Chapter 2
Background

In this chapter we present the basics that will be used in the rest of the thesis, as well as the results that represent the state of the art. Expert readers may skip this chapter.

2.1 Entanglement

If one had to describe quantum physics in just one word, this would probably be *entanglement*. Quantum physics predicts that, for a multipartite system, there exist states which cannot be written as a product of the states of its subsystems; such states are called entangled. This fact is just a direct consequence of the tensor product structure of the Hilbert space that describes a composite quantum system and the linearity of quantum mechanics, also known as the superposition principle; however, it entails deep consequences.

Historically, Einstein, Podolsky and Rosen argued in 1935 that quantum mechanics was an incomplete description of Nature,[1] and entanglement was at the heart of their argument [EPR35]. However, Schrödinger, who first coined the term entanglement, noted that it was the most characteristic feature of quantum mechanics [Sch35]:

Entanglement is not one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.

In 1964 the physicist John Bell came up with a way to test the EPR paradox, and he proved that the statistics obtained through some quantum experiments cannot be reproduced by any local hidden variable theory [Bel64]. This means that Nature can produce correlations between spacelike separated events that can be explained

[1] The authors argued that any complete theory should have an element that describes every 'element of reality' (i.e., a physical quantity whose values can be predicted with certainty without disturbing the system).

J. Tura i Brugués, *Characterizing Entanglement and Quantum Correlations Constrained by Symmetry*, Springer Theses, DOI 10.1007/978-3-319-49571-2_2

neither by an influence continuously propagating (at arbitrary finite speed) from one event to the other nor by a common local cause.

Surprisingly, very few works appeared from 1935 to the early 1990s, when Artur Ekert proposed to use the correlations arising from entangled states for cryptography [Eke91].

Nowadays, entanglement is considered a resource for many quantum information tasks, comprising quantum cryptography [Eke91], quantum teleportation [Ben+93], quantum dense coding [BW92], quantum repeaters based on entanglement purification [Dür+99], lowering bounds on communication complexity [CB97, Gro97], and it is a prerequisite for another important resource in quantum information theory: nonlocal correlations [Bar+05].

2.1.1 Characterization of Entanglement

Quantum states are represented by positive semi-definite linear operators of unit trace acting on a Hilbert space $\mathcal{H}$. Recall that a Hilbert space is an inner product space[2] which is also complete (every Cauchy sequence in $\mathcal{H}$ converges in $\mathcal{H}$ with the norm induced by the inner product in $\mathcal{H}$). For the purposes of this Thesis, $\mathcal{H}$ will be a finite-dimensional complex Hilbert space; i.e., $\mathcal{H} = \mathbb{C}^d$. The set of bounded linear operators acting on $\mathcal{H}$ will be denoted $\mathcal{B}(\mathcal{H})$. By picking an orthonormal basis of $\mathcal{H}$, typically named computational, consisting of the vectors $\{|i\rangle,\ 0 \leq i < d\}$, the elements of $\mathcal{B}(\mathcal{H})$ are represented by $d \times d$ matrices with complex entries, and we denote such set by M_d. The identity matrix from M_d is denoted $\mathbb{1}_d$. The set of elements of $\mathcal{B}(\mathcal{H})$ that correspond to quantum states is denoted by $\mathcal{D}(\mathcal{H})$and it contains the elements of $\mathcal{B}(\mathcal{H})$ with unit trace and non-negative eigenvalues. The elements of $\mathcal{D}(\mathcal{H})$ are called density matrices or density operators. Formally, one has $\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \succeq 0,\ \mathrm{Tr}\rho = 1\}$.

Any density operator $\rho \in \mathcal{D}(\mathcal{H})$ can be written as a convex combination of rank-one projectors:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.1}$$

where $p_i$is a probability distribution (i.e., for all i, $p_i \geq 0$ and $\sum_i p_i = 1$) and $|\psi_i\rangle$ are unit vectors from $\mathcal{H}$, called *ket*s. The co-vectors $\langle\psi_i|$, called *bra*s, are the Hermitian transposition of the vectors $|\psi_i\rangle$ with respect to the computational basis; two vectors $|\psi_i\rangle$ are considered equivalent if they differ only by a global phase. Note that the decomposition (2.1) is not unique in general. The set $\{p_i, |\psi_i\rangle\}_i$is called *ensemble* and different ensembles may lead to the same quantum state ρ. The probability distribution p_i indicates the ignorance or the lack of information that one has on the state of the system. In the case that $p_i = 1$ for some i, the information about

[2]Unless stated otherwise, throughout this Thesis we consider that $\mathcal{H}$ is a vector space defined over the field of complex numbers, denoted $\mathbb{C}$.

the quantum state is maximal and then $\rho = |\psi_i\rangle\langle\psi_i|$ is said to be in a pure state; otherwise we say that the state is mixed. Thus, Eq. (2.1) indicates that any mixed quantum state ρ can be obtained as a convex combination of pure states (rank-one projectors). Thus, $\mathcal{D}(\mathcal{H})$ forms a convex set, and it is completely determined by its extremal points (i.e., those that cannot be written as a convex combination of other elements in $\mathcal{D}(\mathcal{H})$). The extremal points of $\mathcal{D}(\mathcal{H})$ are denoted $\mathrm{Ext}(\mathcal{D}(\mathcal{H}))$.

The Hilbert space $\mathcal{H}$ corresponding to a composite quantum system consisting of parts $A_1, \ldots, A_n$ is endowed with a tensor product structure $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$, where $\mathcal{H}_i$ is the Hilbert space corresponding to the i-th subsystem. This tensor product structure and the linearity of $\mathcal{H}$ are the two key ingredients that lead to the notion of entanglement.

Entanglement Definition

Many concepts in quantum information are defined through a negative qualifier; i.e., one defines what a certain concept is *not*. This is as well the case of entanglement, which is defined as not being separable. The reason for that is the operational interpretation that a separable state has: any separable state can be created by Local Operations and Classical Communication (LOCC) from scratch starting from a pure product state $|\psi\rangle = |\psi_1\rangle \cdots |\psi_n\rangle$ [Wer89]; in other words, a separable state can be produced by parties in separated laboratories that are allowed to exchange classical information via e.g. a telephone line.

Let us illustrate the simplest case; that of a bipartite Hilbert space between parties A and B: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Definition 2.1 A state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is called *separable* if it admits the following convex decomposition [Wer89]:

$$\rho = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad \sum_i p_i = 1, \quad p_i \geq 0, \tag{2.2}$$

where $\rho_A^{(i)} \in \mathcal{D}(\mathcal{H}_A)$ and $\rho_B^{(i)} \in \mathcal{D}(\mathcal{H}_B)$.

In the multipartite case, one has a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$, where there are different notions of separability. The reason for that is that there are many ways to partition a set of n parties, whereas in Definition 2.1 there is only one. Let us denote by $\mathbf{A} = \{A_1, \ldots, A_n\}$ the set of n parties and let us consider $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{H}_{\mathbf{A}})$, where $\mathcal{H}_{\mathbf{A}} = \bigotimes_{i=1}^n \mathcal{H}_{A_i}$ and $\mathcal{H}_{A_i}$ is the Hilbert space corresponding to party A_i. We say that a set of subsets $S = \{S_1, \ldots, S_K\}$, where $S_i \subseteq \mathbf{A}$, is a K-partition of $\mathbf{A}$ if $\bigcup_{i=1}^K S_i = \mathbf{A}$ and for all $i \neq j$, $S_i \cap S_j = \emptyset$. Thus, a K-partition of $\mathbf{A}$ is a way to split the set of n parties into K non-empty, pairwise disjoint, subsets. Let $\mathcal{S}_K$ be the set of all K-partitions.

Definition 2.2 A state $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{H}_{\mathbf{A}})$ is K-separable if it admits the following convex decomposition

$$\rho_{\mathbf{A}} = \sum_{S \in \mathcal{S}_K} p_S \sum_i q_{S,i} \bigotimes_{k=1}^K |\psi_{S_k,i}\rangle\langle\psi_{S_k,i}|, \tag{2.3}$$

where p_S and $q_{S,i}$ are probability distributions and $|\psi_{S_k,i}\rangle \in \mathcal{H}_{A_i}$.

Remark 2.3 Observe that Definition 2.2 is the same as Definition 2.1 for $K = 2$ and $n = 2$. If $K = 2$ and n is arbitrary, the state is called bi-separable, as it can be prepared by allowing the n parties to gather in bipartitions; in this case we abuse notation and we simply denote S as $S|\overline{S}$with $\overline{S} = \mathbf{A}\backslash S$. A state $\rho_{\mathbf{A}}$ is fully separable if it is n-separable, and it is Genuinely Multipartite Entangled (GME) if it does not admit any form of K-separability; in particular, if it is not bi-separable.

Remark 2.4 Definition 2.2 is clearly inspired in the operational way to construct a quantum state: the higher the K, the less effort the parties need to make to produce the state. However, there are other ways to generalize Definition 2.1, also with a clear operational interpretation. This is the case of K-producibility [GTB05]. A state is K-producible if it can be prepared by allowing parties to gather in groups consisting of at most K parties. This leads to another characterization of the set of quantum states. However, the two definitions coincide for the case of GME states that we will mostly consider in Chaps. 3 and 5: GME states are those which are not biseparable or, equivalently, those which are not $(n-1)$-producible.

