Quantum Algorithms and Quantum Entanglement
Terhal, B.M.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Chapter 5
Product Bases, Local Distinguishability and Bound Entanglement

5.1 Introduction
In this chapter we study fundamental properties of quantum mechanical states, operations and measurements. In section 5.2 we review the notions of entanglement, distillation of entanglement and its relation to positive linear maps. In section 5.3 we establish a relation between Bell inequalities and the separability criterion and show under what restrictions they are equivalent. In section 5.4 we present results that relate local distinguishability of sets of product states to bound entanglement. Central in this construction is the notion of an unextendible product basis, of which we will give many examples. We prove that uncompletable product bases cannot be distinguished by a finite number of local operations and classical communication. These uncompletable product bases form new examples of the phenomenon of nonlocality without entanglement. In section 5.5 we present a new family of indecomposable positive linear maps. In the following sections we use the notation $n \otimes m$ or $\mathcal{H}_n \otimes \mathcal{H}_m$ to denote the tensor product between a $n$-dimensional Hilbert space and a $m$-dimensional Hilbert space.

5.2 Quantum Entanglement
The study of entanglement is essential for the understanding of quantum mechanics and the use of quantum mechanics in computation and information processing tasks. Erwin Schrödinger introduced the notion of entanglement and he was the first to understand its fundamental importance; in Ref. [105] we find

"When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each
of them with a representative of its own. I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives (or \( \psi \)-functions) have become entangled.”

The simplest form of entanglement is the entanglement that we find in bipartite pure states. Let \( |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \). We call the state \( |\psi\rangle \) entangled iff \( |\psi\rangle \) cannot be written as a product of pure states:

\[
|\psi\rangle \neq |\psi_a\rangle \otimes |\psi_b\rangle,
\]

(5.2.1)

where \( |\psi_a\rangle \in \mathcal{H}_A \) and \( |\psi_b\rangle \in \mathcal{H}_B \). Equivalently, when we express the pure state \( |\psi\rangle \) as a density matrix \( |\psi\rangle \langle \psi| \), the density matrix is entangled iff it cannot be written as

\[
|\psi\rangle \langle \psi| \neq |\psi_a\rangle \langle \psi_a| \otimes |\psi_b\rangle \langle \psi_b|.
\]

(5.2.2)

The famous example of a bipartite entangled state in \( 2 \otimes 2 \) is the Einstein-Podolsky-Rosen (EPR) singlet state [106, 107]

\[
|\psi^\prime\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle).
\]

We are not only concerned with pure states, but also with mixed states, represented by positive semidefinite Hermitian matrices \( p \) with \( \text{Tr} p = 1 \), the density matrices. Let us give the definition of entanglement for a bipartite density matrix \( p \):

**Definition 3** Let \( p \) be a density matrix on a finite-dimensional Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \). A state \( |\psi\rangle \) of the form \( |\psi^A\rangle \otimes |\psi^B\rangle \) is a (pure) product state in \( \mathcal{H}_A \otimes \mathcal{H}_B \). The density matrix \( p \) is entangled iff \( p \) cannot be written as a convex combination of pure product states, i.e. there does not exist an ensemble \( \{p_i \geq 0, |\psi_i^A\rangle \otimes |\psi_i^B\rangle\} \) such that

\[
p = \sum_i p_i |\psi_i^A\rangle \langle \psi_i^A| \otimes |\psi_i^B\rangle \langle \psi_i^B|.
\]

(5.2.4)

When \( p \) is not entangled \( p \) is called separable.

One would also like to classify entanglement in multipartite systems. A famous example of a tripartite pure entangled state is the Greenberger-Horne-Zeilinger (GHZ) state:

\[
|\psi^\prime\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle).
\]

We have not yet specified which parties the entanglement occurs. When we look at multipartite density matrices, this can lead to surprising results. In section 5.4.3 we will give an example (Example 3) of a
tripartite density matrix which cannot be written as a convex combination of pure product states for all three parties. When viewed as a bipartite density matrix on $\mathcal{H}_{AB} \otimes \mathcal{H}_C$ or $\mathcal{H}_A \otimes \mathcal{H}_{BC}$ or $\mathcal{H}_{AC} \otimes \mathcal{H}_B$, it can be shown that the density matrix is separable. This is impossible if the density matrix is a pure state, but apparently allowed when we consider general density matrices.

### 5.2.1 Quantification of Entanglement

It is important to have a measure of entanglement that quantifies ‘how much entanglement’ a state contains. Here we will only consider a measure of entanglement for bipartite states. For multipartite states the measure of entanglement has to take into account between which subsystems the entanglement occurs. It is an open problem how to define a measure of multipartite entanglement that gives a complete description of the various kinds of entanglement that are present in the state.

Any measure of entanglement $E(\rho)$ where $\rho$ is a density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$ must have the following four natural properties [37, 108]:

1. $E(\rho) \geq 0$ for all density matrices $\rho$ and $E(\rho) = 0$ when $\rho$ is a separable density matrix.

2. $E(\rho)$ is invariant under local unitary transformations, that is, unitary transformations of the form $U = U_A \otimes U_B$.

3. The entanglement $E(\rho)$ cannot increase under local operations and classical communication, that is

$$E(S(\rho)) \leq E(\rho),$$

(5.2.6)

where $S$ is a superoperator that can be implemented with local quantum operations of the two parties A and B and an unlimited amount of classical communication between them.

4. The entanglement $E(\rho)$ is a convex function of $\rho$, i.e.

$$E(\rho = \sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i).$$

(5.2.7)

For pure states $|\psi\rangle$ the conventional measure that obeys the four requirements is the entropy of entanglement. It is defined as

$$E(|\psi\rangle\langle\psi|) = S(\text{Tr}_A |\psi\rangle\langle\psi|) = S(\text{Tr}_B |\psi\rangle\langle\psi|),$$

(5.2.8)

where $S$ is the von Neumann entropy:

$$S(\rho) = -\text{Tr} \rho \log \rho.$$  

(5.2.9)
With this measure the EPR singlet in Eq. (5.2.3) has an entanglement of 1 bit, which is the maximum for a state in $2 \otimes 2$. For mixed states several entanglement measures have been proposed. One favorite measure that was introduced in Ref. [37] that obeys all the requirements is the entanglement of formation. The entanglement of formation for bipartite mixed states is more complicated than for pure states as the decomposition of a mixed state into a convex combination of pure states is not unique. Let $\rho$ be a bipartite density matrix and let $\mathcal{E}_\rho = \{p_i \geq 0, |\psi_i\rangle\}$ be an ensemble into which $\rho$ can be decomposed:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$  \hspace{1cm} (5.2.10)

The entanglement of formation of $\rho$ is defined as

$$E(\rho) = \min_{\mathcal{E}_\rho} \sum_i p_i E(|\psi_i\rangle\langle\psi_i|).$$ \hspace{1cm} (5.2.11)

The entanglement of formation equals the minimal average amount of pure state entanglement that is needed to build the density matrix $\rho$. The minimization in Eq. (5.2.11) makes an analytical computation of the entanglement of formation of mixed states a nontrivial task. Only in $2 \otimes 2$ has the problem of determining the entanglement of formation of any density matrix been completely solved by Wootters [109].

One may require that a measure of entanglement has the additional property of additivity, which does not follow from properties 1-4. An entanglement measure $E$ for bipartite states is additive when for any two density matrices $\rho_1$ on $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$ and $\rho_2$ on $\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$ and $\rho = \rho_1 \otimes \rho_2$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ where $\mathcal{H}_A = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ and $\mathcal{H}_B = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$, the following holds:

$$E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2).$$ \hspace{1cm} (5.2.12)

The entanglement of formation is certainly subadditive

$$E(\rho_1 \otimes \rho_2) \leq E(\rho_1) + E(\rho_2),$$ \hspace{1cm} (5.2.13)

where the equality holds when one uses the optimal individual ensembles $\mathcal{E}_{\rho_1}$ and $\mathcal{E}_{\rho_2}$ in the decomposition of $\rho_1 \otimes \rho_2$. The entanglement for pure states can be shown to be additive, but it has not yet been proved that the entanglement of formation is additive for all density matrices. If the entanglement of formation were not additive then this would mean that the entanglement costs for making $\rho_1 \otimes \rho_2$ would be strictly less than the entanglement costs for making $\rho_1$ and $\rho_2$ separately. It is possible that the entanglement of formation obeys only the requirement of partial additivity, that is, for all $n = 1, 2, \ldots$ $E(\rho^{\otimes n}) = nE(\rho)$ for mixed states $\rho$ [108].

### 5.2.2 Distillation of Quantum Entanglement

The sharing of quantum entanglement between two or more parties is a resource that for many quantum information processing tasks is more powerful than the sharing of classically
correlated states. As mentioned in Chap. 1 section 1.2.3, an EPR state can be used to send quantum information via teleportation. The protocols that employ quantum communication to solve a classical communication complexity problem (sec. 1.2.2) can be replaced by protocols that start from sharing a set of entangled states, which are then used to teleport the quantum data. If in these protocols the two parties start out with a mixed entangled state, they will have to "purify" this state to a pure entangled state before using it in some protocol. This procedure is called distillation [36]. The allowed set of quantum operations in the distillation procedure is restricted to the class of superoperators that is implementable by local quantum operations (LO) and classical communication (CC). Let us give the definition of distillable entanglement:

**Definition 4** [37, 110] The distillable entanglement of a bipartite density matrix \( \rho \) on \( \mathcal{H}_A \otimes \mathcal{H}_B \) with an unlimited amount of local operations and an unlimited amount of classical communication (LO+CC) is the maximum number \( D(\rho) \) such that there exists a sequence of LO+CC TCP maps \( S_i \)

\[
S_i : B((\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n_i}) \rightarrow B(\mathcal{K}_i \otimes \mathcal{K}_i),
\]

with \( n_i \rightarrow \infty \),

\[
\frac{1}{n_i} \log \dim \mathcal{K}_i \rightarrow D(\rho),
\]

and fidelity with respect to a maximally entangled state

\[
\langle \Phi^+ | S_i(\rho^{\otimes n_i}) | \Phi^+ \rangle \rightarrow 1,
\]

where

\[
\rho^{\otimes n_i} = \rho \otimes \ldots \otimes \rho,
\]

and

\[
|\Phi^+ \rangle = \frac{1}{\sqrt{\dim \mathcal{K}_i}} \sum_{j=1}^{\mathcal{K}_i} |jj\rangle.
\]

A density matrix \( \rho \) is called distillable if we can distill a non-zero amount of maximally entangled states from an arbitrary number of copies of \( \rho \).

In words, this definition says that a density matrix \( \rho \) is distillable by LO+CC if, when given a large number of copies of the density matrix \( \rho \), there is a LO+CC procedure that maps these copies onto a set of states in a (smaller) Hilbert space \( \mathcal{K}_i \otimes \mathcal{K}_i \) such that these remaining (distilled) states have a high fidelity with respect to a maximally entangled state—for example the state \( |\Phi^+\rangle \) in \( \mathcal{K}_i \otimes \mathcal{K}_i \). Note that we call a density matrix \( \rho \) distillable when some pure state entanglement can be distilled from it. If only a constant number of maximally entangled...
states can be distilled from an infinite number of copies of \( \rho \), then \( D(\rho) = 0 \). We call such a density matrix distillable though. From property 3, Eq. (5.2.6), it follows that \( D(\rho) \leq E(\rho) \); if \( D(\rho) \) would exceed \( E(\rho) \), we would have increased \( E(\rho) \) by LO+CC.

It has been shown [111] that any entangled density matrix on \( 2 \otimes 2 \) is distillable, in fact it was found that \( D(\rho) > 0 \) for all entangled density matrices on \( 2 \otimes 2 \). In higher dimensions the problem of distillation has turned out to be complicated by the richer structure of the manifold of entangled states and their relation to positive linear maps.

### 5.2.3 Positive Linear Maps

The problem of deciding whether a bipartite density matrix \( \rho \) on \( \mathcal{H}_A \otimes \mathcal{H}_B \) is entangled can be quite hard. It has been shown by the Horodeckis [112] that there exist an intimate connection between the classification of entangled density matrices and the theory of positive linear maps.

Let \( S : B(\mathcal{H}_n) \rightarrow B(\mathcal{H}_m) \) be a linear map. \( S \) is positive when \( S : B(\mathcal{H}_n)^+ \rightarrow B(\mathcal{H}_m)^+ \), where \( B(\mathcal{H}_n)^+ \) denotes the set of positive semidefinite matrices on \( \mathcal{H}_n \). Let \( \text{id}_k \) be the identity map on \( B(\mathcal{H}_k) \). We define the map \( \text{id}_k \otimes S : B(\mathcal{H}_k \otimes \mathcal{H}_n) \rightarrow B(\mathcal{H}_k \otimes \mathcal{H}_m) \) for \( k = 1, 2, \ldots \) by

\[
(\text{id}_k \otimes S) \left( \sum_i \sigma_i \otimes \tau_i \right) = \sum_i \sigma_i \otimes S(\tau_i),
\]

where \( \sigma_i \in B(\mathcal{H}_k) \) and \( \tau_i \in B(\mathcal{H}_n) \). The map \( S \) is \( k \)-positive when \( \text{id}_k \otimes S \) is positive. The map \( S \) is completely positive when \( S \) is \( k \)-positive for all \( k = 1, 2, \ldots \). Following Lindblad [113], the set of physical operations on a density matrix \( \rho \in B(\mathcal{H}_n)^+ \) is given by the set of completely positive trace-preserving maps \( S : B(\mathcal{H}_n) \rightarrow B(\mathcal{H}_m) \). Similarly as \( k \)-positive, one can define a \( k \)-copositive map. Let \( T : B(\mathcal{H}_n) \rightarrow B(\mathcal{H}_n) \) be defined as matrix transposition in a chosen basis for \( \mathcal{H}_n \), i.e.

\[
(T(A))_{ij} = A_{ji},
\]

on a matrix \( A \in B(\mathcal{H}_n) \). The map \( S \) is \( k \)-copositive when \( \text{id}_k \otimes (S \circ T) \) is positive. A positive linear map \( S : B(\mathcal{H}_n) \rightarrow B(\mathcal{H}_m) \) is decomposable if it can be written as

\[
S = S_1 + S_2 \circ T,
\]

where \( S_1 : B(\mathcal{H}_n) \rightarrow B(\mathcal{H}_m) \) and \( S_2 : B(\mathcal{H}_n) \rightarrow B(\mathcal{H}_m) \) are completely positive maps. It has been shown by Woronowicz [114] that all positive linear maps \( S : B(\mathcal{H}_2) \rightarrow B(\mathcal{H}_2) \) and \( S : B(\mathcal{H}_2) \rightarrow B(\mathcal{H}_3) \) are decomposable.

