes \mathbb{C}^3$ case of Theorem 2.15 (Woronowicz's Theorem).