2.1.2 The Separability Problem

Despite having an operationally clear interpretation, deciding in practice if a state $\rho_{\mathbf{A}}$ is K-separable or not is far from trivial, even in the bipartite case where $\mathbf{A} = \{A, B\}$. It was shown by Gurvits in 2003 that this problem is NP-hard[3] [Gur03].

For a few particular cases this question does have a simple complete answer. In general, however, one can obtain only partial results: sufficient, but not necessary, conditions that certify that a state is entangled.

The Bipartite Case

Let us begin with considering the simplest case of two parties. Any bipartite pure state $|\psi_{AB}\rangle \in \mathcal{H}_{AB}$ admits the following decomposition, called Schmidt decomposition [NC00]:

$$|\psi\rangle = \sum_{i=1}^{r(|\psi\rangle)} \alpha_i |e_i\rangle \otimes |f_i\rangle, \tag{2.4}$$

where $\{|e_i\rangle\}_{i=1}^{d_1}$ and $\{|f_i\rangle\}_{i=1}^{d_2}$ form orthonormal basis of their respective Hilbert spaces and $\sum_i |\alpha_i|^2 = 1$. The minimal number of terms $r(|\psi\rangle)$for which the decomposition in Eq. (2.4) is possible is called the Schmidt rank. A bipartite pure state $|\psi\rangle$ is

[3] A problem belongs to the class of complexity NP-hard if any algorithm that solves it can be translated in polynomial time into one solving any problem in NP. Hence, an NP-hard problem is as hard as any problem in NP, although it might be harder.

NP stands for Nondeterministic Polynomial time and it consists of all problems whose solution can be verified in polynomial time by a deterministic Turing machine.

entangled if, and only if, $r(|\psi\rangle) > 1$. This definition is generalized to mixed states, leading to the so-called Schmidt number s of a mixed state, by means of the convex roof extension [TH00]:

$$s = \inf_{\{p_i, |\psi_i\rangle\}_i} \max_i r(|\psi_i\rangle), \tag{2.5}$$

i.e., the Schmidt number of ρ is the minimum over all ensembles that generate ρ (cf. Eq. (2.1)) of the maximal Schmidt rank of the pure states in the ensemble. A mixed state ρ is separable if, and only if, $s = 1$; in such case, the decomposition in Eq. (2.2) is given by the ensemble minimizing Eq. (2.5). The Schmidt number constitutes a measure of entanglement and it is non-increasing under LOCC [Nie99, TH00]. Hence, it divides $\mathcal{D}(\mathcal{H}_{AB})$ into $d_1^2 d_2^2$ nested regions[4] according to s.

In what follows we present two operational criteria for deciding whether a state ρ belongs to the set of separable states, denoted $\mathcal{D}_{\text{sep}}$: the Positive under Partial Transposition (PPT) criterion and certification through an Entanglement Witness (EW).

Separability Based on Positive, but Not Completely Positive, Maps

A map $\Lambda : \mathcal{B}(\mathcal{H}_1) \longrightarrow \mathcal{B}(\mathcal{H}_2)$ is called positive if, for all $\rho \succeq 0$, $\Lambda[\rho] \succeq 0$. However, if ρ is the state of a composite quantum system and we apply Λ to one subsystem only, it may happen that the resulting state is not positive semi-definite; i.e., not physical. Consequently, the positivity of a map is not sufficient to guarantee a physical operation. This caveat is solved through the notion of a completely positive map.

A positive map Λ is Completely Positive (CP) if, for any n and for any $\rho \succeq 0$, $(\mathbb{1}_n \otimes \Lambda)[\rho] \succeq 0$; i.e., no matter what happens to the rest of the system, ρ is mapped onto a positive-semidefinite operator. If in addition Λ is Trace Preserving (TP), then Λ defines a physical operation: CPTP maps map quantum states onto quantum states. CPTP maps are also known as quantum channels.

Any positive map, however, is completely positive on separable states, and this is the idea behind the separability criteria based on positive, but not completely positive, maps: If we apply $(\mathbb{1}_n \otimes \Lambda)$ to a state of the form (2.2), we also obtain a positive state

$$(\mathbb{1}_n \otimes \Lambda)[\rho] = \sum_i p_i \rho_A^{(i)} \otimes \Lambda(\rho_B^{(i)}) \succeq 0. \tag{2.6}$$

Hence, $(\mathbb{1}_n \otimes \Lambda)[\rho] \not\succeq 0$ indicates that ρ is not of the form (2.2) hence it must be entangled.

A necessary and sufficient condition for deciding if a bipartite ρ is separable is that ρ satisfies condition (2.6) for all positive, but not completely positive, maps [HHH96]. In practice, one cannot check this condition for all Λ, but there are maps that very well approximate $\mathcal{D}_{\text{sep}}$.

---

[4]The upper bound $s \leq d_1^2 d_2^2$, stems from Carathodory's theorem [Car11]: Any state expressed as a convex combination like in Eq. (2.2) can be re-expressed as another convex combination of no more than $\dim \mathcal{D}(\mathcal{H}_{AB})$ terms, as $\mathcal{D}(\mathcal{H}_{AB})$ can be embedded into the $\mathbb{R}$-vector space of $d_1 d_2 \times d_1 d_2$ Hermitian matrices, which has dimension $d_1^2 d_2^2$.

The PPT Criterion

By picking $\Lambda = T$, where T is the transposition map with respect to a basis, defined as $T(|i\rangle\langle j|) = |j\rangle\langle i|$ and extended by linearity, one obtains the Peres criterion, a very strong necessary condition for separability [Per96]. In fact, it is also a sufficient condition for any $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ or $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^3)$. This is because all positive maps $\Lambda : \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^d) \longrightarrow \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^d)$ are decomposable[5] for $d = 2$ [Stø63] and for $d = 3$ [Wor76] and if a decomposable map reveals entanglement, so does the transposition map [HHH96].

The Positive under Partial Transposition (PPT) criterion is known to be insufficient for any other bipartite case, as there are entangled states in $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^4)$ and in $\rho \in \mathcal{D}(\mathbb{C}^3 \otimes \mathbb{C}^3)$ for which $\rho^{T_B} \succeq 0$, where $\rho^{T_B} := (\mathbb{1} \otimes T)[\rho]$ is the state ρ partially transposed on Bob's side [Hor97].

The PPT criterion and, in general, any criterion of separability based on positive, but not completely positive, maps is straightforward to generalize to the multipartite scenario, for the case of fully separable states.

If a state $\rho_{\mathbf{A}}$ is n-separable, then for any bipartition $S|\overline{S}$of $\mathbf{A}$, the application of Λ to every party in $\overline{S}$ does not change the positivity of the resulting state: $(\mathbb{1}_S \otimes \bigotimes_{A_i \in \overline{S}} \Lambda_{A_i})[\rho] \succeq 0$. A violation of this condition signals that there is entanglement across that bipartition.

Entanglement Witnesses

The concept of Entanglement Witness (EW) was introduced in [HHH96] as a method to exploit the geometric properties of $\mathcal{D}_{\text{sep}}$. The set of separable states is closed and convex. It will be convenient to consider in this section unnormalized states, so that $\mathcal{D}_{\text{sep}}$is a cone.

The Hahn–Banach theorem [Edw95] states that, given two convex closed sets A_1 and A_2, one of them being compact, there exists a continuous linear map f and a constant $\alpha \in \mathbb{R}$ such that $f(a_1) < \alpha \leq f(a_2)$ for all $a_i \in A_i$. In particular, it implies that a closed convex set in a Banach space is characterized by half-spaces whose normal vectors are non-positive semi-definite elements of the dual cone of $\mathcal{D}_{\text{sep}}$, denoted $\mathcal{P}$. $\mathcal{P}$ is, by definition, the set $\{W \in M_{d_A} \otimes M_{d_B} | \operatorname{Tr}(W\rho) \geq 0,\ \forall\, \rho \in \mathcal{D}_{\text{sep}}\}$. Then, the set of elements $W \in \mathcal{P}$ such that $W \not\succeq 0$ forms a non-convex set. Such an operator W is called Entanglement Witness [Ter00]. Note that we require that W has some negative eigenvalue, so that it can detect some entangled state. We denote by $\mathcal{W}$the set of EWs. A necessary and sufficient condition for $\rho \in \mathcal{D}_{\text{sep}}$ is that $\operatorname{Tr} W\rho \geq 0$ for all $W \in \mathcal{W}$ [HHH96].

Not all elements in $\mathcal{W}$ are necessary to characterize $\mathcal{D}_{\text{sep}}$ and the first attempt to find a minimal set of EWs that determine $\mathcal{D}_{\text{sep}}$ was done in [Lew+00], where the notion of optimal EW was defined. Let us briefly recall it. Given $W \in \mathcal{W}$, consider the sets

$$\Delta_W := \{\rho \in \mathcal{D}(\mathcal{H}) |\ \operatorname{Tr} W\rho < 0\} \tag{2.7}$$

[5]A decomposable map Λ can be written as $\Lambda = \Lambda_1 + \Lambda_2 \circ T$, where Λ_1 and Λ_2 are CP maps. This fact is intimately related to the decomposability of entanglement witnesses via the Choi-Jamiołkowski-Sudarshan isomorphism [Jam72, Cho75].

and

$$\Pi_W := \{|e,f\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} | \langle e,f|W|e,f\rangle = 0\}, \tag{2.8}$$

which are the set of states detected by W and the set of product states with zero expectation value[6] on W, respectively. Given two entanglement witnesses $W_1, W_2 \in \mathcal{W}$, W_1 is finer than W_2 if $\Delta_{W_2} \subset \Delta_{W_1}$; i.e., if W_1 detects more entangled states than W_2. If there is no witness finer than W, then W is optimal. In terms of Π_W, optimal entanglement witnesses are those for which, for any $\varepsilon > 0$ and any operator $P \succeq 0$ with support orthogonal to Π_W, the operator $W - \lambda P \notin \mathcal{W}$; i.e., there exists a product vector $|e', f'\rangle$ for which $\langle e', f'|W - \lambda P|e', f'\rangle < 0$, so $W - \lambda P$ is not an EW. Consequently, if Π_W spans the whole Hilbert space, then W is optimal [Lew+00]. We denote by $\mathrm{Opt}(\mathcal{W})$ the set of optimal entanglement witnesses.

