Quantum information theory (MAT4430) **Spring 2021**

Lecture 5: Convexity and bipartite entanglement

Lecturer: Alexander Müller-Hermes

We have now introduced the formalism of open quantum systems, which describes general quantum systems. Before we turn to quantum information processing protocols, we have to discuss a special feature of quantum systems, which is not present in classical systems: Entanglement. Roughly speaking, entanglement is a special type of correlation of two (or more) quantum systems and it serves as a ressource in quantum information processing. In the exercises, we saw that maximal entanglement enables superdense coding and quantum teleportation, and we will see more examples throughout the course. Here, we will focus on entanglement between two quantum systems, which is known as *bipartite entanglement*. The case of *multipartite entanglement* is much more complicated, and will not be covered in this course. To understand the basics of entanglement theory, we need some basic terminology for talking about convex cones.

1 Convexity and cones

Let us start with two basic definitions:

Definition 1.1 (Convex sets and cones)**.** *Let $\mathcal{V}$ denote a real Euclidean space.*

1. *A set $B \subset \mathcal{V}$ is called* convex *if $\lambda x + (1-\lambda)y \in B$ whenever $x, y \in B$ and $\lambda \in [0,1]$.*
2. *A set $C \subset \mathcal{V}$ is called a* cone *if $\lambda x + \mu y \in C$ for all $x, y \in C$ and all $\lambda, \mu \geqslant 0$.*

It is clear from these definitions that every cone is a convex set, but not every convex set is a cone. In particular, non-empty compact convex sets are never cones. It is also clear that $0 \in C$ for every cone C, but obviously 0 is not necessarily contained in a convex set. We call a convex set $B \subset \mathcal{V}$ a *convex body* if it is compact and has non-empty interior. When $0 \notin B$ for some convex body $B \subset \mathcal{V}$, then we can form a cone $C \subset \mathcal{V}$ by taking

$$\operatorname{cone}(B) = \{\lambda x \ : \ x \in B \text{ and } \lambda \geqslant 0\}.$$

In this case, B is called a *base* for the cone $C = \operatorname{cone}(B)$. It is easy to show that $\operatorname{cone}(B)$ is a closed cone for every convex body B not containing 0. We will use the notation $\operatorname{cone}(\cdot)$ more generally to denote the conic hull of a set, i.e., the smallest cone containing the set. This is similar to the convex hull $\operatorname{conv}(\cdot)$. We will also need the following concepts:

Definition 1.2 (Extreme points and extremal rays)**.** *Let $\mathcal{V}$ denote a real Euclidean space and $B \subset \mathcal{V}$ a convex set and $C \subset \mathcal{V}$ a cone.*

1. *A point $z \in B$ is called an* extreme point *if $z = \lambda x + (1-\lambda)y$ for $x, y \in B$ and $\lambda \in (0,1)$ implies that $x = y = z$.*
2. *A point $x \in C$ generates an* extremal ray $\mathbb{R}_0^+ x \subseteq C$ *if $x - y \in C$ for $y \in C$ implies that $y \in \mathbb{R}_0^+ x$.*

When $B \subset \mathcal{V}$ is a convex body not containing 0, then the extremal rays of the cone $C = \operatorname{cone}(B)$ are generated by the extreme points of B. A convex body B can be expressed as the convex hull[1] of its extreme points

$$B = \operatorname{conv}\left(\operatorname{Ext}(B)\right),$$

[1] Note that the closure is not needed here, since we restrict to compact sets in finite-dimensional spaces.

which is a special case of the *Krein-Milman theorem*. We will sometimes need the following easy facts:

Theorem 1.3. *Let $B \subset \mathcal{V}$ denote a convex body and $f : B \to \mathbb{R}$ a continuous function.*

1. *If f is convex, then $\sup_{x\in B} f(x) = \max_{x\in \mathrm{Ext}(B)} f(x)$.*
2. *If f is concave, then $\inf_{x\in B} f(x) = \min_{x\in \mathrm{Ext}(B)} f(x)$.*

The following theorem gives an upper bound on the number of extreme points needed to express a given point as a convex combination:

Theorem 1.4 (Caratheodory)**.** *If $B \subset \mathcal{V}$ is a convex hull $B = \mathrm{conv}\,(S)$ of a set $S \subseteq \mathcal{V}$, then any $y \in B$ admits a decomposition*

$$y = \sum_{n=1}^{N} p_i x_i,$$

for some probability distribution $p \in \mathcal{P}\,(\{1, \ldots, N\})$ and some $x_1, \ldots, x_N \in S$ with

$$N \leqslant \dim(\mathcal{V}) + 1.$$

We have the following corollary of Caratheodory's theorem:

Corollary 1.5. *For any compact set $S \subset \mathcal{V}$ the convex hull $\mathrm{conv}\,(S)$ is compact.*

Proof. Let $d = \dim(\mathcal{V})$. We will show that $\mathrm{conv}\,(S)$ is sequentially compact, which, in the Euclidean space $\mathcal{V}$, is equivalent to $\mathrm{conv}\,(S)$ being compact. Consider a sequence $(y_n)_{n\in\mathbb{N}} \in \mathrm{conv}\,(S)^{\mathbb{N}}$. By Caratheodory's theorem there are probability distributions $p^{(n)} \in \mathcal{P}\,(\{1, \ldots, d+1\})$ and $(x_1^{(n)}, \ldots, x_{d+1}^{(n)}) \in S^{d+1}$ such that

$$y_n = \sum_{i=1}^{d+1} p_i^{(n)} x_i^{(n)},$$

for each $n \in \mathbb{N}$. Since $\mathcal{P}\,(\{1, \ldots, d+1\})$ and S are compact sets, there exist convergent subsequences $(p^{(n_k)})_{k\in\mathbb{N}} \in \mathcal{P}\,(\{1, \ldots, d+1\})^{\mathbb{N}}$ and $(x_i^{(n_k)}) \in S$ such that

$$p^{(n_k)} \to p \in \mathcal{P}\,(\{1, \ldots, d+1\})$$

and

$$x_i^{(n_k)} \to x_i \in S,$$

as $k \to \infty$, for each $i \in \{1, \ldots, d+1\}$. We conclude that

$$y_{n_k} \to \sum_{i=1}^{d+1} p_i x_i \in \mathrm{conv}(S),$$

as $k \to \infty$, which finishes the proof. □

As for convex bodies, we also have that the cone $C = \mathrm{cone}\,(B)$ generated by a convex body $B \subset \mathcal{V}$ not containing 0 is the conic hull of the union of its extremal rays. By Caratheodory's theorem, every $x \in C$ can be written as

$$x = \sum_{i=1}^{N} x_i,$$

for some $N \leqslant \dim(\mathcal{V}) + 1$ and generators x_i of extremal rays. When studying a cone it is often useful to consider its dual:

Definition 1.6 (Dual cone)**.** *For any cone $C \subset \mathcal{V}$ in a real Euclidean space $\mathcal{V}$ we define the* dual cone C^* *by*

$$C^* = \{y \in \mathcal{V} \ : \ \langle y, x\rangle \geqslant 0 \text{ for any } x \in C\}.$$

It is easy to check that $C^* \subset \mathcal{V}$ is a closed cone whenever C is a cone. The most important result in cone duality is the bipolar theorem. This theorem is a direct consequence of the hyperplane separation theorem, which we state for convenience in a special case:

Theorem 1.7. *If $C \subset \mathcal{V}$ is a non-empty closed cone and $z \notin C$. Then, there exists $y \in C^*$ such that*

$$\langle y, z\rangle < 0.$$

For convenience, we will state the proof of this theorem. It needs the following lemma:

Lemma 1.8. *Let $K \subset \mathcal{V}$ be a non-empty closed convex subset of a real Euclidean space $\mathcal{V}$. Then, there exists a unique $x_{\min} \in K$ such that*

$$\|x_{\min}\|_2 = \inf_{x\in K} \|x\|_2.$$

Proof. Consider a sequence $(x_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ such that $\lim_{n\to\infty} \|x_n\|_2 = \inf_{x\in K} \|x\|_2 =: \delta$. Note that

$$\|x_n + x_m\|_2^2 \geqslant 4\delta^2,$$

for any $n, m \in \mathbb{N}$, since $(x_n + x_m)/2 \in K$. Now, we compute

$$\|x_n - x_m\|_2^2 = 2\|x_n\|_2^2 + 2\|x_m\|_2^2 - \|x_n + x_m\|_2^2 \leqslant 2\|x_n\|_2^2 + 2\|x_m\|_2^2 - 4\delta^2 \to 0,$$

as $n, m \to \infty$. We conclude that $(x_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ is a Cauchy sequence and by completeness of $\mathcal{V}$ and closedness of K there is a point $x_{\min} \in K$ with $\|x_{\min}\|_2 = \inf_{x\in K} \|x\|_2$. Assume now that there is a point $x' \in K$ with $\|x'\|_2 = \inf_{x\in K} \|x\|_2$. Then, we have

$$\|x_{\min} - x'\|_2^2 \leqslant 2\|x_{\min}\|_2^2 + 2\|x'\|_2^2 - 4\delta^2 = 0,$$

showing that $x_{\min} = x'$. □

Now, we can prove the hyperplane separation theorem:

Proof of Theorem 1.7. Consider the closed and convex set $K = \{x - z \ : \ x \in C\}$ and note that $0 \notin K$. By Lemma 1.8 there exists a $v_{\min} \in K$ such that

$$\|v_{\min}\|_2 = \inf_{v\in K} \|v\|_2 =: \delta,$$

and since $0 \notin K$, we have $\delta > 0$. For any $v \in K$ and any $\lambda \in [0, 1]$ we have

$$(1 - \lambda)v_{\min} + \lambda v = v_{\min} + \lambda\,(v - v_{\min}) \in K.$$

Therefore, we have

$$\delta^2 \leqslant \|v_{\min} + \lambda\,(v - v_{\min})\,\|_2^2 = \delta^2 + 2\lambda\langle v_{\min}, v - v_{\min}\rangle + \lambda^2\|v - v_{\min}\|_2^2.$$

Since this inequality holds for all $\lambda \in [0, 1]$ (in particular for $\lambda \to 0$), we conclude that

$$\langle v_{\min}, v\rangle \geqslant \delta^2,$$

for any $v \in K$. By definition of K, this implies that

$$\langle v_{\min}, x\rangle \geqslant \delta^2 + \langle v_{\min}, z\rangle, \tag{1}$$

for every $x \in C$. Inserting $x = 0$ into (1) shows that

$$\langle v_{\min}, z\rangle \leqslant -\delta^2 < 0.$$

Moreover, since (1) holds for any $\lambda x \in C$ with $x \in C$ and any $\lambda \geqslant 0$, we conclude that

$$\langle v_{\min}, x\rangle \geqslant 0,$$

for any $x \in C$. Therefore, we have $v_{\min} \in C^*$ and the proof is finished. □

Now, we can state:

Theorem 1.9 (Bipolar theorem)**.** *For any closed cone $C \subset \mathcal{V}$ in a real Euclidean space $\mathcal{V}$ we have*

$$(C^*)^* = C.$$

Proof. It is clear that $(C^*)^* \supseteq C$. For the other direction consider $z \notin C$. By the hyperplane separation theorem there exists a $y \in C^*$ such that $\langle y, z\rangle = \langle z, y\rangle < 0$ and we conclude that $z \notin (C^*)^*$. □

We will sometimes need a few special properties of cones, which we now prove:

Lemma 1.10 (Interior points)**.** *Let $C \subset \mathcal{V}$ be a closed cone. We have $y \in \operatorname{int}(C^*)$ if and only if*

$$\langle y, x\rangle > 0,$$

for every $x \in C \setminus \{0\}$.

Proof. By definition we have $y \in \operatorname{int}(C^*)$ if some ϵ-ball with $\epsilon > 0$ and center y satisfies $B_\epsilon(y) \subset C^*$. Fix an $x \in C \setminus \{0\}$ and note that

$$\inf_{\|z\|_2 \leqslant 1} \langle y + \epsilon z, x\rangle = \langle y, x\rangle - \epsilon\|x\|_2. \tag{2}$$

Therefore, $\langle y, x\rangle > 0$ has to be satisified if $y \in \operatorname{int}(C^*)$. On the other hand, if $\langle y, x\rangle > 0$ for every $x \in C \setminus \{0\}$, then we can choose $\epsilon = \inf_{x \in K_C} \langle y, x\rangle > 0$ where $K_C = S \cap C$ is the compact set arising as the intersection of the unit sphere

$$S = \{x \in \mathcal{V} \ : \ \|x\|_2 = 1\},$$

and the cone C. By this definition, we have that

$$\epsilon\|x\|_2 \leqslant \langle y, x\rangle,$$

for any $x \in C$ and by (2) we are done.