In Ref. [115] Peres made the observation that every separable density matrix \( \rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B) \) remains positive semidefinite under partial transposition of \( \rho \), \( (\text{id}_A \otimes T_B)(\rho) \). He conjectured that this would not only be a necessary but also a sufficient condition for separability. His conjecture turned out to be true for density matrices on \( 2 \otimes 2 \) and \( 2 \otimes 3 \).

The following theorem by the Horodeckis [112] formulates a necessary and sufficient condition for a density matrix \( \rho \) to be entangled:
Theorem 1 (Horodecki) A density matrix $\rho$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is entangled iff there exists a positive linear map $S: B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ such that

$$(\text{id}_A \otimes S)(\rho),$$

is not positive semidefinite. Here $\text{id}_A$ denotes the identity map on $B(\mathcal{H}_A)$.

Remark An equivalent statement as Theorem 1 holds for positive linear maps $S: B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ and the positive semidefiniteness of $(S \otimes \text{id}_B)(\rho)$.

The consequences of Theorem 1 and Woronowicz’ result is that a bipartite density matrix $\rho$ on $\mathcal{H}_2 \otimes \mathcal{H}_2$ and $\mathcal{H}_3 \otimes \mathcal{H}_3$ is entangled iff $(\text{id}_A \otimes [S_1 + S_2 \circ T])(\rho)$ is not positive semidefinite for some $S_1$ and $S_2$. As $S_1$ and $S_2$ are completely positive maps this is equivalent to testing whether the requirement that $(\text{id}_A \otimes T)(\rho)$ is not positive semidefinite is satisfied.

In the following sections we will sometimes refer to a density matrix having the NPT-property, which means that the density matrix is not positive semidefinite under partial transposition, or a density matrix having the PPT-property.

The partial transposition map is a powerful tool in characterizing entanglement, even in high dimensional Hilbert spaces. In Ref. [116] it was shown that if a bipartite density matrix $\rho$ has the PPT-property, the density matrix cannot be distilled (see definition 4). It is not known whether the converse it true; all density matrices that have the NPT-property are distillable. There are indications that this might not be the case.

In Ref. [117] P. Horodecki found the first examples of density matrices on $\mathcal{H}_2 \otimes \mathcal{H}_4$ and $\mathcal{H}_3 \otimes \mathcal{H}_3$ that are provably entangled, but remain positive semidefinite under the partial transposition map. These states which are not distillable are called bound entangled states.

In sec. 5.4 we will present many new examples of bound entangled states and show how their construction is intimately connected with LO+CC distinguishability of sets of orthogonal product states. In section 5.5 we show how this new class of bound entangled states gives rise to a new family of indecomposable positive linear maps.

5.3 Bell Inequalities and the Separability Criterion

We will start by reproducing a lemma of [112]. This lemma expresses a necessary and sufficient condition for separability of a bipartite density matrix:

Lemma 3 [112] A density matrix $\rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$ is entangled iff there exists a Hermitian operator $H \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ with the properties:

$$\text{Tr} H \rho < 0 \quad \text{and} \quad \text{Tr} H \sigma \geq 0,$$

for all separable density matrices $\sigma \in B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$.

The lemma follows from basic theorems in convex analysis [118]. The proof invokes the existence of a separating hyperplane between the closed convex set of separable density
matrices on $\mathcal{H}_A \otimes \mathcal{H}_B$ and a point, the entangled density matrix $\rho$, that does not belong to it. This separating hyperplane is characterized by the vector $H$ that is normal to it; the hyperplane is the set of density matrices $\tau$ such that $\text{Tr} H \tau = 0$.

From a physics point of view, the Hermitian operator $H$ is the observable that would reveal the entanglement of a density matrix $\rho$. We will call $H$ an entanglement witness. The lemma tells us that there exists such an observable $H$ for any entangled bipartite density matrix. Thus, if one can prove that there exists no such observable for a density matrix $\rho$, it follows that $\rho$ must be separable.

We now turn to the formulation of Bell inequalities. The question of whether quantum mechanics provides a complete description of reality underlies the formulation of Bell's original inequality [119]. The issue is whether the results of measurements can be described by assuming the existence of a classical local hidden variable. The variable is hidden as its value cannot necessarily be measured directly; the average outcome of any measurement is a statistical average over different values that this hidden variable can take. The locality of this variable is required by the locality of classical physics \(^1\). Bell demonstrated that for the state in Eq. (5.2.3), the EPR singlet state, there exists a set of local measurements performed by two parties, Alice and Bob, whose outcomes cannot be described by any local hidden variable theory. The first experimental verification of his result with independently chosen measurements for Alice and Bob was carried out by Alain Aspect [120]. Since Bell's result, much attention has been devoted to finding stronger "Bell inequalities", that is, inequalities that demonstrate the nonlocal character of other entangled states, pure and mixed. It has been found that any bipartite pure entangled state violates some Bell inequality [62]. The situation for mixed states is less clear. Multiple copies of bipartite mixed states that can be distilled (see definition 4) will violate a Bell inequality. The distillability makes it possible to map these states onto pure entangled states after which a pure-state Bell-inequality test will reveal their nonlocal character. But there are many entangled states, such as the ones that we will introduce and discuss in section 5.4.3 for which it is not known whether they violate a Bell inequality.

Interestingly, the general formulation of Bell inequalities [121, 122, 123] has great similarity with the separability criterion of Lemma 3 and there exists a relation between the two.

The general formulation of Bell inequalities comes about in the following way. We will consider only bipartite states here, but the formulation also holds for multipartite states. Let $\mathcal{M}^A_1, \ldots, \mathcal{M}^A_n$ be a set of possible measurements for Alice and $\mathcal{M}^B_1, \ldots, \mathcal{M}^B_n$ be a set of measurements for Bob. For simplicity let us consider measurements in which each outcome corresponds to a single operation element (see section 3.2, Eq. (3.2.6)). The analysis is completely analogous for measurements with more than one operation element per outcome. Thus each measurement is characterized by its operation elements corresponding to its possible outcomes. We write for the $i$th Alice measurement with $k$ outcomes,

$$\mathcal{M}^A_i = (A_{i,1}, A_{i,2}, \ldots, A_{i,k(i)}), \quad \sum_{m=1}^{k(i)} A_{i,m} A_{i,m}^\dagger = 1,$$

\(^1\)No information can travel faster than the speed of light.
and similarly for the \( j \)th measurement of Bob,

\[
\mathcal{M}_J^B = (B_{j,1}, B_{j,2}, \ldots, B_{j,m}), \quad \sum_{m=1}^{(J)} B_{j,m}^B = 1. \tag{5.3.3}
\]

Let \( \vec{P} \) be a vector of probabilities of outcomes of measurements by Alice and Bob on a quantum state \( \rho \). The vector \( \vec{P} \) has three parts denoted with the components \( (P_{A_1|k}, P_{B_1|l}), (P_{A_2|k}, P_{B_2|l}), \ldots) \). For example, when Alice has two measurements with two outcomes each and Bob has one measurement with three outcomes, \( \vec{P} \) will be a 12+4+3 component vector with its components equal to

\[
P_{A_1|k} = \text{Tr} E^A_{i,k} \otimes E^B_{j,l} \rho,
\]

\[
P_{A_2|k} = \text{Tr} E^A_{i,k} \otimes \mathbf{1} \rho,
\]

\[
P_{B|l} = \text{Tr} \mathbf{1} \otimes E^B_{j,l} \rho,
\]

with \( E^A_{i,k} = A^A_{i,k} A^A_{i,k} \) for \( i = 1, 2, k = 1, 2 \) and \( E^B_{j,l} = B^B_{j,l} B^B_{j,l} \) for \( j = 1, l = 1, 2, 3 \). We call \( \vec{P} \) the event vector.

Let \( \lambda \) be a local hidden variable. We choose \( \lambda \) such that when \( \lambda \) takes a specific value, each measurement outcome is made either impossible or made to occur with probability \( 1 \). In other words, given a value of \( \lambda \) a probability of either 0 or 1 is assigned to Alice’s outcomes and similarly for Bob. Then we choose \( \lambda \) to take as many values as are needed to produce all possible patterns of 0s and 1s, all Boolean vectors. These outcome patterns are denoted as Boolean vectors \( B^A_{\lambda} \) and \( B^B_{\lambda} \). For example, when Alice has three measurements each with two outcomes there will be \( 2^6 \) vectors \( B^A_{\lambda} \in \{0, 1\}^6 \). The vector \( B^A_{\lambda} \) has of course the same number of entries as Alice’s part of the event vector \( \vec{P} \) and similarly for Bob. The locality constraint comes in by requiring that the vector of joint probabilities \( B^A_{\lambda} \) is a product vector, i.e. \( B^A_{\lambda} \otimes B^B_{\lambda} \). The total vector is denoted as \( \vec{B}_{\lambda} = (B^A_{\lambda}, B^A_{\lambda}, B^B_{\lambda}) \). An example will serve to elucidate the idea. When, as before, Alice has two measurements each with two outcomes and Bob has one measurement with three outcomes, an example of the vector \( \vec{B}_{\lambda} \) is

\[
\vec{B}_{\lambda} = [(1, 0, 0, 1) \otimes (0, 1, 0), (1, 0, 0, 1), (0, 1, 0)].
\]

We denote the vector \( \vec{B}_{\lambda - \lambda_1} \), when \( \lambda \) takes the value \( \lambda_1 \) as \( \vec{B}_{\lambda_1} \). Any local hidden variable theory can be represented as a vector \( \vec{V} \):

\[
\vec{V} = \sum_i p_i \left( \vec{P}^A_i \otimes \vec{P}^B_i, \vec{P}^A_i, \vec{P}^B_i \right), \tag{5.3.6}
\]

with \( p_i \geq 0 \) and \( \vec{P}^A_i \) and \( \vec{P}^B_i \) are vectors of (positive) probabilities. These vectors are convex combinations of the vectors \( \vec{B}_{\lambda_1}, \ldots, \vec{B}_{\lambda_N} \), where \( N \) is such that \( \vec{B}^A_{\lambda} \) and \( \vec{B}^B_{\lambda} \) are all possible Boolean vectors (see Ref. [123]):

\[
\vec{V} = \sum_i q_i \vec{B}_{\lambda_i}, \tag{5.3.7}
\]
with \( q_i \geq 0 \). Thus we see that the set of local hidden variable theories forms a convex cone \( L_{LLHV(M)} \). The label \( M \) is a reminder that the cone depends on the chosen measurements for Alice or Bob, in particular the number of them and the number of outcomes for each of them. The vectors \( \bar{B}_i \) are the extremal rays \([121]\) of \( L_{LLHV(M)} \). The question then of whether the probabilities of the outcomes of the chosen set of measurements on a density matrix \( \rho \) can be reproduced by a local hidden variable theory, is equivalent to the question whether or not

\[
\bar{P} \in L_{LLHV(M)}. \tag{5.3.8}
\]

It is not hard to see that all separable pure states have event vectors \( \bar{P} \in L_{LLHV(M)} \) as the event vector \( \bar{P} \) for a separable pure state has a product structure \( \bar{P} = (\bar{P}_A \otimes \bar{P}_B, \bar{P}_A, \bar{P}_B) \). It follows that all separable states have event vectors in \( L_{LLHV(M)} \), as they are convex combinations of separable pure states. What about the entangled states? We can use the Minkowski-Farkas lemma for convex sets in \( \mathbb{R}^n \) \([118]\). The lemma implies that \( \bar{P} \notin L_{LLHV(M)} \) iff there exists a vector \( \bar{F} \) such that

\[
\bar{F} \cdot \bar{P} < 0 \quad \text{and} \quad \forall \lambda_i \left[ \bar{F} \cdot \bar{B}_i \geq 0 \right]. \tag{5.3.9}
\]

The equation \( \forall \lambda_i \left[ \bar{F} \cdot \bar{B}_i \geq 0 \right] \) is a Bell inequality. The equation \( \bar{F} \cdot \bar{P} < 0 \) corresponds to the violation of a Bell inequality. Thus, finding a set of measurements and exhibiting the vector \( \bar{F} \) with the properties of Eq. (5.3.9) is equivalent to finding a violation of a Bell inequality. If one can prove that for a density matrix \( \rho \) no such sets of inequalities of the form Eq. (5.3.9) for all possible measurement schemes can be found, then it follows that \( \rho \) can be described by a local hidden variable theory. This concludes our discussion of the literature on the general formulation of Bell inequalities.