There is a class of entanglement witnesses which is much easier to characterize: these are called decomposable witnesses. A decomposable EW $W \in \mathcal{W}$ has the form $W = P + Q^{T_B}$, where $P, Q \succeq 0$ (it is equivalent to take partial transposition on Alice instead of Bob). If this decomposition is not possible, the witness is called indecomposable. Notice the similarities with the notion of decomposable maps, first introduced in [Stø63, Wor76]. Decomposable EWs are those that are translated from decomposable maps via the Choi-Jamiołkowski-Sudarshan isomorphism [Jam72, Cho75].

Geometrically, one has the inclusions $\mathrm{Ext}(\mathcal{W}) \subsetneq \mathrm{Opt}(\mathcal{W}) \subsetneq \partial\mathcal{W}$ [SSŻ09], where $\partial\mathcal{W}$ is the boundary of $\mathcal{W}$ and $\mathrm{Ext}(\mathcal{W})$ is the set that generates extremal rays in $\mathcal{P}$. Each of these inclusions is strict.[7] Note, however that, although extremal (or even exposed[8]) EWs form proper subsets of $\mathrm{Opt}(\mathcal{W})$, they are sufficient to detect all entangled states [SSŻ09, HK11, CS14]. Nevertheless, the definition of optimal EWs is operational, in the sense that it can be recast into an efficient algorithm that brings any $W \in \mathcal{W}$ into an optimal one [Lew+00]. Hence, optimal EWs constitute a useful tool in entanglement theory.

Relating Positive Maps and EWs

The concepts defined for EWs can be recast in terms of positive maps via the Choi-Jamiołkowski-Sudarshan isomorphism [Jam72, Cho75], which relates the set $\mathcal{L}(\mathcal{M}_\lceil, \mathcal{M}_{\lceil'})$ of linear maps from M_d to $M_{d'}$ and the set $M_d \otimes M_{d'}$. Such isomorphism

---

[6] Note that Π_W does not form a subspace; in fact, it can be a finite set.

[7] As an example of $W \in \partial\mathcal{W} \setminus \mathrm{Opt}(\mathcal{W})$, consider the line segment $W(p) = pW_+ + (1-p)W_- \in M_2 \otimes M_2$ and consider the Bell basis $|\psi_\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\phi_\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. Pick $W_\pm = |\psi_\pm\rangle\langle\psi_\pm|^{T_B} \in \mathrm{Ext}(\mathcal{W})$. For any $p \in [0, 1/2) \cup (1/2, 1]$, $W \in \mathcal{W}$, whereas $W(1/2) \succeq 0$. Consequently, $W(p) \notin \mathrm{Opt}(\mathcal{W})$ for any $0 < p < 1$. Hence, by moving to one of the extremes of the segment, $W(p)$ can be optimized. $W(p) \in \partial\mathcal{W}$ because for every $p \in [0, 1]$ and for any $\varepsilon > 0$, $\mathcal{W}(p) - \varepsilon|\phi_+\rangle\langle\phi_+|^{T_B} \notin \mathcal{W}$.

As an example of $W \in \mathrm{Opt}(\mathcal{W}) \backslash \mathrm{Ext}(\mathcal{W})$, a decomposable witness of the form $W = Q^{T_A}$ with $Q \in M_2 \otimes M_2$, $Q \succeq 0$ and $\mathrm{supp}(Q)$ being a Completely Entangled Subspace (CES) is optimal [Lew+00]; however it is not extremal if $\mathrm{rank}(Q) > 1$. A CES is a subspace containing no product vectors (see e.g. [ATL11]).

[8] Exposed EWs form a subset of $\mathrm{Ext}(\mathcal{W})$ [HK11]. All extremal decomposable EWs are exposed [CS14].

sends $\mathcal{P}$ to the cone of positive maps and $\mathcal{W}$ to the set of positive, but not completely positive, maps. Interestingly, a positive map gives a more powerful necessary condition for separability than its corresponding EW.[9] On the other hand, entanglement witnesses correspond to quantum observables, whereas positive, but not completely positive, maps are unphysical. The Structural Physical Approximation (SPA) (see e.g. [HE02, Aug+14]) allows one to overcome this difficulty by mixing a given positive map Λ with the completely depolarizing channel, until the result is a completely positive map: $\Lambda(p) = p\Lambda + (1-p)D$, where $D(X) = \mathrm{Tr}(X)\mathbb{1}_{\mathrm{d}}/d$ is the completely depolarizing channel and $0 \leq p \leq 1$. Clearly, there exists a largest p for which $\Lambda(p)$ is a CP map, denoted p^*. $\Lambda(p^*)$ is then called the SPA of Λ.

Via the Choi-Jamiołkowski-Sudarshan isomorphism one formulates the SPA in terms of EWs: the SPA to an EW $W \in \mathcal{W}$ is

$$W(p_*) = p_* W + (1-p_*)\frac{\mathbb{1}_{d_A d_B}}{d_A d_B}, \tag{2.9}$$

where $p_*^{-1} = 1 + d_A d_B |\lambda_{\min}|$ and $\lambda_{\min}$ is the minimal eigenvalue of W, which is negative.

2.2 Nonlocality

Nonlocality [Bra+14] is a central concept in quantum information theory. In 1964, Bell proved that some predictions of quantum theory cannot be explained through a Local Hidden Variable Model (LHVM) [Bel64], ruling out the possibility that quantum physics was an incomplete theory because of the existence of inaccessible (hidden) variables that would determine with certainty the outcome of measurements performed on a quantum system.

Local models are those that arise naturally within our everyday experience with the classical world. Physicists considered, after the formulation of the EPR paradox [EPR35], whether they could provide an alternative explanation to quantum physics which would be complete and more intuitive, until in 1964 Bell showed that the two of them were in contradiction. Years after, Alain Aspect demonstrated, with an experiment in 1982, that Nature does not admit a LHVM [AGR82].

It is worth mentioning that three −almost simultaneous− landmark experiments had been performed shortly after writing this Thesis, in Delft [Hen+15], Vienna [Giu+15] and Illinois [Sha+15], proving that QT is incompatible with any LHVM theory beyond any reasonable doubt, by closing all the so-called loopholes that one can close in an experiment.

[9] The typical example is the transposition map, which detects all $2 \otimes 2$ and $2 \otimes 3$ states, whereas its corresponding entanglement witness detects just a subset of them [HHH96].

2.2.1 The Device-Independent Formalism

Although a Bell experiment was initially designed to test a fundamental question (whether Nature is nonlocal), we typically present it as a game: a Bell experiment involves two or more parties, which may have interacted in the past, located in space-like separated regions, each of them having access to their share of a physical system, for example, a source of entangled photons. Independently of the state of the system, each party chooses which measurement to perform on their subsystem and gets a result. Thus, each party can be treated as a black box with an input which corresponds to the choice of a measurement and an output that tells its result; nothing is assumed about the internal working of the device nor the object they are measuring.

We label the inputs of the n parties by $\vec{x} = (x_0, \ldots, x_{n-1})$ and the outputs by $\vec{a} = (a_0, \ldots, a_{n-1})$. The labelling of $\vec{x}$ encodes the different tunable parameters relevant for the experiment (i.e., the measurement choice) and the labelling of $\vec{a}$ encodes the possible readouts of the experiment. The way that this labelling is assigned is irrelevant to the Bell's experiment and labels do not even have to correspond to physical quantities.

In the DI framework, one assumes that the parties have Independent and Identically Distributed (IID) preparations of the experiment, in the sense that after repeating it many times, they can infer the underlying conditional probabilities of the outputs given the inputs $P(\vec{a}|\vec{x})$ from the statistics collected from the experiment.[10]

It is also required that the choice of inputs is independent of the state of the system, an assumption often referred to as the *free will* assumption.[11] Sometimes this assumption is partially fulfilled, but it can be remediated through a protocol called randomness amplification (see Chap. 6).

Depending on the physical principles that we take into consideration, some probability distributions $P(\vec{a}|\vec{x})$ may contradict them, so not every mathematically consistent P may be compatible with a given physical principle.

2.2.2 A Geometric Approach to Correlations

In general, we will consider a scenario where n parties, each having access to m measurements which have d outcomes, are performing a Bell experiment, and we denote this Bell scenario by (n, m, d). We denote by $\mathcal{M}_{x_i}^{(i)}$ the x_i-th measurement

[10] There exist other frameworks in which can study nonlocality, such as the ones considered in Sect. 5.5.1. In this Thesis, we consider the typical framework in which parties perform a single measurement on a single copy of their resource and repeat the experiment in the same conditions.