□

The following lemma is useful as well:

Lemma 1.11. *Let $C \subset \mathcal{V}$ be a closed cone. The following are equivalent:*

1. *The cone C is* pointed*, i.e., $C \cap (-C) = \{0\}$.*
2. *The cone C^* is* generating*, i.e., we have $C^* + (-C^*) = \mathcal{V}$.*
3. *The cone C^* has non-empty interior.*

Proof. If C^* is generating, then there exists a basis $\{y_1, \ldots, y_d\} \subset C^*$ and we define the element $e = \sum_{i=1}^d y_i \in C^*$. Whenever

$$\langle e, x \rangle = \sum_{i=1}^{d} \langle y_i, x \rangle = 0,$$

for some $x \in C$ we can conclude that $x = 0$, and therefore $e \in \operatorname{int}(C^*)$ by Lemma 1.10. For any $e \in \operatorname{int}(C^*)$ we have $\langle e, x \rangle > 0$ whenever $x \in C \setminus \{0\}$ and we conclude immediately that C is pointed. Finally, assume that C^* is not generating and let $\{y_1, \ldots, y_k\} \subset C^*$ a maximal independent set for $k < d$. Consider

$$x \in \operatorname{span}\{y_1, \ldots, y_k\}^{\perp} \neq \emptyset.$$

This $x \in \mathcal{V}$ satisfies

$$\langle y, x \rangle = \langle y, -x \rangle = 0,$$

for every $y \in C^*$ and by the bipolar theorem we conclude that both $x \in C$ and $-x \in C$. This shows that C is not pointed. □

For any closed and pointed cone $C \subset \mathcal{V}$, we may consider $y \in \operatorname{int}(C^*)$ and define a convex set $B \subset C$ by $B = C \cap H$, where

$$H = \{x \in \mathcal{V} \ : \ \langle y, x \rangle = 1\}.$$

It can be verified that $B = C \cap H$ is a convex body not containing zero, and hence it is a base for the cone C. This means that we can always pass between a closed and pointed cone and its compact base.

We will need a few other results about duality of cones. For cones $C_1, C_2 \subset \mathcal{V}$ we define their *intersection* $C_1 \cap C_2$ and their *join*

$$C_1 \vee C_2 = \{x + y \ : \ x \in C_1, y \in C_2\}.$$

These two operations are dual to each other. We summarize this and another fact in the following lemma:

Lemma 1.12. *For closed cones $C_1, C_2 \subset \mathcal{V}$ in a real Euclidean space $\mathcal{V}$ we have:*

1. *If $C_1 \subseteq C_2$, then $C_1^* \supseteq C_2^*$.*
2. *We have $(C_1 \cap C_2)^* = \overline{C_1^* \vee C_2^*}$.*

Proof. See exercises. □

2 Example: Quantum states and the cone $B(\mathcal{H})^+$

To get more familiar with the terminology from the previous section let us apply it to the set $D(\mathcal{H})$ of quantum states and the set $B(\mathcal{H})^+$ of positive semidefinite matrices on a complex Euclidean space $\mathcal{H}$. Note that both of these sets are contained in the space $B(\mathcal{H})_{sa}$ of selfadjoint operators. In the following, we will consider the real Euclidean space $\mathcal{V} = B(\mathcal{H})_{sa}$ equipped with the Hilbert-Schmidt inner product. The following points can be verified easily:

- The set $B(\mathcal{H})^+ \subset B(\mathcal{H})_{sa}$ is a closed and pointed cone.
- The cone $B(\mathcal{H})^+ \subset B(\mathcal{H})_{sa}$ is also generating. Specifically, any operator $Z \in B(\mathcal{H})_{sa}$ can be written as $Z = X - Y$ for $X, Y \in B(\mathcal{H})^+$ such that $XY = 0$. This is called the *Jordan-Hahn decomposition* and is an easy consequence of the spectral theorem.

- We have $\langle Y, X\rangle_{HS} = \operatorname{Tr}[YX] \geqslant 0$ for every $X \in B(\mathcal{H})^+$ if and only if $Y \in B(\mathcal{H})^+$. Therefore, we have $(B(\mathcal{H})^+)^* = B(\mathcal{H})^+$ and we say that $B(\mathcal{H})$ is selfdual.
- We have $\mathbb{1}_{\mathcal{H}} \in \operatorname{int}\left((B(\mathcal{H})^+)^*\right)$ since $\operatorname{Tr}[X] = 0$ implies $X = 0$ whenever $X \in B(\mathcal{H})^+$.
- The quantum states $D(\mathcal{H})$ are a convex body and a compact base of the cone $B(\mathcal{H})^+$ and we have
$$D(\mathcal{H}) = B(\mathcal{H})^+ \cap \{X \in B(\mathcal{H})_{sa} \ : \ \operatorname{Tr}[X] = 1\}.$$

Using the spectral decomposition we can show the following theorem characterizing the extreme points of $D(\mathcal{H})$:

Theorem 2.1. *The extreme points of $D(\mathcal{H})$ are the pure states $|\psi\rangle\langle\psi| \in \operatorname{Proj}(\mathcal{H})$.*

Note that the spectral decomposition gives a much better bound than Caratheodory's theorem on the number of pure states needed to express a given quantum state as a convex combination.