There is a nice correspondence between Eq. (5.3.9) and Lemma 3, captured in the following construction: Given a (Farkas) vector \( \bar{F} \) of Eq. (5.3.9) and a set of measurements \( M \) for a bipartite entangled state \( \rho \), one can construct an entanglement witness for \( \rho \) as in Lemma 3. Denote the components of the Farkas vector \( \bar{F} \) as \( (\bar{F}_{A_i, k, B_j, l, l}, \bar{F}_{A_i, k, B_j, l}) \). Then

\[
H = \sum_{i,k,j,l} F_{A_i, k, B_j, l} E_{i, k}^A E_{j, l}^B + \sum_{i,k} F_{A_i, k} E_{i, k}^A \otimes 1 + \sum_{j,l} F_{B_j, l} 1 \otimes E_{j, l}^B, \tag{5.3.10}
\]

where \( E_{i, k}^A = A_{i, k}^\dagger A_{i, k} \) and \( A_{i, k} \) are the operation elements of the \( i \)th measurement with outcome \( k \) for Alice and similarly for Bob. With this construction \( \bar{F} \cdot \bar{P} = \text{Tr} \bar{H} \rho \). Also, one has \( \text{Tr} \bar{H} \sigma \geq 0 \) for any separable density matrix \( \sigma \) as \( \bar{P}_\sigma \in L_{LLHV(M)} \) for all separable density matrices \( \sigma \). Thus a violation of a Bell inequality for a bipartite density matrix \( \rho \) can be reformulated as a entanglement witness \( H \) for \( \rho \). One may ask whether this relation holds in the opposite direction: Given an entanglement witness \( H \) for a bipartite density matrix \( \rho \), does there exist a decomposition of \( H \) into a set of measurements and a vector \( \bar{F} \) as in Eq. (5.3.10), that leads to a violation of a Bell inequality for \( \rho \). The answer to this question seems to be negative for certain mixed states \([124]\). The reason for the discrepancy between the inequalities of Lemma 3 and Eq. (5.3.9) is that the hidden variable cone \( L_{LLHV(M)} \) contains
more than just the separable states; it can also contain vectors which do not correspond to probabilities of outcomes of measurements on a quantum mechanical system. If quantum mechanics is correct then we will never find these sets of outcomes. An example of such an unphysical vector is the following. Let Alice perform two possible measurements on a two-dimensional system. Her first measurement $M_1$ is a projection in the $\{|0\rangle,|1\rangle\}$ basis and her second measurement $M_2$ is a projection in the $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ basis. The hidden variable cone $L_{LHV(M)}$ will contain vectors such as

$$B_\lambda = [(1,0,0,1) \otimes (\ldots), (1,0,0,1), (\ldots)].$$

(5.3.11)

This vector $B_\lambda$ which assigns a probability 1 to outcome $|0\rangle$ and a probability 1 to outcome $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ cannot describe the outcome of these measurements on any quantum mechanical state $\rho$.

These unphysical vectors play an important role in the construction of hidden variable theories for entangled states: their importance is emphasized by the following observation. If we restrict the cone $L_{LHV(M)}$ to contain only vectors that are consistent with quantum mechanics, then we can prove that there exists a “violation of a Bell inequality” for any entangled state. By this we mean the following: We demand that all vectors in the set $L_{LHV(M)}$ correspond to sets of outcomes that can be obtained by measurements on a quantum mechanical system in $\mathcal{H}_A \otimes \mathcal{H}_B$. Here $\mathcal{H}_A \otimes \mathcal{H}_B$ is the Hilbert space on which the density matrix that we would like to describe with a restricted local hidden variable theory is defined. We can call this restricted local hidden variable theory a local quantum mechanical hidden variable theory. One can prove that in this restricted scenario, there will always be a set of measurements under which $\rho$ reveals its nonlocality and its entanglement:

**Theorem 2** Let $\rho$ be a bipartite density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. The density matrix $\rho$ is separable iff there exists a restricted local hidden variable theory of $\rho$.

**Proof** The idea of the proof is the following. All vectors in the restricted local hidden variable theory now correspond to outcomes of measurements on a quantum mechanical system. We chose a set of measurements that completely determines a quantum state in a given Hilbert space. Then there is a 1-1 correspondence between vectors of measurement outcomes and quantum states. Then we show that all vectors in the restricted local hidden variable set correspond to measurement outcomes of separable states. Therefore measurement outcomes from entangled states do not lie in the set described by a restricted local hidden variable theory.

We write the density matrix $\rho$ as

$$\rho = \sum_{i,j} \mu_{ij} \sigma_i \otimes \tau_j + \sum_i \mu_i^A \sigma_i \otimes 1 + \sum_j \mu_j^B 1 \otimes \tau_j,$$

(5.3.12)

where the Hermitian matrices $\{\sigma_i \otimes \tau_j\}_{i=1,j=1}^{d_A-1,d_B-1}$, $\{\sigma_i \otimes 1\}_{i=1}^{d_A-1}$, $\{1 \otimes \tau_j\}_{j=1}^{d_B-1}$ with $d_A = \dim \mathcal{H}_A$ etc., form a basis for the Hermitian operators on $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $|w_{ijkl}\rangle$ be the eigenvectors
of the matrix $\sigma$, and $|w_{j,k}^B\rangle$ be the eigenvectors of $\tau_j$. The projector onto the state $|w_{i,k}^A\rangle$ is denoted as $\pi_{w_{i,k}^A}$, and similarly, the projector onto the state $|w_{j,l}^B\rangle$ is denoted as $\pi_{w_{j,l}^B}$.

Alice and Bob choose a set of measurements such that the probabilities of outcomes of these measurements are given by

$$
\begin{align*}
\text{Tr} \pi_{w_{i,k}^A} \otimes \pi_{w_{j,l}^B} \rho &= p_{i,k,j,l}, \\
\text{Tr} \pi_{w_{i,k}^A} \otimes \mathbf{1} \rho &= p_i^A, \\
\text{Tr} \mathbf{1} \otimes \pi_{w_{j,l}^B} \rho &= p_j^B,
\end{align*}
$$

for all $i, k, j$ and $l$. In order to construct these POVMs they may get outcomes whose probability is given by other expressions than Eq. (5.3.13). What is important is that they, if they would carry out these measurements repeatedly on $\rho$ (a single measurement on each copy of $\rho$), would be able to determine the probabilities $(p_{i,k,j,l}, p_i^A, p_j^B)$. Then they can uniquely infer from these probabilities the state $\rho$. We call this set of measurements $M_c$, a complete set of measurements. Let $L_{LHV(M_c)}^r$ be the convex set of restricted local hidden variable theories. We first consider which density matrices $\rho$ can be described by restricted local hidden variable vectors of the form $(p_A^B \otimes p_A^B, p_A^B, p_A^B)$, where $p_A^B$ is a vector of probabilities $p_{i,k}(p_{j,l})$. The density matrix $\rho = p_A^B \otimes p_B^A$ where $\rho_A = \text{Tr} B \rho$ and $\rho_B = \text{Tr} A \rho$ is a solution of the equations

$$
\begin{align*}
\text{Tr} \pi_{w_{i,k}^A} \otimes \pi_{w_{j,l}^B} \rho &= p_{i,k,j,l}^A, \\
\text{Tr} \pi_{w_{i,k}^A} \otimes \mathbf{1} \rho &= p_i^A, \\
\text{Tr} \mathbf{1} \otimes \pi_{w_{j,l}^B} \rho &= p_j^B,
\end{align*}
$$

for all $i, k, j$ and $l$, since

$$
\text{Tr} \pi_{w_{i,k}^A} \otimes \pi_{w_{j,l}^B} \rho = \text{Tr} \pi_{w_{i,k}^A} \otimes \pi_{w_{j,l}^B} (p_A^B \otimes p_B^A),
$$

As the set of measurements completely determines the density matrix $\rho$ it follows that the solution $\rho = p_A^B \otimes p_B^A$ is the only solution of Eq. (5.3.14) for all $i, k, j$ and $l$. Therefore all the restricted local variable vectors of the form $(\tilde{p}_A^B \otimes \tilde{p}_B^A, \tilde{p}_A^B, \tilde{p}_B^A)$ correspond to separable states. If follows that any convex combination of the restricted local hidden variable vectors $V = \sum_i p_i (\tilde{p}_A^B \otimes \tilde{p}_B^A, \tilde{p}_A^B, \tilde{p}_B^A)$ corresponds to a separable state. As the map from the vectors $\tilde{P}$ to states $\rho$ is 1-1, this is the only density matrix that corresponds to $V$. Thus we can conclude that no vector in the convex set $L_{LHV(M_c)}^r$ corresponds to an entangled state. On the other hand the outcome vector of any separable density matrix lies in $L_{LHV(M_c)}^r$ by the argument given below Eq. (5.3.8). This completes the proof. □

We are now ready to clarify the relation between the separability criterion, Lemma 3, and Bell inequalities. Theorem 2 shows that $L_{LHV(M_c)}^r$ only contains outcome vectors of separable

---

2Note that $L_{LHV(M_c)}^r$ is a set and not a cone, as $V \in L_{LHV(M_c)}^r$ does not imply that $\lambda V \in L_{LHV(M_c)}^r$ with $\lambda > 0$, as we now require that all vectors in $V$ correspond to probabilities of outcomes of measurements on a quantum mechanical system.
5.4 Product Bases, Local Distinguishability and Bound Entanglement

5.4.1 Nonlocality without Entanglement

The EPR singlet, Eq. (5.2.3), or any other pure entangled state, is a prime demonstration of the nonlocality of quantum mechanics. Its entanglement is an asset in protocols such a teleportation and its intrinsic nonlocal character is demonstrated by its violation of a Bell inequality. It is tempting to think that only entangled states, pure or mixed, exhibit some form of nonlocality. Reality however is more subtle than this. In Ref. [125] it was demonstrated that there exists a form of quantum nonlocality that does not need entanglement. The authors of [125] presented a set of nine orthogonal product states in a bipartite $3 \otimes 3$ Hilbert space:

$$\begin{align*}
|v_0\rangle &= \frac{1}{\sqrt{2}} |0\rangle \otimes |0 - 1\rangle, & |v_1\rangle &= \frac{1}{\sqrt{2}} |0\rangle \otimes |0 + 1\rangle, \\
|v_3\rangle &= \frac{1}{\sqrt{2}} |2\rangle \otimes |1 - 2\rangle, & |v_4\rangle &= \frac{1}{\sqrt{2}} |2\rangle \otimes |1 + 2\rangle, \\
|v_5\rangle &= \frac{1}{\sqrt{2}} |0 - 1\rangle \otimes |2\rangle, & |v_6\rangle &= \frac{1}{\sqrt{2}} |0 + 1\rangle \otimes |2\rangle, \\
|v_7\rangle &= \frac{1}{\sqrt{2}} |1 - 2\rangle \otimes |0\rangle, & |v_8\rangle &= \frac{1}{\sqrt{2}} |1 + 2\rangle \otimes |0\rangle,
\end{align*}$$

(5.4.1)

where $\frac{1}{\sqrt{2}} |0 - 1\rangle$ denotes $\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$ etc. Here and further in the text tensor products $\otimes$ are sometimes omitted; the state $|\psi_a, \psi_b\rangle$ is equivalent with $|\psi_a\rangle \otimes |\psi_b\rangle$ or $|\psi_a\rangle \otimes |\psi_b\rangle$. Two parties, Alice and Bob, are given a single copy of one of these nine states, but they are not told which
one they are given. Their task is to determine which one of the nine states they are given by performing local measurements on the state and communicating classically to each other about the outcomes. As these states are mutually orthogonal they can be distinguished when a measurement is done on the joint system of Alice and Bob. It was shown however that it is not possible for the two parties to find out with certainty which state they were given even if they could use an unlimited amount of classical communication and could perform an unlimited number of local measurements and other computational operations. It is not even possible to get the right answer with arbitrary small probability of error. What is important is that these states, being orthogonal product states, do not exhibit any entanglement at all. They form an example of a phenomenon that one could call nonlocality without entanglement.

There could be an interesting use of such states, that surpasses anything that can be done in a strictly classical world. These states could be used in a protocol of secret sharing. Consider the following situation. Alice and Bob are given a secret by a third authorized party Charlie. The idea of the secret sharing is that Alice and Bob are not able to determine the secret alone. For example the American government (the authorized party) lets two employees at Los Alamos National Laboratory share the secret of new weapon. One of the employees is malevolent and the other one can be trusted to keep his part of the secret. The malevolent employee needs information of the trusted employee in order to determine the secret. The trusted employee refuses to reveal the information that he/she has to the malevolent employee. In this scenario if both the employees are malevolent, it is impossible to keep the secret safe, if we do not assume any restrictions on the computational resources and the cunning of the employees.

In a quantum world it might be possible that two malevolent parties are able to keep a secret if their communication is restricted to the transmission of classical messages. Such a quantum scenario that uses entanglement has been investigated in Ref. [126]. Here we propose a protocol that does not use entanglement between the sharing parties. The idea would be the following. The secret is encoded as a word in an alphabet with nine letters, the nine states. We know that the two parties are not able to distinguish between one of the nine states exactly. However, if they would be allowed to send each other quantum data, they are able to uncover the secret. In order for the protocol to be absolutely safe, one will have to be able to show that the two parties will obtain less than a certain small amount of information about the secret for any attack that they can carry out. The establishment of such a protocol and the proof of its safety is a question of current research.

5.4.2 Unextendible Product Bases

We introduce a new concept, that of an unextendible product basis:

Definition 5 Consider a multipartite quantum system $\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i$ with $m$ parties of respective dimension $d_i$, $i = 1, \ldots, m$. A (partial orthogonal) product basis (PB) is a set $S$ of pure orthogonal product states spanning a proper subspace $\mathcal{H}_S$ of $\mathcal{H}$. An unextendible product
basis (UPB) is a PB whose complementary subspace $H_{15}^\perp$ contains no product state.