[11] For instance, if Alice has to choose between measuring the spin of a electron in the direction x and measuring the spin in the direction z, her choice has to be independent on the state of the electron; in other words, the electron cannot know what Alice is going to measure. This situation is relevant in the framework of quantum cryptography tasks, where the manufacturer of the devices and/or the provider of entangled particles is untrusted and can use this information to fake the statistics $P(\vec{a}|\vec{x})$, compromising security (see Sect. 6.3.2).

performed by i-th party. The object under consideration is then

$$P(a_0, \ldots, a_{n-1}|x_0, \ldots x_{n-1}), \quad 0 \leq a_i < d, \quad 0 \leq x_i < m. \tag{2.10}$$

Geometrically, one can think of (2.10) as a vector with $(md)^n$ coordinates, each corresponding to a possible combination of $a_0, \ldots, a_{n-1}|x_0, \ldots x_{n-1}$. Let us name such vector $\vec{P}$.

The problem of which probability distributions $\vec{P}$ are sound has been considered since more than a century ago; way before the genesis of modern probability, theory by George Boole, in his theory of *conditions of possible experience* [Boo62], but it was Froissart who reintroduced it in terms of nonlocality and physical principles from the geometric perspective [Fro81] that allows a systematic characterization of correlations in terms of convex sets.

Mathematical Constraints

Since $\vec{P}$ has to be a valid probability distribution, it has to fulfill Kolmogórov's axioms of Probability Theory [Kol33]. Consequently, the elements of $\vec{P}$ have to be non-negative and normalized.

Hence, only $m^n(d^n - 1)$ components of $\vec{P}$ remain independent and the non-negativity constraints $P(a_0, \ldots, a_{n-1}|x_0, \ldots x_{n-1}) \geq 0$ define a region in space, which we denote $\mathbf{P}$.

Note that $\mathbf{P}$ is a convex set. Recall that a set $\mathbf{P}$ is convex if, and only if, for all $\vec{P}_1, \vec{P}_2 \in \mathbf{P}$ the line segment $\vec{P}(\lambda) = \lambda \vec{P}_1 + (1 - \lambda)\vec{P}_2$ (where $\lambda \in [0, 1]$) belongs to $\mathbf{P}$. $\vec{P}(\lambda)$ is called a convex combination of $\vec{P}_1$ and $\vec{P}_2$. $\mathbf{P}$ is convex because it is the intersection of a number of half-spaces (non-negativity conditions) and a number of affine subspaces (normalization conditions). The intersection of convex sets is a convex set.

We shall name a set defined as a finite intersection of half-spaces a convex polyhedra. If, in addition, it is bounded, we shall call it a convex polytope; $\mathbf{P}$ is an example of a convex polytope.

Every convex polytope admits a dual description: On the one hand, it can be fully characterized either as the intersection of a minimal number of half-spaces (the intersection of the polytope with the hyperplane defining one of such half-spaces is called *facet*; the intersection of the polytope with a hyperplane defining any half-space which contains it and touching the boundary is called *face*). On the other hand, it can be equivalently characterized by listing all its extreme points (the ones that cannot be written as convex combinations of others with $\lambda \in (0, 1)$; such points are called *vertices*).

It is computationally a hard problem to go from one description to the other, especially in large dimension spaces.[12] Its complexity is $O(n^{\lfloor D/2 \rfloor} + n \log n)$, where n is the number of vertices (inequalities) and D the dimension of the affine space; $\lfloor \cdot \rfloor$ is the floor function [Cha93].

[12] A convex polyhedra admits this dual description as well, if we allow for vertices to be at infinity. Some programs avoid this by working in the Projective space instead of the Affine space, by treating points as rays, for example [Fuk14].

The No-Signalling Set

It is a natural postulate in a physical theory that the speed at which information travels is bounded; in particular, to be consistent with Einstein's relativity theory, information cannot travel faster than light. Therefore, two events happening at spacelike separated regions cannot instantaneously affect each other. This impossibility of instantaneous communication is known as the No-Signalling (NS) principle. In terms of $\vec{P}$, the NS principle has a simple formulation: the choice of measurement performed by one of the parties cannot influence the statistics observed by the rest; i.e., for all $x_i \neq x_i'$,

$$\sum_{a_i} P(\vec{a}|\vec{x}) = \sum_{a_i} P(\vec{a}|\vec{x}\,'), \tag{2.11}$$

where $\vec{x} = (x_0, \ldots, x_i, \ldots, x_{n-1})$ and $\vec{x}\,' = (x_0, \ldots, x_i', \ldots, x_{n-1})$. Note that when the *NS* holds, the marginal probability distribution

$$P(a_0, \ldots, \widehat{a_i}, \ldots, a_{n-1}|x_0, \ldots, \widehat{x_i}, \ldots, x_{n-1}) = \sum_{a_i} P(\vec{a}|\vec{x}) \tag{2.12}$$

is well defined (the notation $\widehat{\cdot}$ indicates that the element under the hat is missing). Observe that condition (2.11) can be applied recursively to any subset of parties.

The resulting region for which probabilities are no-signalling is also a convex polytope, as it is the intersection of $\mathbf{P}$ with the vector subspaces given by (2.11). This set is known as the no-signalling polytope and we denote it $\mathbf{P}_{NS}$. The number of independent components[13] of any $\vec{P} \in \mathbf{P}_{NS}$ is reduced to $(m(d-1)+1)^n - 1$. The facets of $\mathbf{P}_{NS}$ are easy to specify, as they are the non-negativity constraints subjected to normalization and NS constraints. Its vertices, known as PR-boxes [PR94], are hard to compute in general, and they are known only in few scenarios [Bar+05, Fri12].

The Quantum Set

When $\vec{P}$ is obtained from a quantum state on which local quantum measurements are performed, one obtains a different set of possible correlations, the quantum set of correlations fulfilling Quantum Theory (QT), which we denote by $\mathbf{Q}$.

Following the axioms of quantum physics, $\vec{P}$ has to be obtained via Born's rule:

$$P(a_0, \ldots, a_{n-1}|x_0, \ldots, x_{n-1}) = \mathrm{Tr}\left(\rho \cdot \bigotimes_{i=0}^{n-1} \Pi^{(i)}_{a_i|x_i}\right), \tag{2.13}$$

---

[13] This follows from a simple combinatorical argument: The number of independent components of $\vec{P} \in \mathbf{P}_{NS}$ is given by the normalization conditions of probabilities and the number of different marginals because of the NS principle: For every party, one can choose whether to measure it or not; if it is indeed measured, there are m possible measurements to perform, and for each measurement there are $d-1$ outcomes to specify (because the last outcome can always be recasted as a function of the rest by means of the normalization conditions). If nobody measures, there is no value needed to specify, so we rule out this possibility.

where $\rho \in \mathcal{D}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$ of unspecified dimension and $\{\Pi^{(i)}_{a_i|x_i}\}$ define a Positive-Operator Valued Measure (POVM) on the i-th party. A POVM fulfills that its POVM elements, $\Pi^{(i)}_{a_i|x_i}$, are positive semi-definite and they form a resolution of the identity: $\sum_{a_i} \Pi^{(i)}_{a_i|x_i} = \mathbb{1}^{(i)}$. Note that, since the dimension of $\mathcal{H}$ is unconstrained, one can assume, without loss of generality, that ρ is in a pure state and that the POVM is in fact a von Neumann (Projective Measurement (PM)) measurement; i.e., the POVM elements are, in addition, pairwise orthogonal projectors.

Because $\dim_{\mathbb{C}} \mathcal{H}$ is unconstrained, $\mathbf{Q}$ forms a convex set. However, it is not a polytope and its boundary is unknown in practically all cases. Surprisingly, it turns out that although $\mathbf{Q}$ is contained in $\mathbf{P}_{NS}$, a fact that follows directly from (2.13) fulfilling (2.11), it is strictly smaller [PR94]. It remains today an open question *What should one require, in addition to the no-signalling principle, in order to recover quantum correlations?* To this aim, several operational principles have been proposed: Non-trivial communication complexity [Dam99, Bra+06], no advantage for nonlocal computation [Lin+07], information causality [Paw+09], macroscopic locality [NW10], local orthogonality [Fri+13]. However, each of them defines a superset of $\mathbf{Q}$.

It is possible to approximate $\mathbf{Q}$ with a convergent hierarchy of spectrahedrons[14] $\mathbf{Q} \subseteq \cdots \subseteq \mathbf{Q}_2 \subseteq \mathbf{Q}_{1+AB} \subseteq \mathbf{Q}_1$ [NPA08]. Interestingly, it was recently shown that a generalization of the level of the Navascués–Pironio–Acín (NPA) Hierarchy $1 + AB$ to the multipartite case recovers all the operational principles mentioned above (except for information causality, which remains unknown) [Nav+15].

The LHVM Set

Imagine a Bell experiment with $n = 2$ parties. In general, the obtained statistics $P(ab|xy)$ will not be of the form $P(a|x)P(b|y)$. This lack of independence is not surprising, nor does it imply an influence of one party to another; Alice and Bob may simply have established some correlation in the past, when they were allowed to interact or to agree on a common strategy. The idea behind a local theory, however, is that whatever interaction or factor relevant to both outcomes, described by a variable λ, must decouple the two probabilities, so that, if we know λ, they become independent: $P(ab|xy\lambda) = P(a|x\lambda)P(b|y\lambda)$.

Observe that, when λ is known, the outcome of Alice does not depend on the choice of input of Bob nor on his result, and vice-versa.