3 Separability and entanglement

We start with the central definition of this lecture:

Definition 3.1 (Separability)**.** *For Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ we define the cone*

$$\operatorname{Sep}(\mathcal{H}_A, \mathcal{H}_B) = \operatorname{cone}\{X_A \otimes Y_B \ : \ X_A \in B(\mathcal{H}_A)^+, Y_B \in B(\mathcal{H}_B)^+\} \subset B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}.$$

We call a positive operator $X_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$ separable *if $X_{AB} \in \operatorname{Sep}(\mathcal{H}_A, \mathcal{H}_B)$, and otherwise we will call X_{AB}* entangled*.*

We will call a quantum state $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ separable if $\rho_{AB} \in \operatorname{Sep}(\mathcal{H}_A, \mathcal{H}_B)$ and otherwise it is called entangled. Entanglement plays a fundamental role in quantum information theory, and it can be seen as a resource enabling many useful quantum protocols such as teleportation or superdense coding. Such protocols are often based on entangled pure states (e.g., maximally entangled states), and there are many open problems related to the generation of pure entangled quantum states from mixed entangled quantum states.

To motivate the notion of entanglement further let us mention the following simple observation showing that local measurements of separable quantum states is inherently classical:

Theorem 3.2 (Local hidden variables)**.** *For Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ consider a pair of POVMs $\{P_n\}_{n=1}^N \subset B(\mathcal{H}_A)^+$ and $\{Q_m\}_{m=1}^M \subset B(\mathcal{H}_B)^+$. For any separable quantum state $\rho_{AB} \in \operatorname{Sep}(\mathcal{H}_A, \mathcal{H}_B) \cap D(\mathcal{H}_A \otimes \mathcal{H}_B)$, there exists a probability distribution $r \in \mathcal{P}(\{1, \ldots, K\})$ and conditional probability distributions $p^A(\cdot|k) \in \mathcal{P}(\{1, \ldots, N\})$ and $q^B(\cdot|k) \in \mathcal{P}(\{1, \ldots, M\})$ such that*

$$\operatorname{Prob}(n, m) = \sum_{k=1}^K r(k) p^A(n|k) q^B(m|k).$$

Proof. The separable quantum state $\rho_{AB} \in \operatorname{Sep}(\mathcal{H}_A, \mathcal{H}_B) \cap D(\mathcal{H}_A \otimes \mathcal{H}_B)$ can be written as

$$\rho_{AB} = \sum_{k=1}^K r(k) \sigma_k^A \otimes \tau_k^B,$$

for a probability distribution $r \in \mathcal{P}(\{1, \ldots, K\})$ and quantum states $\sigma_k^A \in D(\mathcal{H}_A)$ and $\tau_k^B \in D(\mathcal{H}_B)$ for any $k \in \{1, \ldots, K\}$. Now, we define the conditional probability distributions by

$$p^A(n|k) = \operatorname{Tr}\left[P_n \sigma_k^A\right] \quad \text{and} \quad q^B(m|k) = \operatorname{Tr}\left[Q_m \tau_k^B\right],$$

for any $k \in \{1, \ldots, K\}$, and the proof is finished. □

The previous theorem shows that the correlations observed in the outcome statistics of local measurements of a separable quantum state are classical. In the 1930s it was proposed that the weird effects of quantum theory can be explained by so-called *hidden variables*, i.e., that there are classical quantities underlying the physical reality, which are unknown (or hidden) and influence the outcome of experiments. In particular, such hidden variables might become classically correlated and then influence the outcomes of local measurements of an entangled pure state so that such outcomes come out with the same value. The previous theorem shows that local measurements of separable states indeed follow such a *local hidden variable model* with the hidden variable being the value of k. However, we will see later that many[2] entangled quantum states give rise to measurement statistics under local measurements that are incompatible with any local hidden variable model.