Here are two examples of a UPB on $3 \otimes 3$ (two qutrits):

**Example 1:** Consider five vectors in real three-dimensional space forming the apex of a regular pentagonal pyramid, the height $h$ of the pyramid being chosen such that nonadjacent apex vectors are orthogonal. The vectors are

$$ v_i = N \left( \cos \frac{2 \pi i}{5}, \sin \frac{2 \pi i}{5}, h \right), \quad i = 0, \ldots, 4, \quad (5.4.2) $$

with $h = \frac{1}{2} \sqrt{1 + \sqrt{5}}$ and $N = \frac{2}{\sqrt{5} + \sqrt{5}}$. The following five states in $3 \otimes 3$ form the UPB Pent

$$ \tilde{\rho}_i = v_i \otimes \tilde{v}_{2i \mod 5}, \quad i = 0, \ldots, 4. \quad (5.4.3) $$

**Example 2:** The following five states on $3 \otimes 3$ form the UPB Tiles

$$ |v_0\rangle = \frac{1}{\sqrt{2}} |0\rangle |0 - 1\rangle, \quad |v_2\rangle = \frac{1}{\sqrt{2}} |2\rangle |1 - 2\rangle, $$

$$ |v_1\rangle = \frac{1}{\sqrt{2}} |0 - 1\rangle |2\rangle, \quad |v_3\rangle = \frac{1}{\sqrt{2}} |1 - 2\rangle |0\rangle, $$

$$ |v_4\rangle = (1/3)|0 + 1 + 2\rangle |0 + 1 + 2\rangle. \quad (5.4.4) $$

The first four states are the interlocking tiles of [125], Eq. (5.4.1), and the fifth state works as a “stopper” to force the unextendibility. (In fact, the sets Pent and Tiles are both members of a single six-parameter family of UPBs [129])

The orthogonality relations between the members of the set, both for Pent as well as Tiles, are depicted in Fig. 5.1. The states are given as vertices in the graph. When two vertices are connected by, say, a Bob-edge, it means that the states are orthogonal on Bob’s side and similar for Alice.

In both these examples one can observe that any subset of three vectors on either side spans the full three-dimensional space. This implies that there cannot be a product vector orthogonal to these states and thus both these PBs are UPBs.

We can formalize the way in which these two examples were constructed to give a necessary and sufficient condition for a PB on a multipartite system to be a UPB:
Lemma 4 Let $P$ be a partition of a PB $S$ into disjoint sets $S = S_1 \cup S_2 \cup \ldots S_m$ where $S_i$ is a set of states associated with the $i^{th}$ party. Let $\pi_j$ be the projector onto the $j^{th}$ state in $S$. Let $\rho_i^P = \sum_j \text{Tr}(\otimes_{k \neq i} \mathcal{H}_k) \pi_j$. The set $S$ forms a UPB on $\bigotimes_{i=1}^m \mathcal{H}_i$ iff for all partitions $P$ at least one $\rho_i^P$ has full rank, equal to $d_i$.

Proof If for all partitions $P$ there is a local $\rho_i^P$ with full rank, then it is not possible to add a new product state to $S$ that is orthogonal to all the members in $S$. If a set of states $S$ forms a UPB, but there exists a partition $P$ for which all $\rho_i^P$ have less than full rank, then we arrive at a contradiction, as we can add a product state to the UPB in the following way. One takes the partition $P$ that gives rise to the matrices $\rho_i^P$ that all have less than full rank $d_i$. Then a new state can be added that is orthogonal to the states in $S_1$ on $\mathcal{H}_1$, the states in $S_2$ on $\mathcal{H}_2$ etc., such that this new state is orthogonal to all the members in $S$. □

In principle Lemma 4 can be used recursively to explore whether a set of states $S$ can be completed to a full basis, but it is not known whether there exist an efficient algorithm that performs this task.

The lemma provides a simple lower bound on the number of states $k$ in a UPB:

$$k \geq \sum_i (d_i - 1) + 1.$$  \hfill (5.4.5)

If $k$ is equal to $\sum_i (d_i - 1)$ or smaller then one can partition $S$ into sets of size $|S_i| \leq d_i - 1$. This partition has the property that $\text{Rank}(\rho_i^P) < d_i$ for all $i$ and therefore the set $S$ cannot be a UPB.

5.4.3 Bound Entanglement

Bipartite UPBs lead directly to the construction of density matrices that have bound entanglement. These bipartite bound entangled states are positive semidefinite under partial transposition (PPT), although they are entangled. The PPT-property implies that no pure state entanglement can be distilled from these states.

Proposition 6 Let $S$ be a bipartite unextendible product basis $\{ |a_i \rangle \otimes |\beta_i \rangle \}_{i=1}^{|S|}$ in $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. We define a density matrix $\rho_S$ as

$$\rho_S = \frac{1}{\dim \mathcal{H} - |S|} \left( 1_{AB} - \sum_{i=1}^{|S|} |a_i \rangle \langle a_i| \otimes |\beta_i \rangle \langle \beta_i| \right),$$ \hfill (5.4.6)

where $1_{AB}$ is the identity on $\mathcal{H}$. The density matrix $\rho_S$ is entangled. Furthermore, the matrix $(\text{id}_A \otimes [S_1 + T \circ S_2]) (\rho_S)$ for all completely positive maps $S_1$ and $S_2$, is positive semidefinite.

Proof The density matrix $\rho_S$ is proportional to the projector on the complementary subspace $\mathcal{H}_S^\perp$. As $S$ is unextendible $\mathcal{H}_S^\perp$ contains no product states. Therefore the density matrix is entangled. It is not hard to see that $(\text{id}_A \otimes T)(\rho_S)$ is positive semidefinite. It has been proved
in Ref. [116] that when \((\text{id}_A \otimes T)(\rho_S)\) is positive semidefinite that \((\text{id}_A \otimes T \circ S_2)(\rho_S)\) where \(S_2\) is any completely positive map, is also positive semidefinite. Therefore \((\text{id}_A \otimes [S_1 + T \circ S_2])(\rho_S)\) is also positive semidefinite. □

We now give an example of a tripartite UPB:

**Example 3:** Consider a set Shifts of orthogonal product states between three parties \(A, B,\) and \(C\):

\[
\{|0, 1, +\}, |1, +, 0\}, |+, 0, 1\}, |-, -, -\}, \quad (5.4.7)
\]

with \(\pm = |0\pm 1\rangle\) (unnormalized). There is no product state that is orthogonal to these four states, as any subset of two states spans the full 2-dimensional space on one side. The complementary state constructed as in Eq. (5.4.6) has the curious property that it is 2-way separable, i.e., the entanglement between every split into two parties is zero. This refutes a conjecture that was made in Ref. [130]. To show that, for example, the entanglement between \(A\) and \(BC\) is zero, one writes the BC parts of the states in Eq. (5.4.7) as \(a = |1, +\rangle, b = |+, 0\rangle, c = |0, 1\rangle\) and \(d = |-, -\rangle\). Note that \(\{a, b\}\) are orthogonal to \(\{c, d\}\).

Consider the vectors \(a^\perp\) and \(b^\perp\) in the Span\((a, b)\) and the vectors \(c^\perp\) and \(d^\perp\) in the Span\((c, d)\). Now, one can complete the original set of vectors to a full product basis between \(A\) and \(BC\) with the states \(\{|0, a^\perp\}, |1, b^\perp\}, |+, c^\perp\}, |-, d^\perp\}\}. By the symmetry of the states, this is also true for the other splits \(AB\) versus \(C\) and \(AC\) versus \(B\). This implies that the density matrix \(\rho_{\text{Shifts}}\) constructed as in Eq. (5.4.6) of the UPB Shifts has multipartite bound entanglement. If the entanglement was distillable, then it would be possible to make entanglement over some bipartite split, say, \(A\) and \(BC\). This is in contradiction with the fact that these states are 2-way separable and the entanglement cannot be created by local operations and classical communication.

This argument can be generalized to any multipartite UPB, even though the partial transposition criterion cannot be applied directly to a multipartite state. Let \(S\) be a multipartite UPB. The density matrix \(\rho_S\) derived as in Eq. (5.4.6) from \(S\) has bound entanglement. This follows from the fact that for any bipartite split on the multipartite system into a system 1 and a system 2 by grouping of the parties, the matrix \((\text{id}_1 \otimes T_2)(\rho_S)\) is positive semidefinite. This implies that \(\rho_S\) considered as a density matrix on system 1 and system 2 is either separable or has bound entanglement. Then it follows that any global entanglement can never be distilled, as this distillation would create free entanglement over some bipartite split. Any entanglement in the density matrix \(\rho_S\) of a multipartite UPB \(S\) must therefore be bound.

**General UPBs**

It is possible to generalize the first three examples of UPBs to higher dimensions and more parties. We list some of these generalizations:
- **GenShifts**, a UPB on $\otimes_{i=1}^{2k-1} \mathcal{H}_2$ with $2k$ members. The first state is $|0, \ldots, 0, 0\rangle$. The second is

$$|1, \psi_1, \psi_2, \ldots, \psi_{k-1}, \psi_{k-1}^\perp, \ldots, \psi_1^\perp, \psi_1\rangle.$$  

(5.4.8)

The states $|\psi_i\rangle$ and $|\psi_j\rangle$ for all $i \neq j$ are neither orthogonal nor identical. Also, $|\psi_i\rangle$ is neither orthogonal nor identical to the state $|0\rangle$ for all $i$. The other states in the UPB are obtained by (cyclic) right shifting the second state, i.e. the third state is

$$|\psi_1^+, 1, \psi_1, \psi_2, \ldots, \psi_{k-1}, \psi_{k-1}^+, \ldots, \psi_1^+\rangle.$$  

(5.4.9)

These states are all orthogonal in the following way. The state $|0, \ldots, 0, 0\rangle$ is special and it is orthogonal to all the other states as they all have a $|1\rangle$ for some party. Leaving this special state aside, all states are orthogonal to the next state, their first right-shifted state, by the orthogonality of $|\psi_{k-1}\rangle$ and $|\psi_{k-1}^\perp\rangle$. All states are orthogonal to the 2nd right-shifted state by the orthogonality of $|\psi_1\rangle$ and $|\psi_1^+\rangle$. The 3rd right-shifted state is made orthogonal with $|\psi_{k-2}\rangle$ and $|\psi_{k-2}^\perp\rangle$. We can continue this until the last $(2k - 2)$th right-shifted state and we are done.

As there are no states repeated on one side in the UPB all sets of two states span a two-dimensional space and Lemma 4 implies that the set is a UPB.

- **GenTiles**, a bipartite PB on $n \otimes n$ where $n$ is even. These states have a tile structure which in the case of $6 \otimes 6$ is shown in Fig. 5.2. A tile represents one or more states. For example, the tile in the upperleft corner of Fig. 5.2 represents 2 states each of which is of the form

$$(\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) \otimes |0\rangle.$$  

(5.4.10)

The general construction is the following. One labels a set of $n$ orthonormal states as $|0\rangle, \ldots, |n-1\rangle$. One takes $n(n/2 - 1)$ states of the form $|k\rangle \otimes |\omega_{m,k+1}\rangle$, $m = 1, \ldots, n/2 - 1$, and $k = 0, \ldots, n - 1$ where $|\omega_{m,k}\rangle$ is defined as

$$|\omega_{m,k}\rangle = \sum_{j=0}^{n/2-1} \omega^{jm} |j + k \text{ mod } n\rangle.$$  

(5.4.11)

where $\omega = e^{i\pi/n}$ and thus $\omega^{jm} = e^{i4\pi jm/n}$. Note that $\langle \omega_{m,k} | \omega_{n,k}\rangle$ is proportional to $\delta_{mn}$. Similarly, one takes $|\omega_{m,k}\rangle \otimes |k\rangle$, $m = 1, \ldots, n/2 - 1$, and $k = 0, \ldots, n - 1$. Then one adds the “stopper” which is the state $\sum_i |i\rangle \otimes \sum_j |j\rangle$. Note that the set has $n^2 - 2n + 1$ states, which is much more than the minimum of Eq. (5.4.5). This construction can be proved to be a UPB in $4 \otimes 4$ and $6 \otimes 6$ by exhaustive checking of all partitions. This procedure runs into problems for arbitrary high dimension, but one may conjecture that

**Conjecture 1** The set of states GenTiles forms a UPB on $n \otimes n$ for all even $n \geq 4$. 

5.4 Product Bases, Local Distinguishability and Bound Entanglement

Figure 5.2: Tile structure of the bipartite $6 \otimes 6$ UPB.

- Tensor powers of UPBs. The following theorem holds:

**Theorem 3** Given two bipartite UPBs $S_1$ and $S_2$ with members $|\psi^1_i\rangle = |\alpha^1_i\rangle \otimes |\beta^1_i\rangle$, $i = 1, \ldots, l_1$ on $n_1 \otimes m_1$ and members $|\psi^2_i\rangle = |\alpha^2_i\rangle \otimes |\beta^2_i\rangle$, $i = 1, \ldots, l_2$ on $n_2 \otimes m_2$ respectively. The PB $\{ |\psi^1_i\rangle \otimes |\psi^2_i\rangle \}_{i=1}^{l_1} \otimes \{ |\psi^2_i\rangle \}_{i=1}^{l_2}$ is a bipartite UPB on $n_1 n_2 \otimes m_1 m_2$.