In general this λ may be inaccessible to us, and we call it *hidden variable*. In fact, λ may not be the same in every round of the Bell experiment, as it may include not fully controllable physical quantities, or the parties may agree to change their strategy at every round. Hence, it is natural to describe it via a probability distribution $p(\lambda)$.

This is what motivates the definition of a Local Hidden Variable Model (LHVM): We say that $\vec{P}$ admits a LHVM if it can be written in the form

[14] A spectrahedron is the feasible set of a Semi-Definite Program (SDP).

$$P(\vec{a}|\vec{x}) = \int_\Lambda p(\lambda) \prod_{i=0}^{n-1} P(a_i|x_i\lambda)\mathrm{d}\lambda, \tag{2.14}$$

where Λ is the space of hidden variables, $p(\lambda) \geq 0$ and $\int_\Lambda p(\lambda)\mathrm{d}\lambda = 1$.

The set of probabilities admitting the form (2.14) is again a polytope, known as the local polytope and we denote it $\mathbf{P}_L$. The functions $P(a_i|x_i\lambda)$ are called local *response functions* and they need not be deterministic. However, every probability distribution can be expressed as a convex combination of deterministic events (one for each outcome and the weight of the convex combination corresponds to the probabilities of the events). These deterministic events are delta functions $\delta(a_i, f_i(x_i, \lambda))$, where f_i is some deterministic function that takes the information available to the i-th party, namely, x_i and λ, and produces an outcome in $\{0, \ldots, d-1\}$. Consequently, a LHVM admits also the form [Fin82]

$$P(\vec{a}|\vec{x}) = \int_\Lambda q(\lambda) \prod_{i=0}^{n-1} \delta(a_i, f_i(x_i, \lambda))\mathrm{d}\lambda, \tag{2.15}$$

for a (possibly different) probability distribution $q(\lambda)$.

Equation (2.15) already gives information on how to construct the vertices of $\mathbf{P}_L$, for they are the probability functions of the form $P(\vec{a}|\vec{x}) = \prod_{i=0}^{n-1} \delta(a_i, \tilde{f}_i(x_i))$, with $\tilde{f}_i(x_i) \in \{0, \ldots, d-1\}$; i.e., the ones that cannot be expressed as a convex combination of λ. Varying the possible choices of $\tilde{f}_i(x_i)$ we obtain the $(md)^n$ different vertices of $\mathbf{P}_L$.

$\mathbf{P}_L$ is a subset of $\mathbf{Q}$ because every probability of the form (2.14) can be constructed with a fully separable state; and it is a strictly smaller set because there are quantum states and measurements that produce $\vec{P}$'s which are outside $\mathbf{P}_L$ [Bel64]. These probability distributions are called nonlocal.

The half-spaces containing $\mathbf{P}_L$ are called *Bell inequalities*. If a Bell inequality corresponds to a facet of $\mathbf{P}_L$, we shall name it *tight* Bell inequality.[15] If a Bell inequality is violated by some $\vec{P} \in \mathbf{P}_{NS}$ we call it *non-trivial*. Finding all Bell inequalities is an extremely difficult task and only a few scenarios have been completely solved, none of them for more than 3 parties[16] [PS01, Pir14].

Since the labelling of parties, measurements and outcomes is arbitrary, the different sets of correlations obey some symmetries (e.g. shuffling the outcomes of a certain measurement in a Bell inequality will lead to another Bell inequality) and Bell inequalities can be grouped (see [Ros15], Chapter III) in classes.[17] In the $(2, 2, 2)$ scenario, the only non-trivial class of Bell inequalities is the one derived by Clauser,

[15] Note, however, that in polytope theory, a tight inequality is one which just touches the polytope.

[16] See also [Fri12] for an interesting duality relation between the vertices and facets of $\mathbf{P}_{NS}$ and $\mathbf{P}_L$ in the $(n, 2, 2)$ scenario. A repository of the currently known Bell inequalities can be found in [RBG14].

[17] The same argument applies to PR-boxes [Bar+05].

Horne, Shimony and Holt [Cla+69] whereas in the $(3, 2, 2)$ scenario one finds 46 different classes [Śli03].

2.2.3 Multipartite Nonlocality

Both the definition of a fully separable state (cf. Eq. (2.2)) and a LHVM (cf. Eq. (2.14)) look similar. Analogously to the case of entanglement, in the multipartite scenario, various degrees of nonlocality are possible. However, the case of nonlocality is subtler, in the sense that one should specify what are the rules for the response functions of more than one party.

Genuine multipartite nonlocality was first introduced by Svetlichny in 1987 [Sve87]. Analogously to the biseparable case, Svetlichny defined a 3-partite probability distribution to be bi-local if it was of the form

$$
\begin{aligned}
P(abc|xyz) = &\int_\Lambda p_{AB|C}(\lambda)P_{AB}(ab|xy\lambda)P_C(c|z\lambda)\mathrm{d}\lambda \\
&+ \int_\Lambda p_{AC|B}(\lambda)P_{AC}(ac|xz\lambda)P_B(b|y\lambda)\mathrm{d}\lambda \\
&+ \int_\Lambda p_{BC|A}(\lambda)P_{BC}(bc|yz\lambda)P_A(a|x\lambda)\mathrm{d}\lambda.
\end{aligned} \tag{2.16}
$$

Operationally, terms such as $P_{AB}(ab|xy\lambda)$ mean that Alice and Bob can exchange an arbitrary amount of communication between themselves, but not with Charlie. So, $P_{AB}(ab|xy\lambda)$ can be any mathematically sound probability distribution; in particular, a signalling one. This, however, leads to grandfather-type paradoxes [Ban+13].

There are basically two possibilities to avoid these issues: one is to require that the probability distributions $P_{AB}(ab|xy\lambda)$ satisfy the no-signalling constraints (2.11) [Alm+10]; such correlations are called No-Signalling Bi-Local (NSBL). Another one is to require that the correlations of the form $P_{AB}(ab|xy\lambda)$ appearing in (2.16) are time-ordered (e.g. Alice can signal to Bob or vice-versa, but not both at the same time); such correlations are called Time-Ordered Bi-Local (TOBL) [Gal+12]. All such constraints define convex polytopes and one has the chain of inclusions $\mathbf{P}_L \subsetneq \mathbf{P}_{NSBL} \subsetneq \mathbf{P}_{TOBL} \subsetneq \mathbf{P}_{\text{Svetlichny}} \subsetneq \mathbf{P}$ [Ban+13].

In the general case of n parties, having in mind the different flavors of multipartite locality stemming from the considerations mentioned above, one defines a probability distribution $P(\vec{a}|\vec{x})$ to be K-local if it is of the form

$$
P(\vec{a}|\vec{x}) = \sum_{S\in\mathcal{S}_K} p_S \int_\Lambda p_S(\lambda)\prod_{k=1}^{K} p_k(\vec{a}_{|S_k}|\vec{x}_{|S_k}\lambda)\mathrm{d}\lambda. \tag{2.17}
$$

Analogously to the case of (2.3), if $K = 2$ we will say that $\vec{P}$ is bi-local, whereas if $K = n$, we shall name it fully local. If $\vec{P}$ cannot be written as (2.17) with $K = 2$, then it is called Genuinely Multipartite Nonlocal (GMN).

Monogamy of Correlations

A nonlocal probability distribution $\vec{P} \notin \mathbf{P}_L$ will violate some Bell inequality. Geometrically, the farther $\vec{P}$ is from $\mathbf{P}_L$, the higher its violation will be. The amount of violation (up to normalization) of a Bell inequality is often taken as a measure of nonlocality.[18] Physical principles (such as quantum mechanics or no-signalling theories) prevent nonlocality from being distributed arbitrarily between several parties. Entanglement does also display these kind of constraints, known as monogamy relations [CKW00]. In the case of nonlocal correlations, monogamies of correlations impose a tradeoff between the violation of a Bell inequality between two sets of parties, **A**and **B** and the same Bell inequality between the first set **A** and another one **C**.

As an example, let us consider 3 parties ABC and the Clauser–Horne–Shimony–Holt (CHSH) inequality [Cla+69]:

$$I_{AB} = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle, \tag{2.18}$$

where each correlator $\langle A_xB_y\rangle$ is defined as follows: $P(a = b|xy) - P(a \neq b|xy)$. The classical bound for which I_{AB} defines a facet of $\mathbf{P}_L$ for the $(2, 2, 2)$ scenario is $I_{AB} \leq 2$. If Alice, Bob and Charlie share arbitrary quantum resources, then $I_{AB}^2 + I_{AC}^2 \leq 8$ [TV06]. Even if they share a No- Signalling resource, a monogamy relation holds, namely $|I_{AB}| + |I_{AC}| \leq 4$ [Ton09].

2.2.4 Local Models

Both entanglement and nonlocality are valuable resources for quantum information theory, although inequivalent ones. Because every separable quantum state produces local correlations, entanglement is necessary for nonlocality. In the case of pure states, Gisin showed that every entangled pure state can display nonlocal correlations [Gis91]. In the case of mixed states, there are bipartite states, known as Werner states, for which, no matter what measurements are performed on them, its statistics are of the form (2.14) [Wer89]; i.e., they admit a Local Hidden Variable Model.

In general, very little is known about which quantum states admit a local model [ADA14] essentially because one has to explicitly construct the response functions $P(a_i|x_i\lambda)$. In the multipartite case, even less is known: For example, when one considers GME states, even those pure, it is unknown whether all GME states are GMN

[18] There is another formulation of measure of nonlocality formulated by Elitzur–Popescu–Rohrlich (EPR2) [EPR92], which measures the nonlocal content of $\vec{P}$ by decomposing it as a convex combination of a no-signalling distribution $\vec{P}_{NS} \in \mathbf{P}_{NS}$ and a local distribution $\vec{P}_L \in \mathbf{P}_L$ with maximal p: $\vec{P} = p\vec{P}_{NS} + (1-p)\vec{P}_L$.