4 Positive maps and entanglement witnesses

We will now compute the dual cone of $\mathrm{Sep}\,(\mathcal{H}_A, \mathcal{H}_B)$. For this we will need the Choi-Jamiolkowski isomorphism and the set of positive maps, i.e., linear maps $P : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ such that $P(B(\mathcal{H}_A)^+) \subseteq B(\mathcal{H}_B)^+$. Let us start with two elementary observations:

Lemma 4.1 (Decompositions of operators)**.** *For a Euclidean space $\mathcal{H}$ consider an operator $Z \in B(\mathcal{H})$. Then, there exist positive operators $X_1, X_2, X_3, X_4 \in B(\mathcal{H})^+$ such that*

$$Z = X_1 - X_2 + i(X_3 - X_4).$$

Proof. For $Z \in B(\mathcal{H})$ define

$$H_1 = (Z + Z^\dagger)/2 \in B(\mathcal{H})_{sa} \quad \text{and} \quad H_2 = i(Z^\dagger - Z)/2 \in B(\mathcal{H})_{sa},$$

which are also called the real and imaginary part of Z. It is easy to check that

$$Z = H_1 + iH_2.$$

Now, we can use the Jordan-Hahn decomposition to show find positive operators $X_1, X_2 \in B(\mathcal{H})^+$ satsifying $H_1 = X_1 - X_2$ and positive operators $X_3, X_4 \in B(\mathcal{H})^+$ satsifying $H_2 = X_3 - X_4$. These operators give rise to the decomposition from the theorem. □

Lemma 4.2. *For Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ and any positive map $P : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ we have:*

1. *The Choi operator $C_P \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ is selfadjoint.*
2. *The adjoint $P^* : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ is a positive map.*

Proof. By Lemma 4.1 any $Z \in B(\mathcal{H}_A)$ admits the decomposition $Z = X_1 - X_2 + i(X_3 - X_4)$ with $X_1, X_2, X_3, X_4 \in B(\mathcal{H}_A)^+$. Now, we note that

$$\begin{aligned} P(Z)^\dagger &= (P(X_1) - P(X_2) + i(P(X_3) - P(X_4)))^\dagger \\ &= P(X_1) - P(X_2) - i(P(X_3) - P(X_4)) = P(Z^\dagger), \end{aligned}$$

[2] but not all!

for any $Z \in B(\mathcal{H}_A)$. We conclude that

$$\begin{aligned}(C_P)^\dagger &= \left(\sum_{i,j=1}^{d_A} |i_A\rangle\langle j_A| \otimes P\left(|i_A\rangle\langle j_A|\right)\right)^\dagger \\ &= \sum_{i,j=1}^{d_A} |j_A\rangle\langle i_A| \otimes P\left(|i_A\rangle\langle j_A|\right)^\dagger \\ &= \sum_{i,j=1}^{d_A} |j_A\rangle\langle i_A| \otimes P\left(|j_A\rangle\langle i_A|\right) = C_P.\end{aligned}$$

This shows the first statement.

For the second statement note that $\mathrm{Tr}\left[XY\right] \geqslant 0$ for any $X \in B(\mathcal{H})^+$ holds if and only if $Y \in B(\mathcal{H})^+$, which is equivalent to the aforementioned fact that the cone $B(\mathcal{H})^+$ is selfdual for any Euclidean space $\mathcal{H}$. Now, note that

$$\mathrm{Tr}\left[XP(Y)\right] = \mathrm{Tr}\left[P^*(X)Y\right] = \mathrm{Tr}\left[YP^*(X)\right] \geqslant 0$$

for any $X \in B(\mathcal{H}_B)^+$ and any $Y \in B(\mathcal{H}_A)^+$ whenever the linear map $P : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is positive. □

Theorem 4.3 (Block-positive cone)**.** *For Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ we define the cone of* block-positive *operators by*

$$\mathrm{BP}\left(\mathcal{H}_A, \mathcal{H}_B\right) = \{C_P \ : \ P : B(\mathcal{H}_A) \to B(\mathcal{H}_B) \text{ positive map}\} \subset B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}.$$

Then, we have

$$\mathrm{Sep}\left(\mathcal{H}_A, \mathcal{H}_B\right)^* = \mathrm{BP}\left(\mathcal{H}_A, \mathcal{H}_B\right).$$