**Proof** Assume the contrary, i.e. there is a product state that is orthogonal to this new ensemble which we call PB$^2$. The idea is to show that this leads to a contradiction and thus PB$^2$ is a UPB. Note first that for any UPB a partition $P$ into a set with 0 states for Bob and all states for Alice give rise to a $p^A$ (see Lemma 4) that has full rank; the states on Alice's side together must span the entire Hilbert space of Alice. Also note that if one takes a tensor product of two UPBs this partition in which all states are assigned to Alice still leads to a $p^A$ that has full rank on Alice's side as $\text{Rank}(p^A) = \text{Rank}(p^A_1) \cdot \text{Rank}(p^A_2)$.

The set PB$^2$ has $l_1 l_2$ members. The new hypothetical product state to be added to the set has to be orthogonal to each member either on Bob's side or on Alice's side, or on both sides. One can represent such an orthogonality pattern as a rectangle of size $l_1$ (number of columns) by $l_2$ (number of rows) filled with the letters A and B, depending on how the new state is orthogonal to a member of the PB$^2$, see Fig. 5.3. When this hypothetical state is orthogonal on both sides, we are free to choose an A or B in the corresponding square. Consider a row of this rectangle. The pattern of As and the Bs can be viewed as a partition of the $S_1$ UPB. For example in the partition of $S_1$ corresponding to the first row in Fig. 5.3 Alice gets the states $|\alpha^1_1\rangle$ and $|\alpha^1_3\rangle$ and Bob gets $|\beta^1_1\rangle$ and $|\beta^1_2\rangle, \ldots, |\beta^1_{l_1}\rangle$. Since $S_1$ is a UPB, either Alice's states span the full Hilbert space of
dimension $n_1$ or Bob's states span the full Hilbert space of dimension $m_1$. Assume that Bob's states span the full Hilbert space of dimension $m_1$. Then of course the states $|\beta_1^1\rangle$ and $|\beta_1^2\rangle$ lie in the space spanned by $|\beta_1^1\rangle$ and $|\beta_1^2\rangle$, ..., $|\beta_1^{m_1}\rangle$. Thus any hypothetical product state that is orthogonal to all states $|\beta_1^1\rangle \otimes |\psi_1^2\rangle$, $|\beta_1^2\rangle \otimes |\psi_1^2\rangle$, ..., $|\beta_1^{m_1}\rangle \otimes |\psi_1^2\rangle$, is also orthogonal to $|\beta_1^1\rangle \otimes |\psi_1^2\rangle$ and $|\beta_1^2\rangle \otimes |\psi_1^2\rangle$. Thus filling the whole row with Bs is a possible way to make the new state orthogonal. This argument can be applied to every row and every column, making them either all As or all Bs. This will eventually lead to a rectangle with only As or with only Bs. This implies however that $\Pi^2$ does not have full rank on either Alice's or Bob's side which is in contradiction with the original sets forming UPBs.

Figure 5.3: The As and Bs denote on what side a hypothetical product state is orthogonal to the members of $\Pi^2$.

The theorem has the consequence that arbitrary tensor powers of bipartite UPBs are again UPBs. The theorem holds for multipartite states as well, where patterns of As and Bs are replaced by As, Bs, Cs etc.

- A generalization of the UPB Pent to $3 \otimes 3 \otimes 3$. Define the following states

$$\vec{v}_i = N (\cos \frac{2\pi i}{7}, \sin \frac{2\pi i}{7}, h), \quad i = 0, \ldots, 6,$$

with $h = \sqrt{-\cos \frac{4\pi}{7}}$ and $N = 1/\sqrt{1 + \cos \frac{4\pi}{7}}$. The following seven states in $3 \otimes 3 \otimes 3$ form the UPB Sept

$$\vec{p}_i = \vec{v}_i \otimes \vec{v}_{2i \mod 7} \otimes \vec{v}_{3i \mod 7}, \quad i = 0, \ldots, 6.$$

The orthogonality of these vectors $\vec{p}_i$ is shown in Fig. 5.4. To prove that these states form a UPB, we must show that any subset of three of them on one of the three sides (Lemma 4) spans the full three-dimensional space. As the vectors $\vec{v}_i$ form the apex of a regular septagonal pyramid, there is no subset of three of them that lies in a two-dimensional plane. It is not known whether the complementary state $p_{\text{Sept}}$ has bipartite bound entanglement or whether it is a separable state over a bipartite split.
This construction can be extended to $3^m$; we have $n$ parties and $p = 2n + 1$ states where $p$ is a prime number. Thus one can have $(n,p) = (2, 5), (3, 7), (5, 11)$ etc. The states in the polygonal pyramid with $p$ vertices are defined as
\[
\vec{v}_i = N_p(\cos \frac{2\pi i}{p}, \sin \frac{2\pi i}{p}, h_p), \quad i = 0, \ldots, 2n. \tag{5.4.14}
\]

In \textbf{Sept} and \textbf{Pent}, $h_p$ was chosen such that nonadjacent vertices were orthogonal. For higher primes $p$ one has to make a choice dependent on $p$. In order for the vectors to the vertex $i$ and to the vertex $m + i$ to be made orthogonal by lifting the vectors out of the plane of the polygon, we must have
\[
\frac{\pi}{2} \leq \frac{2\pi m}{p} (\leq \pi), \tag{5.4.15}
\]
i.e. the angle between the vectors in the plane must be larger than 90 degrees. One can always find such an $m$ given a $p$, for example, for $p = 7$, $m = 2$ or 3. With the choice of $m$ one fixes $h_p$ and $N_p$ as
\[
h_p = \sqrt{-\cos \frac{2\pi m}{p}}, \quad N_p = 1/\sqrt{1 + |\cos \frac{2\pi m}{p}|}. \tag{5.4.16}
\]

Finally, the UPB is
\[
\vec{v}_i = \vec{v}_i \otimes \vec{v}_{2i \mod p} \otimes \ldots \otimes \vec{v}_{m \mod p}, \quad i = 0, \ldots, 2n. \tag{5.4.17}
\]

The primality of $p$ ensures that there are no states repeated on one side: if $ki \mod p = kj \mod p$ for some integers $i \neq j$ and some integer $k = 1, \ldots, 2n$ then this would imply that $p$ is divisible. Orthogonality is also ensured by primality. As in Fig. 5.4 there will be a party for whom next neighbor states are orthogonal, there will be a party for whom every second neighbor states is orthogonal, etc. up to the $n$th neighbor. This implies that all vertices in the orthogonality graph are mutually connected (orthogonal). From basic three-dimensional geometry it follows that any set of three vectors has full rank when $h_p \neq 0$ and thus these generalized sets form UPBs.

![Figure 5.4: The Sept UPB on $3 \otimes 3 \otimes 3$.](image-url)
• We would like to mention a conjecture by Peter Shor on the existence of a UPB based on quadratic residues. These are sets of orthogonal product states on \( n \otimes n \) where \( n \) is such that \( 2n - 1 \) is a prime \( p \) of the form \( 4m + 1 \). Thus we can have \((m, p, n) = (1, 5, 3), (3, 13, 7) \) etc. The sets contains \( p = 2n - 1 \) members, the minimal number for a UPB (Eq. (5.4.5)). Let \( Z_p^* \) be \( Z_p \setminus \{0\} \). Let \( Q_p \) be a group of quadratic residues, that is, elements \( q \in Z_p^* \) such that

\[ q = x^2 \mod p. \tag{5.4.18} \]

for an integer \( x \). The set \( Q_p \) is a group under multiplication. The order of the group is \( \frac{p-1}{2} \). The following properties hold: when \( q_1 \in Q_p \) and \( q_2 \notin Q_p \), a quadratic nonresidue, then \( q_1q_2 \notin Q_p \). Also, if \( q_1 \notin Q_p \) and \( q_2 \notin Q_p \), then \( q_1q_2 \in Q_p \) [127]. The states of the UPB are

\[ |Q(a)\rangle \otimes |Q(xa)\rangle \text{ for } a \in Z_p, \quad x \in Z_p^*, \quad x \notin Q_p, \tag{5.4.19} \]

where

\[ |Q(a)\rangle = (N, 0, \ldots, 0) + \sum_{q \in Q_p} e^{2\pi i qa/p} e_q, \tag{5.4.20} \]

where \( N \) is a normalization constant to be fixed for orthogonality and \( e_q \) are unit vectors of the form \((0, 1, 0, \ldots, 0), (0, 0, 1, 0, \ldots, 0) \) etc. The dimension \( n \) of the Hilbert space is \( \frac{p+1}{2} \), one more than the order of \( Q_p \). One can prove that these vectors can be made orthogonal by an appropriate choice of \( N \):

\[ \langle Q(a)|Q(b)\rangle \langle Q(xa)|Q(xb)\rangle = (|N|^2 + \sum_{q \in Q_p} e^{2\pi i qa/p}(|N|^2 + \sum_{q \in Q_p} e^{2\pi i qx(b-a)/p}). \tag{5.4.21} \]

One uses the properties of \( Q_p \) to find that for \((b-a) \neq 0\):

\[ \sum_{q \in Q_p} e^{2\pi i q(b-a)/p} + \sum_{q \in Q_p} e^{2\pi i qx(b-a)/p} = \sum_{x \in Z_p^*} e^{2\pi i x(b-a)/p} = -1. \tag{5.4.22} \]

Thus the orthogonality relation of Eq. (5.4.21) for \( b \neq a \) is of the form

\[ (|N|^2 + s)(|N|^2 - 1 - s) = 0, \tag{5.4.23} \]

where

\[ s = \sum_{q \in Q_p} e^{2\pi i q(b-a)/p}. \tag{5.4.24} \]

Note that \( s \) can take two values depending on whether \( b - a \) is a quadratic residue or a quadratic nonresidue. In order to show that \( s \) is real, one considers \( s^* \) in which one sums over \(-q\). As \( q \in Q_p \) and \(-1 \in Q_p \) when \( p \) is of the form \( 4m + 1 \) (see Theorem 82,[127]), we have that \(-q \in Q_p \). Therefore \( s = s^* \). Thus for all values that \( s \) can take, Eq. (5.4.23) has a solution for \( N \).
Conjecture 2 (Shor) The states given in Eq. (5.4.19) and Eq. (5.4.20) on $n \otimes n$ with $2n - 1$ a prime of the form $4m + 1$ with the appropriate value of $N$ determined by the solution of Eq. (5.4.23) form a UPB.

The proof will require the application of Lemma 4, that is, one must show that any set of $n$ states on either side spans the full $n$-dimensional Hilbert space. This conjecture has been proved for $p = 5$, $p = 13$ and $p = 17$. These sets form a generalization of the Pent UPB that was presented in section 5.4.2 and Figure 5.1. Drawn as graphs as in Fig. 5.1, they are regular polygons, with a prime number $p$ (of the form $4m + 1$) of vertices. The elements of the quadratic residue group $Q_p$ correspond to the periodicity of the vectors that are orthogonal on one side. For example, when $p = 13$, one has quadratic residues $1, 3, 4, 9, 10$ and $12$. Thus on, say, Alice’s side, every vertex is connected to its first neighbor (1), every vertex is connected with the 3rd neighbor (3) etc. On Bob’s side the orthogonality pattern follows from the quadratic nonresidues.

5.4.4 Global versus Local Rank

The construction of bound entangled states based on UPBs suggests that bound entangled density matrices only come with a large rank. The idea is that when a basis is nearly complete, it is always possible to extend the basis and therefore our construction fails. The following theorem captures this observation and is relevant for any kind of bipartite bound entangled state with PPT. The theorem was conjectured by the author and proved together with P. Horodecki [128].

Theorem 4 Let $\rho$ be a bipartite density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. Define $R_A = \text{Rank}(\text{Tr}_A \rho)$ and similarly $R_B$. Let $R$ be the rank of $\rho$ itself. If

$$\max(R_A, R_B) > R,$$  \hspace{1cm} (5.4.25)

then $\rho$ is distillable.

Proof First of all, one can observe that when $\max(R_A, R_B) > R$ the state has to be entangled. Any separable state can be written as a convex combination of a set of product states $\{|\psi_i, \phi_i\}\}$. The number of linearly independent states $|\psi_i\rangle$ which determines $R_A$ is a lower bound on the number of linearly independent states $|\psi_i, \phi_i\rangle$ which determines $R$, and similarly for $R_B$.