[Bra+14]. In Chap. 5, we address this question and show that there exist GME states that do not display GMN.

2.3 Systems of Indistinguishable Particles

So far, we have considered entanglement and nonlocality in the setting of n spacelike separated particles belonging to Alice, Bob, Charlie, etc. One can as well consider the characterization of quantum correlations at short distances, where the particles involved (e.g. photons, electrons) have an indistinguishable character that has to be taken into account.

When one is given a system $\rho_{\mathbf{A}}$ of indistinguishable particles, then $\rho_{\mathbf{A}}$ remains invariant under any permutation of its subsystems; otherwise they could be distinguished.

Consider $\mathfrak{S}_n$, the group of permutations of n elements. Consider as well the n-partite Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$. $\mathfrak{S}_n$ acts on $\mathcal{H}$ by means of permuting each component of the computational basis of $\mathcal{H}$ and this action is extended by linearity to every element of $\mathcal{H}$. This action has a natural representation that assigns to each $\sigma \in \mathfrak{S}_n$ a permutation matrix $\Pi_\sigma$defined as

$$\Pi_\sigma|i_0\rangle \otimes \cdots \otimes |i_{n-1}\rangle = |i_{\sigma^{-1}(0)}\rangle \otimes \cdots \otimes |i_{\sigma^{-1}(n-1)}\rangle. \tag{2.19}$$

Definition 2.5 A quantum state $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{H})$ is Permutationally Invariant (PI) if, for any $\sigma \in \mathfrak{S}_n$

$$\rho_{\mathbf{A}} = \Pi_\sigma \rho_{\mathbf{A}} \Pi_\sigma^\dagger. \tag{2.20}$$

2.3.1 *The Block Decomposition of a Permutationally Invariant Operator. Schur–Weyl Duality*

Given a permutationally invariant quantum state $\rho_{\mathbf{A}}$, it turns out that one can choose a basis of $(\mathbb{C}^d)^{\otimes n}$ such that its form is extremely simplified: In this basis, $\rho_{\mathbf{A}}$ is block-diagonal, and the size of each block is exponentially small compared to the $d^n \times d^n$ whole matrix $\rho_{\mathbf{A}}$ expressed in the computational basis. The reason for this simplification lies on a mathematical result known as Schur–Weyl duality, which says that $(\mathbb{C}^d)^{\otimes n}$ can be naturally decomposed in terms of irreducible representations of the groups $\mathfrak{S}_n$and $\mathcal{U}_d$(the group of $d \times d$ unitary matrices). This construction is explained in detail in Appendix A.

Given a PI quantum state $\rho_{\mathbf{A}}$, it decomposes $\mathcal{H}$ into the following direct sum (*cf.* Theorem A.9):

$$(\mathbb{C}^d)^{\otimes n} \cong \bigoplus_{\lambda \vdash (d,n)} \mathcal{K}_\lambda \otimes \mathcal{H}_\lambda, \tag{2.21}$$

where λ runs over all partitions of n with at most d elements and $\oplus$ denotes direct sum. $\mathcal{K}_\lambda$ is known as the multiplicity space. In the basis (2.21) $\rho_{\mathbf{A}}$ is block-diagonal.

The Qubit Case

If $d = 2$, the construction of (2.21) can be explicitly given and it corresponds to the case of n spin-1/2 particles. In this case, λ would run over the partitions of n with, at most, 2 elements, so one can translate (2.21) to a language closer to Physics:

$$(\mathbb{C}^2)^{\otimes n} \cong \bigoplus_{J=J_0}^{n/2} \mathcal{K}_J \otimes \mathcal{H}_J. \tag{2.22}$$

Usually, $\mathcal{H}_J$ are called the spin Hilbert spaces, as $\dim \mathcal{H}_J = 2J + 1$ and $\mathcal{K}_J$ the multiplicity spaces, which account for the different possibilities for the n qubits to obtain to a spin-J state. The multiplicity spaces are of dimension 1 if $J = n/2$ and

$$\dim \mathcal{K}_J = \binom{n}{n/2 - J} - \binom{n}{n/2 - J - 1} \tag{2.23}$$

otherwise.

A permutationally invariant n-qubit state $\rho_{\mathbf{A}}$, in the basis given by (2.21) takes the form

$$\rho_{\mathbf{A}} = \bigoplus_{J=J_0}^{n/2} \frac{p_J}{\dim \mathcal{K}_J} \mathbb{1}_J \otimes \rho_J, \tag{2.24}$$

where p_J forms a probability distribution and ρ_J are the so-called spin states, which can be viewed as density operators of $\mathcal{D}(\mathbb{C}^{2J+1})$.

Hence, a permutationally invariant n-qubit state $\rho_{\mathbf{A}}$ is uniquely determined by specifying its blocks ρ_J, an amount of information exponentially small compared to a general n-qubit state.

The following basis automatically gives a projection onto the J-th block (defining $m = n - 2J$; note that m is always an even number):

$$\{|D_{2J}^k\rangle \otimes |\psi^-\rangle^{\otimes m/2}\}_{k=0\ldots 2J}, \tag{2.25}$$

where $|D_{2J}^k\rangle$ is the $2J$ qubit Dicke state with k excitations (*cf.* Sect. 2.3.2, Eq. (2.27)) and $|\psi^-\rangle$ is the singlet state

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.26}$$

2.3.2 Symmetric States

The so-called symmetric states (or Dicke states) were first introduced by R.H. Dicke in 1954, when studying the emission of light from a cloud of atoms [Dic54]. He found that, when the atoms were in certain entangled states, the intensity of radiation scaled quadratically with the number of atoms, whereas if they were radiating independently, this intensity scaled linearly. Since then, Dicke states have been widely studied and they have been produced in experiments.

Dicke states can be defined either as the simultaneous eigenstates of the total angular momentum operators $J_z = 1/2 \sum_i \sigma_z^{(i)}$ and J^2, where $\sigma_z^{(i)}$ is the Pauli matrix acting on site i and $J^2 = J_x^2 + J_y^2 + J_z^2$, or as symmetric superpositions of states with the same number of excitations (throughout this Thesis we shall consider qubits, so that a Dicke state is defined by n qubits and k excitations and denoted $|D_n^k\rangle$):

$$|D_n^k\rangle = \binom{n}{k}^{-1/2} \sum_{\sigma} \sigma(|0\rangle^{\otimes n-k}|1\rangle^{\otimes k}). \tag{2.27}$$

Dicke states form an important subclass of permutationally invariant states, and they correspond to the first block in the decomposition (2.21); i.e., the one corresponding to the partition $\lambda = (n)$. They span the so-called *symmetric space* and the symmetric space is closed[19] under the action of $U^{\otimes n}$ for any unitary U.

We shall denote the symmetric space by $\mathcal{S}(\mathcal{H}) := \mathrm{Span}\{|D_n^k\rangle\}_{k=0\ldots n}$ and we will call a density operator symmetric if $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{S}(\mathcal{H}))$. In the case of n qubits, a symmetric state $\rho_{\mathbf{A}}$ cannot have rank greater than $n+1$, as these are the elements in (2.27).

PPT Entanglement in the Symmetric States

The multipartite PPT criterion and, in general, any entanglement criterion based on positive, but not completely positive maps, is hard to compute in systems of large n as, even if it is efficient to test on a single bipartition $S|\overline{S}$, the number of bipartitions scales as 2^n. However, for permutationally invariant states, this is greatly simplified: Now the criterion "n-separable implies $(\mathbb{1}_S \otimes \bigotimes_{a_i \in \overline{S}} \Lambda_{A_i})[\rho] \succeq 0$" will be the same, regardless of which particular parties are picked in S. Hence, it only depends on the number of parties in S, denoted $|S|$. Hence, if a PI state is n-separable, only $n-1$ conditions need to be checked. In the particular case $\Lambda = T$, only $\lfloor n/2 \rfloor$ are necessary, as global transposition preserves the positivity of the whole state. This motivates the definition of partial transposition for symmetric states as ρ^{Γ_k}, where $k = |\overline{S}|$ is the number of parties that have been transposed. A state which is PPT with respect to every bipartition will be called fully PPT.

[19] A nice way to see this is via the so-called Majorana representation [Maj32], which assigns a product state to every pure Dicke state; when taking a superposition of all permutations of this product state, one recovers the original Dicke state. For $d = 2$ this assignment is unique and it can be easily visualized in the Bloch sphere. Then, the action of $U^{\otimes n}$ is just a rotation of the Bloch sphere [Mar11].

The zoo of separability classes for symmetric states is also greatly simplified: Symmetric states are either n-separable, or GME, and there is no other possibility. This makes them even more interesting, as proving that a general quantum state is GME might turn into a difficult task.