Proof. By Lemma 4.2, adjoints of positive maps are again positive and we find that

$$\langle C_P, X_A \otimes Y_B\rangle_{HS} = \langle (\mathrm{id}_A \otimes P)\left(\omega_{AB}\right), X_A \otimes Y_B\rangle_{HS} = \langle \omega_{AB}, X_A \otimes P^*(Y_B)\rangle_{HS} \geqslant 0,$$

for any positive map $P : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$, any $X_A \in B(\mathcal{H}_A)^+$ and any $Y_B \in B(\mathcal{H}_B)^+$. Since the tensor products $X_A \otimes Y_B$ for $X_A \in B(\mathcal{H}_A)^+$ and $Y_B \in B(\mathcal{H}_B)^+$ generate the cone $\mathrm{Sep}\left(\mathcal{H}_A, \mathcal{H}_B\right)$, we conclude that $\mathrm{Sep}\left(\mathcal{H}_A, \mathcal{H}_B\right)^* \supseteq \mathrm{BP}\left(\mathcal{H}_A, \mathcal{H}_B\right)$.

For the other direction consider $W_{AB} \in \mathrm{Sep}\left(\mathcal{H}_A, \mathcal{H}_B\right)^* \subset B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}$. By the Choi-Jamiolkowski isomorphism there exists a linear map $Q : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ such that $W_{AB} = C_Q$. As before, we can compute

$$\langle W_{AB}, X_A \otimes Y_B\rangle_{HS} = \langle \omega_{AB}, X_A \otimes Q^*(Y_B)\rangle_{HS} = \mathrm{Tr}\left[X_A^T Q^*(Y_B)\right],$$

where we used the necklace identities in the final equality. By assumption, we have

$$\langle W_{AB}, X_A \otimes Y_B\rangle_{HS} = \mathrm{Tr}\left[X_A^T Q^*(Y_B)\right] \geqslant 0$$

for any $X_A \in B(\mathcal{H}_A)^+$ and any $Y_B \in B(\mathcal{H}_B)^+$. Therefore, we conclude that $Q^* : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ and also $Q : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ are positive maps, which implies that $W_{AB} \in \mathrm{BP}\left(\mathcal{H}_A, \mathcal{H}_B\right)$. This finishes the proof. □

It is not so easy to decide whether operators belong to the cone $\mathrm{BP}\left(\mathcal{H}_A, \mathcal{H}_B\right)$. The following lemma sometimes helps a little with this:

Lemma 4.4. *For $X_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}$ the following are equivalent:*

1. *We have $X_{AB} \in \mathrm{BP}\left(\mathcal{H}_A, \mathcal{H}_B\right)$.*

2. *For every* $|x\rangle \in \mathcal{H}_A$ *and every* $|y\rangle \in \mathcal{H}_B$ *we have*

$$(\langle x| \otimes \langle y|) X_{AB} (|x\rangle \otimes |y\rangle) \geqslant 0.$$

Proof. This lemma is simply the fact that the operators $|x\rangle\langle x| \otimes |y\rangle\langle y|$ for $|x\rangle \in \mathcal{H}_A$ and $|y\rangle \in \mathcal{H}_B$ generate the extremal rays of $\mathrm{Sep}\,(\mathcal{H}_A, \mathcal{H}_B)$. □

Operators $W_{AB} \in \mathrm{BP}\,(\mathcal{H}_A, \mathcal{H}_B) \setminus B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$ are sometimes called *entanglement witnesses* since they "witness" the entanglement in some entangled operators. The following corollary (which is implicit already in the proof of the previous theorem) makes this point of view a bit more explicit:

Corollary 4.5 (Entanglement witnesses)**.** *Consider a selfadjoint operator* $X_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}$ *for Euclidean spaces* $\mathcal{H}_A$ *and* $\mathcal{H}_B$*. The following are equivalent:*

1. *The operator* X_{AB} *is separable.*
2. *For any* $W_{AB} \in \mathrm{BP}\,(\mathcal{H}_A, \mathcal{H}_B)$ *we have* $\langle W_{AB}, X_{AB}\rangle_{HS} \geqslant 0$*.*
3. *For any positive map* $P : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ *we have* $(\mathrm{id}_A \otimes P)\,(X_{AB}) \in B(\mathcal{H}_A \otimes \mathcal{H}_A)^+$*.*