Without loss of generality let $R_A$ be the largest local rank. Let $\rho_A = \text{Tr}_A \rho$ in its diagonal form be diag$(\lambda_1, \ldots, \lambda_{R_A}, 0, \ldots, 0)$. One can apply a local filter [131] on Alice’s side to the state $\rho$.

$$\rho_W = \frac{(W \otimes 1) \rho (W^\dagger \otimes 1)}{\text{Tr}(W \otimes 1) \rho (W^\dagger \otimes 1)},$$  \hspace{1cm} (5.4.26)
where $W = \text{diag}(1/\sqrt{\lambda_1}, \ldots, 1/\sqrt{\lambda_{RA}}, 0, \ldots, 0)$ in the same basis as $\rho_A$. The filtering corresponds to the performance of a POVM measurement by Alice. The operation elements of her POVM measurements are $cW$ and $\sqrt{1 - |c|^2}W^\dagger W$ where $c$ is chosen such that $1 - |c|^2 W^\dagger W$ has eigenvalues in the interval $[0, 1]$. Then with probability $p_W = \text{Tr}(cW \otimes 1) \rho (c^*W^\dagger \otimes 1)$ the state $\rho_W$ is obtained and with probability $1 - p_W$ the filtering fails. Note that it is not a problem to have a certain probability of failure in a distillation protocol as one will have an arbitrary number of copies of the state. The reduced density matrix $\rho_{AW}$ of the filtered state $\rho_W$ has the same rank and its eigenvalues are equal to $\frac{1}{R^A}$ or 0. The rank of $\rho$ can only decrease or stay the same by filtering. From this it follows that for any eigenvalue $\lambda_{\rho_{AW}}$

$$\lambda_{\rho_{AW}} = \frac{1}{R^A} < \frac{1}{R} \leq \lambda_{\rho_{PW}}^{\text{max}},$$

(5.4.27)

where $\lambda_{\rho_{PW}}^{\text{max}}$ is the largest eigenvalue of $\rho_W$. Now we invoke a theorem in Ref. [131] which says that any bipartite density matrix $\rho$ for which there exists a pure state $|\psi\rangle$ such that

$$\langle \psi | (\rho_A \otimes 1) - \rho | \psi \rangle < 0,$$

(5.4.28)

is distillable. Take $|\psi\rangle$ to be the eigenvector of $\rho_W$ with maximum eigenvalue and it follows from Eq. (5.4.27) and Eq. (5.4.28) that $\rho_W$ and therefore $\rho$ is distillable. This completes the proof. □

The consequence of this theorem is that there exists no bipartite bound entangled state on any $\mathcal{H}_A \otimes \mathcal{H}_B$ that has rank 2. The reason is that when the maximum local rank of a bipartite rank 2 density matrix $\rho$ exceeds 2, Theorem 4 implies that the state is distillable. On the other hand if both local ranks of $\rho$ are smaller than or equal to 2, then the density matrix $\rho$ effectively has support only on a $2 \otimes 2$ subspace. But it is known that all entangled density matrices on $2 \otimes 2$ are distillable [111].

It also follows that any bipartite PB S on $n \otimes m$ with a number of states $k = nm - 2$ is extendible. By construction the complementary state $\rho_S$ has the PPT-property. However, $\rho_S$ has rank 2 and there do not exist bound entangled states with rank 2. Therefore $\rho_S$ must be separable and it follows that S is extendible. One can carry the argument one step further. After adding the new product state to the set S, we can ask whether one can find the last product state of the basis. Again, that state, which is a pure state must have the PPT-property. It is not hard to show that all entangled pure state have the NPT-property and therefore this last basis state must be a product state. Hence we have shown that any bipartite PB S in $\mathcal{H}$ which has dim $\mathcal{H} - 2$ states is not only extendible but also completable.

5.4.5 Local Distinguishability and Uncompletable Product Bases

In the preceding sections we showed how UPBs give rise to entangled states that cannot be distilled. It turns out that this is not the only interesting property that these sets of states have. One can ask whether the members of a UPB are distinguishable by Local quantum Operations and Classical Communication (LO+CC). The situation is the same as we described in section
5.4.1. We will consider sets of product states which are mutually orthogonal, such as the UPBs. This implies that these states are distinguishable when arbitrary quantum measurements are allowed. When the set of states is given by \( \{ |\psi_j\rangle \}_{j=1}^{|S|} \), then a projection measurement with projectors \( \{ \pi_j = |\psi_j\rangle \langle \psi_j | \}_{j=1}^{|S|} \) and \( \pi_{S^+} = 1 - \sum_j \pi_j \) would distinguish the states in the set \( S \). The question is whether measurements that exactly distinguish the set of states can be implemented with local operations and classical communication only. Let us assume that two parties Alice and Bob are given one of the five states in the Pent set and they have to determine by LO+CC which one they have. It is not hard to see that for a set such as Pent straightforward attempts at finding an appropriate series of measurements are bound to fail; the way in which the states are made orthogonal, partially on Alice's side, partially on Bob's side seems to preclude the existence of a perfect measurement. The parties seem to end up with disturbing the states by measuring them and this disturbance then results in a set of non-orthogonal product states that can no longer be distinguished.

![Figure 5.5: Measurement tree for two copies of the Pent ensemble.](image)

In order to understand what kinds of measurement protocols are possible, we consider the situation in which the two parties are given two copies of the same state of the Pent set. We can then show that there is a LO+CC that reliably identifies the states. This measurement procedure is presented in Fig. 5.5. Each level of the tree corresponds to a measurement by either Alice or Bob. After each measurement round Alice and Bob communicate classically to discuss the results. In this protocol only (incomplete) von Neumann measurements (see Chap. 3, sec. 3.2) are performed and they are denoted by their operation elements which are projectors. The states of the Pent set themselves are denoted as \( A_0, \ldots, A_4 \) for Alice's part of the Pent states and \( B_0, \ldots, B_4 \) for Bob's part in correspondence with \( i = 0, \ldots, 4 \) in Eq. (5.4.3). Thus in the first round Alice's measurement has two outcomes, associated with the projector on her \( |0\rangle \) state and the projector on the span of her \( |2\rangle \) and \( |3\rangle \) states, which obey the relation

\[
\pi_0 + \pi_{\text{span}(A_3,A_2)} = 1.
\]  

(5.4.29)

As one can see in Fig. 5.5 by a two-round protocol on the first state, Alice and Bob have reduced the number of states to be distinguished to at most three. Now it is not hard to see that
three orthogonal product states can always be distinguished by von Neumann measurements (see also sec. 5.4.8).

One can associate with the leaves of such a measurement tree the series of projections that resulted in the series of measurement outcomes. For example, in the tree of Fig. 5.5, the leaf all the way to the left can be associated with the projector:

\[ \pi_{A_0} \otimes \pi_{B_0}. \]  

These projectors at the ends of the tree are called 'leaf-projectors'. Aside from local von Neumann measurements a party can also perform local POVM measurements. But by Neumark's theorem [62] any POVM measurement on a Hilbert space \( \mathcal{H} \) can be viewed as an (incomplete) von Neumann measurement in an extended higher dimensional Hilbert space \( \mathcal{H}_{ext} \). When the number of POVM outcomes is finite, this extended Hilbert space is finite. Note that the conversion of a local POVM to a local von Neumann measurement corresponds to a local extension of the Hilbert space, i.e. for a bipartite system a Hilbert space \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \) is extended to \( \mathcal{H}_{ext} = (\mathcal{H}_A \oplus \mathcal{H}'_A) \otimes (\mathcal{H}_B \oplus \mathcal{H}'_B) \) where \( \mathcal{H}'_A \) and \( \mathcal{H}'_B \) are the extensions of the local Hilbert spaces \( \mathcal{H}_A \) and \( \mathcal{H}_B \). In the following analysis the local measurements are restricted to have a finite number of outcomes. Furthermore we require that the number of rounds in the entire protocol is finite. Thus one can say that we restrict ourselves to finite resources in time and space. Every local measurement with a finite number of outcomes can be decomposed into a series of local measurements with two outcomes only with the understanding that subsequent levels of the measurement tree can correspond to actions of the same party.

A special class of local measurements are the measurements that we call dissections. A dissection measurement is one in which the set of states \( S \) is split into two sets 1 and 2. The states themselves are unchanged by the measurement, but the outcome of the measurement tells us whether the state that one is given was in set 1 or in set 2. More general measurement schemes can project the states in \( S \) onto other states that might or might not be orthogonal.

In the last section we briefly mentioned the notion of a completion of a set of orthogonal product states. Let us now give the definition of an uncompletable set of orthogonal product states.

**Definition 6** Consider a multipartite quantum system \( \mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i \) with \( m \) parties of respective dimension \( d_i, i = 1, ..., m \). An uncompletable product basis in \( \mathcal{H} \) is a PB that cannot be completed with orthogonal product states to a full orthonormal product basis for \( \mathcal{H} \).

**Remark** The uncompletable product basis is defined with respect to \( \mathcal{H} \). An orthogonal product basis in \( \mathcal{H} \) could be uncompletable in \( \mathcal{H} \), but completable to a full product basis for \( \mathcal{H}_{ext} \), when the set is embedded in \( \mathcal{H}_{ext} \). In section 5.4.6 we will give an example of such a set.

The following theorem captures an essential connection between completability and exact local distinguishability:
Theorem 5 Given a set $S$ of orthogonal product states (PB) on $H = \bigotimes_{i=1}^{m} H_i$ with dim$H_i = d_i, i = 1, ..., m$. If the set $S$ is exactly distinguishable with finite resources by local incomplete von Neumann measurements on $H_{\text{ext}}$—which can be $H$ itself or any finite local extension of $H$—and classical communication, then the set $S$ is completable to an orthogonal basis for $H_{\text{ext}}$.

Proof One shows how the measurement protocol leads directly to a way to complete the set $S$. At some stage of their protocol, the parties (1) may have been able to eliminate members of the original set of states $S$ and (2) they may have mapped, by performing their von Neumann measurements, the remaining set of orthogonal states into a new set of orthogonal states $S'$. Note that the remaining states have to be orthogonal, otherwise the measurement could never be exact. Determining which member they have in this new set uniquely determines with which state of $S$ they started with. At this stage, party $i_0$ performs a von Neumann measurement. Let $K'$ be the Hilbert space in which the remaining states are known to lie (including the local extensions that are needed in order for any subsequent measurement to be described as a von Neumann measurement). The measurement of party $i_0$ is given by a decomposition of the Hilbert space $K' = K_{\text{else}} \otimes K_{i_0}$ with $K_{\text{else}} = \bigotimes_{j \neq i_0} K_j$, into 2 orthogonal subspaces, $K_{\text{else}} \otimes \pi_1 K_{i_0}$ and $K_{\text{else}} \otimes \pi_2 K_{i_0}$.

If a state in $S'$ lies in one of these subspaces, it will be unchanged by the measurement. If a state $|\alpha\rangle \otimes |\beta\rangle$, where $|\alpha\rangle \in K_{\text{else}}$, is not contained in one of the subspaces, it will be projected onto one of the states $\{|\alpha\rangle \otimes \pi_1 |\beta\rangle, |\alpha\rangle \otimes \pi_2 |\beta\rangle\}$. Let $S''$ be this new projected set of states, containing both the unchanged states in $S'$ as well as the possible projections of the states in $S'$. If one of the subspaces $K_{\text{else}} \otimes \pi_1 K_{i_0}$ or $K_{\text{else}} \otimes \pi_2 K_{i_0}$ does not contain a member of $S''$, it can be 'completed' directly; one can freely choose a product basis for this space. For a subspace that does contain members of $S''$, let us assume that it can be completed with product states orthogonal to members of $S''$. In this way one has completed $S''$ on the full Hilbert space $K$ since the two orthogonal-subspace completions are orthogonal sets and they are a decomposition of $K$. However, one has now completed the set $S''$ rather than the set $S'$. Fortunately, one can replace the projected states $|\alpha\rangle \otimes \pi_1 |\beta\rangle, |\alpha\rangle \otimes \pi_2 |\beta\rangle$ by the original state $|\alpha\rangle \otimes |\beta\rangle$ and 1 orthogonal state by making a linear combination of $|\alpha\rangle \otimes \pi_1 |\beta\rangle$ and $|\alpha\rangle \otimes \pi_2 |\beta\rangle$ orthogonal to $|\alpha\rangle \otimes |\beta\rangle$. These two states are orthogonal to all other states as each $|\alpha\rangle \otimes \pi_1 |\beta\rangle$ was already orthogonal to all other states. Thus at each round of measurement, a completion of the set of states $S'$ is achieved assuming a completion of the subspaces determined by the measurement.

The tree of nested subspaces will always lead to a subspace that contains only a single state of the set, as the measurement protocol was able to tell the states in $S$ apart exactly. But such a subspace containing only one state can easily be completed and thus, by induction, we have proved that the original set $S$ can be completed. $\Box$

Before discussing the consequences of this theorem, we will show how one can strengthen the result to include measurements that have an arbitrary small probability of error. First, one has to define what it means for a set of states to be distinguishable with some probability of
Definition 7 Given a set $S$ of orthogonal product states (PB) on $\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i$ with $\dim \mathcal{H}_i = d_i, i = 1, ..., m$. Let $\mathcal{M}$ be a local incomplete von Neumann measurement protocol on a finite-dimensional Hilbert space $\mathcal{H}_{\text{ext}}$ which can be a local extension of $\mathcal{H}$, that includes classical communication between the local parties. Let $\mathcal{D}(\mathcal{M})$ be a decision scheme that associates each leaf of the measurement tree of $\mathcal{M}$ with a state of the set $S$, meaning that upon the outcomes of leaf $j$, we decide that the associated state $i$ is the state that we were given of the set $S$. A set $S$ is $\epsilon$-distinguishable if there exists an $\mathcal{M}$ and a $\mathcal{D}(\mathcal{M})$ such that

$$P_{\text{suc},\mathcal{M}} = \min_{i \in S} \sum_{j \mid j \to i} \text{Prob}(\pi_j|i) \geq 1 - \epsilon,$$

(5.4.31)

where $\pi_1, \ldots, \pi_k$ are the leaf-projectors of the measurement tree of $\mathcal{M}$. $\text{Prob}(\pi_j|i)$ is the probability that given the state $i$ we obtain the measurement outcomes of leaf $\pi_j$. The sum over the leaf-projectors is constrained to leaf-projectors that lead to deciding for state $i$, which is indicated by $j \to i$.

In words this definition says that the set $S$ is $\epsilon$-distinguishable if the probability of deciding correctly for a state in $S$ is greater than or equal to $1 - \epsilon$ for any state that the parties are given from $S$. This definition makes it possible to state the following lemma:

Lemma 5 Given a set $S$ of orthogonal product states (PB) on $\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i$ with $\dim \mathcal{H}_i = d_i, i = 1, ..., m$. If the set $S$ is $\epsilon$-distinguishable for all $\epsilon > 0$ then $S$ is exactly distinguishable.