Applying Γ_k, transposition on k subsystems, breaks the symmetry of ρ: It is false in general that $\rho^{\Gamma_k} \in \mathcal{D}(\mathcal{S}(\mathcal{H}_{\mathbf{A}}))$. However, the symmetries in the partially transposed subsystems and the untouched ones are kept, so that $\rho^{\Gamma_k} \in \mathcal{D}(\mathcal{S}(\mathcal{H}_S) \otimes \mathcal{S}(\mathcal{H}_{\overline{S}}))$, for $k = |S|$. In the case of qubits, this means that the rank of ρ^{Γ_k} is $O(n^2)$, more precisely, bounded by $(n + 1 - k)(k + 1)$, so it is possible to keep track of the transformation Γ_k efficiently. We shall denote by $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathcal{H})$the set of density operators acting on $\mathcal{H}$ corresponding to symmetric states PPT with respect to every bipartition.

It was known that all PPT symmetric states of two and three qubits are fully separable [Eck+02]. The reason is that there is only one possible nontrivial bipartition to consider: (1, 1) and (2, 1), respectively, and then the sufficiency condition for the PPT criterion carries, as one can think of $\mathcal{S}(\mathbb{C}^2) \otimes \mathcal{S}(\mathbb{C}^2)$ as $\mathbb{C}^2 \otimes \mathbb{C}^2$ and of $\mathcal{S}(\mathbb{C}^2)^{\otimes 2} \otimes \mathcal{S}(\mathbb{C}^2)$ as $\mathbb{C}^3 \otimes \mathbb{C}^2$. However it was an open question whether this result would still be true for systems of 4 qubits or more.

In the case of 5 and 6 qubits, Tóth and Gühne found examples of GME symmetric states which are PPT with respect to the most balanced partition $\lfloor n/2 \rfloor, \lceil n/2 \rceil$, although they would break the PPT condition with respect to some other bipartitions [TG09].

Genuine multipartite entanglement is considered to be the strongest form of entanglement, whereas PPT states are considered the weakest.[20] Almost paradoxically, it turns out that one can find fully PPT states which are also GME for more than 3 qubits, as we study in Chap. 3.

References

[ADA14] R. Augusiak, M. Demianowicz, A. Acín, Local hidden-variable models for entangled quantum states. J. Phys. A: Math. Theor. **47**(42), 424002 (2014). doi:10.1088/1751-8113/47/42/424002

[AGR82] A. Aspect, P. Grangier, G. Roger, Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedanken experiment: a new violation of Bell's inequalities. Phys. Rev. Lett. **49**(2), 91–94 (1982). doi:10.1103/PhysRevLett.49.91

[Alm+10] M.L. Almeida, D. Cavalcanti, V. Scarani, A. Acín, Multipartite fully nonlocal quantum states. Phys. Rev. A **81**(5), 052111 (2010). doi:10.1103/PhysRevA.81.052111

[20]It was shown in [HHH98] that bipartite PPT states cannot be distilled; i.e., no matter how many copies of a non-distillable state are available, there is no protocol that would produce a pure maximally entangled state $|\psi^+\rangle$. This is the reason why bound entanglement (i.e., entanglement of undistillable states) is considered the weakest form of entanglement.

Interestingly, a conjecture by Peres related the concepts of nonlocality and bound entanglement, claiming that all bound entangled states admit a local model. The intuition that bound entanglement is too weak to violate a Bell inequality was proven to be false both in the multipartite [VB12] and the bipartite [VB14] scenarios very recently.

[ATL11] R. Augusiak, J. Tura, M. Lewenstein, A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces. J. Phys. A: Math. Theor. **44**(21), 212001 (2011). doi:10.1088/1751-8113/44/21/212001. Featured with insights. Editor's choice: Highlights of 2011

[Aug+14] R. Augusiak, J. Bae, J. Tura, M. Lewenstein, Checking the optimality of entanglement witnesses: an application to structural physical approximations. J. Phys. A: Math. Theor. **47**(6), 065301 (2014). doi:10.1088/1751-8113/47/6/065301. Editor's choice: Highlights of 2014

[Ban+13] J.-D. Bancal, J. Barrett, N. Gisin, S. Pironio, Definitions of multipartite nonlocality. Phys. Rev. A **88**(1), 014102 (2013). doi:10.1103/PhysRevA.88.014102

[Bar+05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts nonlocal correlations as an information-theoretic resource. Phys. Rev. A **71**(2), 022101 (2005). doi:10.1103/PhysRevA.71.022101

[Bel64] J.S. Bell, On the Einstein-Podolsky-Rosen paradox. Physics **1**(3), 195–200 (1964)

[Ben+93] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993). doi:10.1103/PhysRevLett.70.1895

[Boo62] G. Boole, On the theory of probabilities. Philos. Trans. R. Soc. Lond. **152**, 225–252 (1862). doi:10.1098/rstl.1862.0015

[Bra+06] G. Brassard, H. Buhrman, N. Linden, A. Allan Méthot, A. Tapp, F. Unger, Limit on nonlocality in any world in which communication complexity is not trivial. Phys. Rev. Lett. **96**(25), 250401 (2006). doi:10.1103/PhysRevLett.96.250401

[Bra+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, Bell nonlocality. Rev. Mod. Phys. **86**(2), 419–478 (2014). doi:10.1103/RevModPhys.86.419

[BW92] C.H. Bennett, S.J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. **69**(20), 2881–2884 (1992). doi:10.1103/PhysRevLett.69.2881

[Car11] C. Carathéodory, Über den variabilitätsbereich der fourier'schen konstanten von ositiven harmonischen funktionen Italian. Rendiconti del Circolo Matematico di Palermo **32**(1) (1911)

[CB97] R. Cleve, H. Buhrman, Substituting quantum entanglement for communication. Phys. Rev. A **56**(2), 1201–1204 (1997). doi:10.1103/PhysRevA.56.1201

[Cha93] B. Chazelle, An optimal convex hull algorithm in any fixed dimension English. Discrete Comput. Geom. **10**(1), 377–409 (1993). doi:10.1007/BF02573985. ISSN: 0179-5376

[Cho75] M.-D. Choi, Completely positive linear maps on complex matrices. Linear Algebra Appl. **10**(3), 285–290 (1975). doi:10.1016/0024-3795(75)90075-0. ISSN: 0024-3795

[CKW00] V. Coffman, J. Kundu, W.K. Wootters, Distributed entanglement. Phys. Rev. A **61**(5), 052306 (2000). doi:10.1103/PhysRevA.61.052306

[Cla+69] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. **23**(15), 880–884 (1969). doi:10.1103/PhysRevLett.23.880

[CS14] D. Chruściński, G. Sarbicki, Entanglement witnesses: construction, analysis and classification. J. Phys. A: Math. Theor. **47**(48), 483001 (2014). doi:10.1088/1751-8113/47/48/483001

[Dam99] W. van Dam, Nonlocality and communication complexity. Ph.D. thesis, University of Oxford (1999)

[Dic54] R.H. Dicke, Coherence in spontaneous radiation processes. Phys. Rev. **93**(1), 99–110 (1954). doi:10.1103/PhysRev.93.99

[Dür+99] W. Dür, H.-J. Briegel, J.I. Cirac, P. Zoller, Quantum repeaters based on entanglement purification. Phys. Rev. A **59**(1), 169–181 (1999). doi:10.1103/PhysRevA.59.169

[Eck+02] K. Eckert, J. Schliemann, D. Bruß, M. Lewenstein, Quantum correlations in systems of indistinguishable particles. Ann. Phys. **299**(1), 88–127 (2002). doi:10.1006/aphy.2002.6268. ISSN: 0003-4916

[Edw95] R.E. Edwards, *Functional Analysis: Theory and Applications Dover*, Books on Mathematics (Dover Pub., 1995). ISBN: 9780486681436

[Eke91] A.K. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991). doi:10.1103/PhysRevLett.67.661

[EPR35] A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**(10), 777–780 (1935). doi:10.1103/PhysRev.47.777

[EPR92] A.C. Elitzur, S. Popescu, D. Rohrlich, Quantum nonlocality for each pair in an ensemble. Phys. Lett. A **162**(1), 25–28 (1992). doi:10.1016/0375-9601(92)90952-I

[Fin82] A. Fine, Hidden variables, joint probability, and the Bell inequalities. Phys. Rev. Lett. **48**(5), 291–295 (1982). doi:10.1103/PhysRevLett.48.291

[Fri+13] T. Fritz, A.B. Sainz, R. Augusiak, J.B. Brask, R. Chaves, A. Leverrier, A. Acín, Local orthogonality as a multipartite principle for quantum correlations. Nat. Commun. **4**, 2263 (2013)

[Fri12] T. Fritz, Polyhedral duality in Bell scenarios with two binary observables. J. Math. Phys. **53**(7), 072202 (2012). doi:10.1063/1.4734586

[Fro81] M. Froissart, Constructive generalization of Bell's inequalities English. Il Nuovo Cimento B **64**(2), 241–251 (1981). doi:10.1007/BF02903286. ISSN: 0369-3554

[Fuk14] K. Fukuda, *cddlib* (2014), http://www.inf.ethz.ch/personal/fukudak/cdd_home/

[Gal+12] R. Gallego, L. Erik Würflinger, A. Acín, M. Navascués, Operational framework for nonlocality. Phys. Rev. Lett. **109**(7), 070401 (2012). doi:10.1103/PhysRevLett.109.070401

[Gis91] N. Gisin, Bell's inequality holds for all non-product states. Phys. Lett. A **154**(5–6), 201–202 (1991). doi:10.1016/0375-9601(91)90805-I. ISSN: 0375-9601

[Giu+15] M. Giustina, M.A.M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M.W. Mitchell, J. Beyer, T. Gerrits, A.E. Lita, L.K. Shalm, S. Woo Nam, T. Scheidl, R. Ursin, B. Wittmann, A. Zeilinger, Significant-loophole-free test of Bell's theorem with entangled photons. Phys. Rev. Lett. **115**(25), 250401 (2015). doi:10.1103/PhysRevLett.115.250401