Proof. The equivalence of 1. and 2. follows immediately from Theorem 4.3. It is also clear that

$$(\mathrm{id}_A \otimes P)\,(X_A \otimes Y_B) = X_A \otimes P(Y_B) \in B(\mathcal{H}_A \otimes \mathcal{H}_A)^+,$$

for any positive map $P : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ and any $X_A \in B(\mathcal{H}_A)^+$ and any $Y_B \in B(\mathcal{H}_B)^+$. Therefore, 1. implies 3.. To see that 3. implies 2. note that

$$\langle W_{AB}, X_{AB}\rangle_{HS} = \langle \omega_{AB}, (\mathrm{id}_A \otimes P)\,(X_{AB})\rangle_{HS} = \langle \Omega_{AB}|\,(\mathrm{id}_A \otimes P)\,(X_{AB})\,|\Omega_{AB}\rangle \geqslant 0,$$

for the positive map $P : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ defined such that $W_{AB} = C_{P^*}$. □

We finish this section with a few elementary observations about the convex structures of the cones $\mathrm{Sep}\,(\mathcal{H}_A, \mathcal{H}_B)$ and $\mathrm{BP}\,(\mathcal{H}_A, \mathcal{H}_B)$:

- Clearly, the cones $\mathrm{Sep}\,(\mathcal{H}_A, \mathcal{H}_B)$ and $\mathrm{BP}\,(\mathcal{H}_A, \mathcal{H}_B)$ are closed and pointed.
- By duality we conclude that both cones are generating as well and therefore they have non-empty interiors.

5 The positive partial transpose criterion

How can we tell whether a quantum state is entangled or not? In general, this question turns out to be difficult. It has been shown that deciding whether a quantum state $\rho_{AB} \in D(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ is ϵ-close to the set of separable quantum states is an NP-hard problem in the dimensions d_A and d_B and if ϵ is scaling like the inverse of a polynomial in d_A and d_B. It is unlikely[3] that this problem can be solved efficiently on a classical (or quantum) computer.

Even though the separability problem is not efficiently solvable, there are neccessary conditions for separability, which can be quite helpful. The easiest conditions are derived from Corollary 4.5 by choosing a particular positive map $P : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$. One of the most well-studied choices is given by the transpose map:

[3] and would yield a 1.000.000$ prize

Definition 5.1 (Partial transpose)**.** *For a selfadjoint operator* $X_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}$ *we define its (right)* partial transpose *by*

$$X_{AB}^{\Gamma} = (\mathrm{id}_A \otimes \vartheta_B)(X_{AB}).$$

We say that X_{AB} *has* positive partial transpose *or that* X_{AB} *is PPT if*

$$X_{AB}^{\Gamma} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)^+.$$

The set of PPT operators[4] *will be denoted by*

$$PPT(\mathcal{H}_A, \mathcal{H}_B) = \{X_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa} \ : \ X_{AB}^{\Gamma} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)^+\}.$$

By Corollary 4.5 we can show that a quantum state is entangled by showing that it is not PPT. An example of this is the (unnormalized) maximally entangled state $\omega_d \in B(\mathbb{C}^d \otimes \mathbb{C}^d)^+$ where it can be checked that

$$\omega_d^{\Gamma} = C_{\vartheta} = \mathbb{F}_d \notin B(\mathbb{C}^d \otimes \mathbb{C}^d)^+.$$

The operator $\mathbb{F}_d \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$ arising as the Choi operator of the transpose map is also called the *flip operator* due to its property $\mathbb{F}_d(|v\rangle \otimes |w\rangle) = |w\rangle \otimes |v\rangle$ for any $|v\rangle, |w\rangle \in \mathbb{C}^d$. More generally, we note the following theorem:

Theorem 5.2. *We have* $\mathrm{Sep}(\mathcal{H}_A, \mathcal{H}_B) \subseteq PPT(\mathcal{H}_A, \mathcal{H}_B) \cap B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$.

Remarkable, there is a converse of the previous theorem in small dimensions:

Theorem 5.3. *We have* $\mathrm{Sep}\left(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}\right) = PPT\left(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}\right) \cap B(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})^+$ *if and only if*

$$(d_A, d_B) \in \{(2,2), (2,3), (3,2)\},$$

or if $d_A = 1$ *or* $d_B = 1$.

The case $(d_A, d_B) = (2,2)$ is commonly attributed to Størmer (although he disagrees with this), and the cases $(d_A, d_B) \in \{(2,3), (3,2)\}$ are due to Woronowicz. The proofs of these two cases are very different and we will not present the proof of Woronowicz' result. However, recently an "easy" method has been discovered by Aubrun and Szarek for how to prove the case of $(d_A, d_B) = (2,2)$. We will do most of this proof in the exercises and the lecture.

[4] Note that some authors use the term PPT to mean positive and having positive partial transpose, which we do not!