Proof As one is restricted to using finite resources, one can set the total number of levels in the binary measurement tree to a certain large number $L$ and set the dimensions of the local extensions $\dim \mathcal{H}_{i,\text{ext}} = d_i, i = 1, ..., m$. All measurement trees (plus decision schemes) that have at most $L$ levels and correspond to local extensions of which the dimensions are upper bounded by $\dim \mathcal{H}_{i,\text{ext}} = d_i,\text{ext}$ can then be characterized by five sets of variables:

1. the structure of the tree $T$, i.e. the distribution of the length of its branches,
2. an assignment $A$ of levels to the various parties A, B, C etc.,
3. the dimension $\text{Dim}$ in which the von Neumann measurement takes place for each node of the tree,
4a) the rank $R$ and the number of the projectors pertaining to each node of the tree,
4b) and the projectors $P$ themselves pertaining to each node of the tree,
5. a decision scheme $D$ that infer from measurement outcomes –the leafs of the tree– decisions about what the original state was.

Consider the function $P_{\text{suc},\mathcal{M}}$ as in Eq. (5.4.31). The domain of this function is the set $(T, A, \text{Dim}, R, P, D)$. The set of trees $T$, assignments $A$, decisions $D$, dimensions $\text{Dim}$ and the set of ranks $R$ of the projectors are all discrete sets with a finite number of elements.
Consider a measurement at a single node. We fix the number of projectors, the dimension of the Hilbert space and the rank of the projectors at this node. Let \((\pi_1, \pi_2)\) be a set of projectors at this node. Then another set \((\pi'_1, \pi'_2)\) can be obtained by unitary transformations \(U_i \pi_i = \pi'_i\). This implies that the set \((\pi_1, \pi_2)\) is a compact set, as the set of unitary transformations in a finite-dimensional Hilbert space is a compact set. The function \(P_{\text{suc}, \mathcal{M}}\) is continuous on this compact set. The entire domain of the function \(P_{\text{suc}, \mathcal{M}}\) is the union of a finite number of compact sets. Then, if there exists measurements and decision schemes such that \(P_{\text{suc}, \mathcal{M}}\) is larger or equal than \(1 - \epsilon\) for all \(\epsilon\), there also exist a scheme for which \(P_{\text{suc}, \mathcal{M}} = 1\). This measurement corresponds to exactly distinguishing the members of \(S\).

**Corollary 1** Given a set \(S\) of orthogonal product states \((PB)\) on \(\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i\) with \(\dim \mathcal{H}_i = d_i, i = 1, \ldots, m\). If this set \(S\) is \(\epsilon\)-distinguishable for all \(\epsilon > 0\), then \(S\) is exactly completable on \(\mathcal{H}_{\text{ext}}\), a locally extended Hilbert space or \(\mathcal{H}\) itself.

This follows from Theorem 5 and Lemma 5.

Let us give a final theorem, that relates the question of completabiliy to the property of entanglement:

**Theorem 6** Given a set \(S\) of orthogonal product states \((PB)\) on \(\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i\) with \(\dim \mathcal{H}_i = d_i, i = 1, \ldots, m\). If the set \(S\) is \(\epsilon\)-distinguishable for all \(\epsilon > 0\), then the complementary density matrix \(\rho_S\), Eq. (5.4.6), is separable.

**Proof** If the exact measurement is a von Neumann measurement on \(\mathcal{H}_i\), then by Corollary 1 the set \(S\) can be completed with product states to a basis for \(\mathcal{H}_i\). Thus, the density matrix \(\rho_S\) which is the uniform mixture of these product states that complete \(S\), is separable. If the exact measurement is a von Neumann measurement on \(\mathcal{H}_{\text{ext}}\), then the density matrix \(\rho_{S, \text{ext}}\) is separable. One can obtain \(\rho_S\) on \(\mathcal{H}\) by local projections from \(\mathcal{H}_{\text{ext}}\) onto \(\mathcal{H}\) and therefore \(\rho_S = P_{\text{it}} \rho_{S, \text{ext}} P_{\text{it}}\) is separable as well.

This theorem implies that a multipartite UPB \(S\) is not distinguishable with arbitrary small probability of error by LO+CC, using finite resources, since the density matrix \(\rho_S\) is entangled. The UPBs are new illustrations of the phenomenon of nonlocality without entanglement. The strength of the result as compared to the results in Ref. [125], is that the indistinguishability has been proved for any UPB, whereas in Ref. [125] only the set of states of Eq. (5.4.1) were shown not to be distinguishable with arbitrary small probability of error. The weakness of this result is that we have restricted the set of measurements to ones that can be performed using finite resources. This was necessary as a POVM measurement with an infinite number of outcomes describes a von Neumann measurement in an infinite dimensional Hilbert space. It is not clear how to extend the notions of completabiliy on an infinite dimensional Hilbert space. Also, it is unclear whether a result such as Lemma 5 would hold for measurements that could use infinite resources.
5.4.6 Local Extensions and Deficits of Product States

In the last section care has been taken to include POVM measurements in a local measurement scheme. But do there exist PBs that are exactly distinguishable by POVMs but not by von Neumann measurements in the original Hilbert space? It turns out that there are such sets. Here is an example of such a set on $3 \otimes 4$, the set PO. Consider the states $v_j \otimes w_j^\perp$, $j = 0, \ldots, 4$ with $v_j$ the states of the Pent UPB as in Eq. (5.4.2) and $w_j^\perp$ defined as

$$w_j^\perp = \sqrt{\frac{1}{5}} \left( \frac{1}{\cos(\pi/5)} \cos(2j\pi/5), \frac{1}{\cos(\pi/5)} \sin(2j\pi/5), \frac{1}{\cos(\pi/5)} \cos(4j\pi/5), \frac{1}{\cos(\pi/5)} \sin(4j\pi/5) \right).$$

Note that $w_j^\perp w_{j+1} = 0$ (addition mod 5). The orthogonality graph of these states is the same as for Pent, Figure 5.1. One can show that this set, albeit extendible on $3 \otimes 4$, is not computable: One can at most add three vectors: $v_0 \otimes (w_0^\perp, w_1^\perp, w_4^\perp)$, $v_2 \otimes (w_2^\perp, w_3^\perp, w^\perp)$, and $(v_0, v_3)^\perp \otimes (w_1^\perp, w_3^\perp, w_4^\perp)$.

The POVM measurement that is performed by Bob on the four-dimensional side has five projector elements, each projecting onto a vector

$$\bar{u}_j = \frac{1}{\sqrt{2}} (\sin(2j\pi/5), \cos(2j\pi/5), -\sin(4j\pi/5), \cos(4j\pi/5)),$$

with $j = 0, \ldots, 4$. Note that $\bar{u}_0$ is orthogonal to vectors $\bar{w}_0, \bar{w}_2$ and $\bar{w}_3$, or, in general, $\bar{u}_i$ is orthogonal to $\bar{w}_i, \bar{w}_{i+2}, \bar{w}_{i+3}$ (addition mod 5). This means that upon Bob’s POVM measurement outcome, three vectors are excluded from the set; then the remaining two vectors on Alice’s side, $\bar{v}_{i+1}$ and $\bar{v}_{i+4}$, are orthogonal and can thus be distinguished.

Since the set is distinguishable by a POVM, it is computable. The completion of this set in $3 \otimes 5$ is particularly simple. Bob’s Hilbert space is extended to a five-dimensional space. The POVM measurement can be extended to a projection measurement in this five-dimensional space with orthogonal projections onto the states $\bar{x}_i = (\bar{u}_i, 0) + \frac{1}{2}(0, 0, 0, 0, 1)$. Then a completion of the set in $3 \otimes 5$ are the following ten states:

$$
\begin{align*}
(v_1, v_4)^\perp &\otimes \bar{x}_0, \quad v_0 \otimes (w_0^\perp \in \text{Span}(\bar{x}_4, \bar{x}_1)), \\
(v_0, v_2)^\perp &\otimes \bar{x}_1, \quad v_1 \otimes (w_1^\perp \in \text{Span}(\bar{x}_0, \bar{x}_2)), \\
(v_1, v_3)^\perp &\otimes \bar{x}_2, \quad v_2 \otimes (w_2^\perp \in \text{Span}(\bar{x}_1, \bar{x}_3)), \\
(v_2, v_4)^\perp &\otimes \bar{x}_3, \quad v_3 \otimes (w_3^\perp \in \text{Span}(\bar{x}_2, \bar{x}_4)), \\
(v_0, v_3)^\perp &\otimes \bar{x}_4, \quad v_4 \otimes (w_4^\perp \in \text{Span}(\bar{x}_3, \bar{x}_0)).
\end{align*}
$$

There is another interesting feature of this set. Let’s take the set PO and add one of the product states, say the vector,

$$v_0 \otimes (w_0^\perp, w_1^\perp, w_4^\perp),$$

to make it a six-state ensemble $\text{PO}^+$. The complementary density matrix $\rho_{\text{PO}^+}$, Eq. (5.4.6), has rank $12 - 6 = 6$. Is $\rho_{\text{PO}^+}$ a separable density matrix? We can enumerate the product states
that are orthogonal to the members of $\text{PO}^+$, but are not necessarily mutually orthogonal:

$$
\tilde{v}_3 \otimes (\tilde{w}_2, \tilde{w}_3, \tilde{w}_4)^{\perp},
\tilde{w}_2 \otimes (\tilde{w}_1, \tilde{w}_2, \tilde{w}_3)^{\perp},
(\tilde{v}_1, \tilde{v}_3)^{\perp} \otimes (\tilde{w}_1, \tilde{w}_2, \tilde{w}_4)^{\perp},
(\tilde{v}_1, \tilde{v}_2)^{\perp} \otimes (\tilde{w}_1, \tilde{w}_3, \tilde{w}_4)^{\perp}.
$$

(5.4.36)

This means that the space on which $\rho_{\text{PO}^+}$ has support contains only four product states, whereas $\rho_{\text{PO}^+}$ has rank 6. Therefore $\rho_{\text{PO}^+}$ must be entangled. The entanglement of $\rho_{\text{PO}^+}$ is bound by construction.

We have constructed a new bound entangled state whose range is not without product states but has a product state deficit. As any UPB set, the set $\text{PO}^+$ is not locally distinguishable with finite means. This construction works in a very general way:

**Lemma 6** Given a set $S$ of orthogonal product states (PB) on $\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i$ with $\dim \mathcal{H}_i = d_i$, $i = 1, ..., m$. If the set $S$ is not computable to a full basis for $\mathcal{H}$, but is completable in some $\mathcal{H}_{ext}$, then there always exist a set of orthogonal product states in $\mathcal{H}_{ext}^S$ such that when we add these states to $S$ to make the ensemble $S^+$, the complementary density matrix $\rho_{S^+}$ is bound entangled.

*Proof* Assume that there does not exist such an augmented ensemble $S^+$. This will lead to a contradiction. The fact that $S$ is completable in $\mathcal{H}_{ext}$ makes it possible to add at least one product state to $S$, see Theorem 6. Let us call this state $|\psi_1\rangle$. The density matrix $\rho_{S_1}$ complementary to the ensemble $S_1 = S \cup \{ |\psi_1\rangle \}$ is either entangled or separable. If it is entangled, then we have found the desired augmentation of $S$. If it is separable, then there is at least one state, let us call it $|\psi_2\rangle$, in the range of $\rho_{S_1}$ which is a product state. Note that $|\psi_2\rangle$ is orthogonal to $|\psi_1\rangle$. Then we can augment $\rho_{S_1}$ with this new orthogonal product state $|\psi_2\rangle$ to make the set $\rho_{S_2}$. Consider its complementary density matrix $\rho_{S_2}$. Repeat the arguments as before. If we find that all density matrices $\rho_{S_1}, \rho_{S_2}, ..., \rho_{\dim \mathcal{H}_{ext}^S}$ are separable, then we have found a completion of the original set $S$ with orthogonal product states. This leads to a contradiction, because $S$ is not computable in $\mathcal{H}$.

*Remark* While the lemma shows that there exists a set of orthogonal product states that when added to the set $S$ leads to a bound entangled state, the proof also suggests a simple way to find this set. The bound entangled state that we find by this procedure can be a bound entangled state corresponding to a UPB, that is the augmented set $S^+$ is a UPB, or it can be an entangled state, based on a set such as $\text{PO}^+$, which is supported on a subspace which has a product state deficit.

### 5.4.7 Rank and the Optimal Decomposition of a Density Matrix

Some of the uncompletable sets of product states exhibit additional interesting properties. It was shown by Uhlmann [132] that every bipartite density matrix $\rho$ admits an optimal decomposition, that is, a decomposition that achieves the entanglement of formation $E(\rho)$, Eq.
(5.2.11), with at least \( \text{Rank}(\rho) \) and at most \( \text{Rank}(\rho)^2 \) different pure states. No examples of density matrices for which more than \( \text{Rank}(\rho) \) states are needed to construct the optimal decomposition were previously known. By numerical minimization it was found that the state complementary to the Tiles UPB, as introduced in section 5.4.2, has an entanglement of formation of 0.213726 bits. This complementary state \( \rho_{\text{Tiles}} \) has rank 4. However, it was found that the optimal ensemble of pure states consists of five pure states. A similar result was found for the Pent UPB which has an entanglement of 0.232635 bits, made by mixing together five pure states. Thus both these density matrices are numerical examples of states for which more states are needed in the optimal decomposition than the rank of the state.

The following result exhibits a whole class of separable states which have this peculiar property.

**Theorem 7** Let \( \{ |\alpha_i \rangle \otimes |\beta_i \rangle \}_{i=1}^{|S|} \) be a PB \( S \) in \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \). If \( S \) is uncompletable in \( \mathcal{H} \), but \( S \) is completable in some local extension \( \mathcal{H}_{\text{ext}} \) of \( \mathcal{H} \), then \( \rho_S \) has the property that the number of different pure states in the optimal decomposition of \( \rho_S \) exceeds the rank of \( \rho_S \).