[Gro97] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325–328 (1997). doi:10.1103/PhysRevLett.79.325

[GTB05] O. Gühne, G. Tóth, H.J. Briegel, Multipartite entanglement in spin chains. New J. Phys. **7**(1), 229 (2005). doi:10.1088/1367-2630/7/1/229

[Gur03] L. Gurvits, Classical deterministic complexity of Edmonds' problem and quantum entanglement. in, *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing, STOC '03* (ACM, San Diego, CA, USA, 2003), pp. 10–19. doi:10.1145/780542.780545. ISBN: 1-58113-674-9

[HE02] P. Horodecki, A. Ekert, Method for direct detection of quantum entanglement. Phys. Rev. Lett. **89**(12), 127902 (2002). doi:10.1103/PhysRevLett.89.127902

[Hen+15] B. Hensen, H. Bernien, A.E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M.W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature **526**(7575) (2015), 682–686. doi:10.1038/nature15759

[HHH96] M. Horodecki, P. Horodecki, R. Horodecki, Separability of mixed states: necessary and sufficient conditions. Phys. Lett. A **223**(1–2), 1–8 (1996). doi:10.1016/S0375-9601(96)00706-2. ISSN: 0375-9601

[HHH98] M. Horodecki, P. Horodecki, R. Horodecki, Mixed-state entanglement and distillation: is there a "Bound" entanglement in nature? Phys. Rev. Lett. **80**(24), 5239–5242 (1998). doi:10.1103/PhysRevLett.80.5239

[HK11] K.-C. Ha, S.-H. Kye, Entanglement witnesses arising from exposed positive linear maps. Open Syst. Inf. Dyn. **18**(04), 323–337 (2011). doi:10.1142/S1230161211000224

[Hor97] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition. Phys. Lett. A **232**(5), 333–339 (1997). doi:10.1016/S0375-9601(97)00416-7. ISSN: 0375-9601

[Jam72] A. Jamiołkowski, Linear transformations which preserve trace and positive semidefiniteness of operators. Rep. Math. Phys. **3**(4), 275–278 (1972). doi:10.1016/0034-4877(72)90011-0. ISSN: 0034-4877

[Kol33] A.N. Kolmogórov, *Grundbegriffe der Wahrscheinlichkeitsrechnung* (Springer, Berlin, 1933)

[Lew+00] M. Lewenstein, B. Kraus, J.I. Cirac, P. Horodecki, Optimization of entanglement witnesses. Phys. Rev. A **62**(5), 052310 (2000). doi:10.1103/PhysRevA.62.052310

[Lin+07] N. Linden, S. Popescu, A.J. Short, A. Winter, Quantum nonlocality and beyond: limits from nonlocal computation. Phys. Rev. Lett. **99**(18), 180502 (2007). doi:10.1103/PhysRevLett.99.180502

[Maj32] E. Majorana, Atomi orientati in campo magnetico variabile Italian. Il Nuovo Cimento **9**(2), 43–50 (1932). doi:10.1007/BF02960953. ISSN: 0029-6341

[Mar11] D.J.H. Markham, Entanglement and symmetry in permutation-symmetric states. Phys. Rev. A **83**(4), 042332 (2011). doi:10.1103/PhysRevA.83.042332

[Nav+15] M. Navascués, Y. Guryanova, M.J. Hoban, A. Acín, Almost quantum correlations. Nat. Commun. **6**, 6288 (2015). doi:10.1038/ncomms7288

[NC00] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (2000). doi:10.1080/00107514.2011.587535

[Nie99] M.A. Nielsen, Conditions for a class of entanglement transformations. Phys. Rev. Lett. **83**(2), 436–439 (1999). doi:10.1103/PhysRevLett.83.436

[NPA08] M. Navascués, S. Pironio, A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New J. Phys. **10**(7), 073013 (2008). doi:10.1088/1367-2630/10/7/073013

[NW10] M. Navascus, H. Wunderlich, A glance beyond the quantum model. Proc. R. Soc. A: Math. Phys. Eng. Sci. **466**(2115), 881–890 (2010). doi:10.1098/rspa.2009.0453

[Paw+09] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski, Information causality as a physical principle. Nature **461**(7267), 1101–1104 (2009). doi:10.1038/nature08400

[Per96] A. Peres, Separability criterion for density matrices. Phys. Rev. Lett. **77**(8), 1413–1415 (1996). doi:10.1103/PhysRevLett.77.1413

[Pir14] S. Pironio, All Clauser-Horne-Shimony-Holt polytopes. J. Phys. A: Math. Theor. **47**(42), 424020 (2014). doi:10.1088/1751-8113/47/42/424020

[PR94] S. Popescu, D. Rohrlich, Quantum nonlocality as an axiom English. Found. Phys. **24**(3), 379–385 (1994). doi:10.1007/BF02058098. ISSN: 0015-9018

[PS01] I. Pitowsky, K. Svozil, Optimal tests of quantum nonlocality. Phys. Rev. A **64**(1), 014102 (2001). doi:10.1103/PhysRevA.64.014102

[RBG14] D. Rosset, J.-D. Bancal, N. Gisin, Classifying 50 years of Bell inequalities. J. Phys. A: Math. Theor. **47**(42), 424022 (2014). doi:10.1088/1751-8113/47/42/424022, http://www.faacets.com/

[Ros15] D. Rosset, Characterization of correlations in quantum networks. Ph.D. thesis, Université de Gen‘eve (2015)

[Sch35] E. Schrödinger, Discussion of probability relations between separated systems. Math. Proc. Camb. Philos. Soc. **31**(04), 555–563 (1935). doi:10.1017/S0305004100013554. ISSN: 1469-8064

[Sha+15] L.K. Shalm, E. Meyer-Scott, B.G. Christensen, P. Bierhorst, M.A. Wayne, M.J. Stevens, T. Gerrits, S. Glancy, D.R. Hamel, M.S. Allman, K.J. Coakley, S.D. Dyer, C. Hodge, A.E. Lita, V.B. Verma, C. Lambrocco, E. Tortorici, A.L. Migdall, Y. Zhang, D.R. Kumor, W.H. Farr, F. Marsili, M.D. Shaw, J.A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M.W. Mitchell, P.G. Kwiat, J.C. Bienfang, R.P. Mirin, E. Knill, S. Woo Nam, Strong loophole-free test of local realism*. Phys. Rev. Lett. **115**(25), 250402 (2015). doi:10.1103/PhysRevLett.115.250402

[SSŻ09] Ł. Skowronek, E. Størmer, K. Życzkowski, Cones of positive maps and their duality relations. J. Math. Phys. **50**(6), 062106 (2009). doi:10.1063/1.3155378

[Stø63] E. Størmer, Positive linear maps of operator algebras. Acta Math. **110**, 233–278 (1963). doi:10.1007/BF02391860. ISSN: 0001-5962

[Sve87] G. Svetlichny, Distinguishing three-body from two-body nonseparability by a Bell-type inequality. Phys. Rev. D **35**(10), 3066–3069 (1987). doi:10.1103/PhysRevD.35.3066

[Ter00] B.M. Terhal, Bell inequalities and the separability criterion. Phys. Lett. A **271**(5–6), 319–326 (2000). doi:10.1016/S0375-9601(00)00401-1. ISSN: 0375-9601

[TG09] G. Tóth, O. Gühne, Entanglement and permutational symmetry. Phys. Rev. Lett. **102**(17), 170503 (2009). doi:10.1103/PhysRevLett.102.170503

[TH00] B.M. Terhal, P. Horodecki, Schmidt number for density matrices. Phys. Rev. A **61**(4), 040301 (2000). doi:10.1103/PhysRevA.61.040301

[Ton09] B. Toner, Monogamy of non-local quantum correlations. Proc. R. Soc. A: Math. Phys. Eng. Sci. **465**(2101), 59–69 (2009). doi:10.1098/rspa.2008.0149

[TV06] B. Toner, F. Verstraete, *Monogamy of Bell Correlations and Tsirelson's Bound* (2006). arXiv:quant-ph/0611001

[VB12] T. Vértesi, N. Brunner, Quantum nonlocality does not imply entanglement distillability. Phys. Rev. Lett. **108**(3), 030403 (2012). doi:10.1103/PhysRevLett.108.030403

[VB14] T. Vértesi, N. Brunner, Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement. Nat. Commun. **5**, 5297 (2014). doi:10.1038/ncomms6297

[Wer89] R.F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. Phys. Rev. A **40**(8), 4277–4281 (1989). doi:10.1103/PhysRevA.40.4277

[Wor76] S.L. Woronowicz, Positive maps of low dimensional matrix algebras. Rep. Math. Phys. **10**(2), 165–183 (1976). doi:10.1016/0034-4877(76)90038-0. ISSN: 0034-4877

[Śli03] C. Śliwa, Symmetries of the Bell correlation inequalities. Phys. Lett. A **317**(34), 165–168 (2003). doi:10.1016/S0375-9601(03)01115-0. ISSN: 0375-9601

Springer

http://www.springer.com/978-3-319-49570-5

Characterizing Entanglement and Quantum Correlations
Constrained by Symmetry
Tura i Brugués, J.
2017, XXV, 237 p. 17 illus., 8 illus. in color., Hardcover
ISBN: 978-3-319-49570-5