**Proof** Since the set of states \( S \) is completable in a local extension of \( \mathcal{H} \), the state \( \rho_S \) is separable by Theorem 6. However we know that \( \rho_S \) was uncompletable in \( \mathcal{H} \), therefore \( \rho_S \) cannot be decomposed with an ensemble of orthogonal product states. Any optimal decomposition of \( \rho_S \) has to use nonorthogonal product states. The von Neumann entropy of \( \rho_S \) is equal to \( S(\rho_S) = \log \text{Rank}(\rho_S) \) as \( \rho_S \) is the identity matrix on a space of dimension \( \text{Rank}(\rho_S) \). In order to achieve this entropy the optimal decomposition of \( \rho_S \) has to use more than \( \text{Rank}(\rho_S) \) product states, as any density matrix \( \rho \) which is a mixture of only \( n \) non-orthogonal states has entropy strictly less than \( \log n \) bits. \( \square \)

The only example so far is the set PO in \( 3 \otimes 4 \), which was distinguishable by a set of orthogonal projectors in \( 3 \otimes 5 \), but could not be completed in \( 3 \otimes 4 \). The complementary density matrix \( \rho_{\text{PO}} \) on \( 3 \otimes 4 \) has rank seven, but the separable decomposition consists of ten non-orthogonal states. These ten non-orthogonal product states are obtained by projecting the orthogonal states of the completion, Eq. (5.4.34) back into the \( 3 \otimes 4 \) Hilbert space. It is not known whether there exists a separable decomposition with more than seven but with less than ten states.

### 5.4.8 Restrictions

The method to create bound entangled states from UPBs is not always successful. In particular one can show that

**Theorem 8** Any set of orthogonal product states \( \{ |\alpha_i \rangle \otimes |\beta_i \rangle \}_{i=1}^k \) in \( 2 \otimes n \) for any \( n \geq 2 \) is distinguishable by local measurements and classical communication and therefore completable to a full product basis for \( 2 \otimes n \).
5.4 Product Bases, Local Distinguishability and Bound Entanglement

**Proof** The measurement is a three round protocol. Let Alice be associated with the two-dimensional side and Bob with the \( n \)-dimensional side. Alice divides \( S \) in subsets \( P_i \) in the following way:

\[
P_i = \{ |\alpha_i\rangle \otimes |\beta_i^1\rangle, |\alpha_i\rangle \otimes |\beta_i^2\rangle, \ldots, |\alpha_i^k\rangle \otimes |\beta_i^k\rangle \}
\]

i.e., Alice's part of the states in set \( P_i \) is either \( |\alpha_i\rangle \) or \( |\alpha_i^\perp\rangle \). The states \( |\alpha_i\rangle \) and \( |\alpha_j\rangle \) for \( i \neq j \) are neither orthogonal nor identical. When \( P_i \) contains a set of states \( \{ |\alpha_i\rangle \otimes |\beta_i^1\rangle, \ldots, |\alpha_i^k\rangle \otimes |\beta_i^k\rangle \} \) for some \( k > 1 \) then due to the orthogonality of the states, we must have that \( \langle \beta_i^j | \beta_i^m \rangle = \delta_{jm} \) for \( j, m = 1, \ldots, k \). The same is true for \( P_i \) containing a set of states in which \( |\alpha_i^\perp\rangle \) is repeated. Furthermore, all the members of the set \( P_i \) have to be orthogonal to all the members of a set \( P_j \) for \( i \neq j \) on Bob's side as they are never orthogonal on Alice's side. The measurement goes as follows. Bob performs a measurement of which the operation elements are projectors \( \Pi_{ij} \) on the subspace spanned by his side of the states in each \( P_i \). These projectors have the property that \( \Pi_{ij} \Pi_{jk} = 0 \) for \( i \neq j \). The outcome tells Bob in which set \( P_i \) the original state lies. After Bob sends this information, the label \( i \), to Alice, she does a measurement that distinguishes \( |\alpha_i\rangle \) from \( |\alpha_i^\perp\rangle \). Then Bob is left to finish the protocol by distinguishing between states that repeat on Alice's side, for example the states \( |\alpha_1\rangle |\beta_1^1\rangle \) and \( |\alpha_1\rangle |\beta_1^2\rangle \). He can distinguish between these states, because they are mutually orthogonal on his side. Theorem 5 then implies that \( S \) is computable. \( \square \)

**Local Dissectibility as a Graph Problem**

One can express local dissections on a set of orthogonal product states (PB) as operations on the orthogonality graph of the PB. Consider for example the sets in Fig. 5.7. The dimension of Alice's and Bob's Hilbert space is larger than or equal to four, otherwise these patterns would not be possible. In case (a) it is not hard to see how Alice and Bob would go about measuring the set. State 2 is orthogonal to all the others on Alice's side. Thus Alice can distinguish the sets (2) and (134) by measuring with the local projectors \( \Pi_{a2} \) and \( \Pi_{a2}^\perp \). If she finds (2) the protocol is finished. If she finds (134) Bob continues the measurement. The states 1, 3 and 4 form a clique—a graph in which all the vertices are connected—on Bob's side. Therefore a measurement that uses the projectors \( \Pi_{b1}, \Pi_{b3} \) and \( \Pi_{b4} \) distinguishes perfectly between 1, 3 and 4. These measurements are all dissection measurements, that is, they split the total set of states into two or more subsets in which each state occurs only once. In this case Alice first makes the dissection into the sets (2) and (134), after which Bob dissects (134) as (1)(3)(4). Let us translate such a dissection measurement in graph language. A complete bipartite graph is a graph \( G \) in which the set of vertices \( V \) can be split in two sets \( V_1 \) and \( V_2 \) such that every vertex in \( V_1 \) is connected to every vertex in \( V_2 \) by an edge and vertices of \( V_1 \) and \( V_2 \) are not directly connected amongst each other. The vertices of the orthogonality graph \( G \) of a \( m \)-partite PB \( S \) in \( \mathcal{H} \) represent the members of \( S \). Recall that \( \mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_m \). The edges are colored with \( m \) different colors such that if two members of \( S \) are orthogonal on \( \mathcal{H}_i \), color \( i \) is used for the edge. One can have multiply colored edges between vertices. To describe
whether a multipartite PB is dissecible we will need the notion of a complete bipartite graph of a single color in which vertices in \( V_1 \) (or \( V_2 \)) can be connected amongst each other. We call this kind of graph an (over)complete bipartite graph of a single color \(^3\). Fig. 5.6 shows an example of such a graph, some of the vertices in \( V_1 \) are mutually connected by Bob's edges.

![](image)

**Figure 5.6**: An example of an (over)complete bipartite graph of Bob's color.

One can write down the following translation of a series of dissection measurements into a decomposition of the graph:

**Proposition 7** Let \( S \) be a multipartite PB on \( \mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i \) with \( \dim \mathcal{H}_i = d_i, i = 1, \ldots, m \) represented by an orthogonality graph \( G \). Then \( S \) is exactly distinguishable by local dissections and classical communication iff there exists a decomposition of the graph \( G \) of \( S \) into a hierarchical tree of (over)complete bipartite graphs of a single color such that the leaves of the tree correspond to single vertices.

**Proof** At each round of the dissection measurement the set of vertices \( V \) of the graph \( G \) is cut in two sets \( V_1 \) and \( V_2 \) such that each state represented by a vertex in \( V_1 \) is orthogonal to each state represented by a vertex in \( V_2 \) for the \( i \)th party. In graph language: \( G \) is an (over)complete bipartite graph of color \( i \). Let \( G_1 \) be the graph with vertices \( V_1 \) and the edges connecting vertices in \( V_1 \) and similarly for \( G_2 \). In the next round of measurement each of the graphs \( G_1 \) and \( G_2 \) is cut according to the bipartition in an (over)complete bipartite graph of a possibly different color. This process is repeated until the resulting graphs consist a single vertex. Then we conclude that all the states in \( S \) have been distinguished. \( \Box \)

Let us consider Fig. 5.7(b). There is no (over)complete bipartite graph of a single color. However we can perform a more general von Neumann measurement. Alice can measure with the projector \( \pi_{\alpha_1, \alpha_2} \) and the projector \( \pi_{\alpha_1, \alpha_2}^\perp \) where \( \pi_{\alpha_1, \alpha_2} = 1 - \pi_{\alpha_1, \alpha_2}^\perp \). The projector \( \pi_{\alpha_1, \alpha_2}^\perp \) projects onto states that are orthogonal to \( \ket{\alpha_1} \) and \( \ket{\alpha_2} \). This will distinguish the sets (12) and (4), but it will project state 3 on either \( \pi_{\alpha_1, \alpha_2}^\perp \ket{\alpha_3} \) or \( \pi_{\alpha_1, \alpha_2}^\perp \ket{\alpha_3} \). Thus one can say that we cut the set into subsets (123) and (34). When (34) is found, Bob can finish the protocol directly. When Alice gets (123), she now can distinguish between (1) and (23) since they form a complete bipartite graph. What about the final distinction between 2 and 3? These

\(^3\)There does not appear to exist a standard terminology for this kind of graph.
states started out as orthogonal on Alice's side, then with Alice's first measurement $|\alpha_3\rangle$ was mapped onto $\pi_{\alpha_1,\alpha_2}|\alpha_3\rangle$. This projected state is however still orthogonal to $|\alpha_2\rangle$, as $|\alpha_2\rangle$ did not have a component outside the space spanned by $|\alpha_1\rangle$ and $|\alpha_2\rangle$ and thus

$$0 = \langle \alpha_2 | \alpha_3 \rangle = \langle \alpha_2 | \pi_{\alpha_1,\alpha_2} | \alpha_3 \rangle.$$  \hspace{1cm} (5.4.38)

Here we can notice a more general rule. A local 2-outcome von Neumann measurement is called orthogonality preserving on a set of (multipartite) orthogonal product states $S$ if after measurement the states in $S$ are still mutually orthogonal. Suppose we can find an (over)complete bipartite graph of a single color that includes all the vertices but 1 in the orthogonality graph of a set of (multipartite) orthogonal product states $S$. Then one can show that there exists a local von Neumann measurement that is orthogonality preserving. The party associated with the color of the (over)complete bipartite graph does the measurement and splits the set of states $S$ minus one state $|\rho\rangle$ into the sets $S_1$ and $S_2$. Let $\pi$ be the projector associated with the set $S_1$ and $1 - \pi$ be the projector associated with the set $S_2$. The state $|\rho\rangle$ is projected onto $\pi |\rho\rangle$ and $(1 - \pi) |\rho\rangle$. However, $\pi |\rho\rangle$ is orthogonal to all the members of $S_1$ since the states in $S_1$ have support only on the subspace $\pi \mathcal{H}$, and also orthogonal to $S_2$ since they only have support on the subspace $(1 - \pi) \mathcal{H}$. The same argument holds for the state $(1 - \pi) |\rho\rangle$. Unfortunately, there are von Neumann measurements that are orthogonality preserving which are not expressible in terms of graph language only. With these tools, one can easily show that bipartite PBs of 2, 3 and 4 orthogonal product states in any dimension (consistent with the number of states) are always completable. One shows that these sets are locally distinguishable by considering their graphs, then one invokes Theorem 5 to conclude their completable.

![Figure 5.7: Examples of PBs, represented as two color graphs, that are distinguishable by LO+CC.](image)

### 5.4.9 Transfer of Indistinguishable Product States

Consider a set of bipartite orthogonal product states $S$ that are not exactly distinguishable by local operations and classical communication. Say Alice holds half of the unknown product state out of the ensemble $S$. She wants to send this state to Charlie by means of classical communication and local measurements in her lab. Let Bob, the holder of the other half, be fully cooperative in this scheme, and that he, as is Alice, is restricted to using local
measurements and classical communication. We will show that when the states in \( S \) cannot be locally distinguished, Alice will not be able to transfer her state exactly to Charlie. In a scenario where Alice and Bob share some classically correlated information, it is always possible for Alice to transmit this correlation to a third party, even when Alice and Bob are ignorant about the information that they share. In the quantum scenario we ask whether it is possible for Alice to transfer her half of an unknown product state which is correlated with Bob to a third party, possibly in a way that does not reveal to Alice which state she transferred. If Alice and Bob could measure what state they have, then it is clear that the information about the state can be transferred from Alice to Charlie. They convert their correlated quantum state to a piece of classical information. However, when Alice and Bob cannot tell with absolute certainty what state they have, even though it is a product state, it is not possible to transfer Alice’s part to Charlie. The reason is the following. If it could be achieved by means of classical communication and local measurements only, then all the classical information that Alice sends to Charlie might as well be sent to Bob. Thus if Charlie can reconstruct half of the state with this information, then so can Bob. Now Bob, possessing both parts of the product state, does a local projection measurement on the orthogonal states in \( S \). Since the states are orthogonal this measurement will uniquely determine which state in \( S \) he shared with Alice. This is in contradiction with the premise that the states in \( S \) are not exactly distinguishable by \( \text{LO+CC} \). What this construction illustrates is that even though no entanglement is involved, the quantum states that the two parties share exhibit some essential nonlocal quantum features.

5.4.10 The Use of Separable Superoperators

We have shown in the last sections that there exist sets of orthogonal product states that are not locally distinguishable. In this section we address the question of what kind of measurement does distinguish them. We are interested in finding measurements that need the least amount of resources in terms of entanglement between the two or more parties.

Let us introduce a class of quantum operations that are close relatives of operations that can be implemented by local quantum operations and classical communication, the separable superoperators and measurements:

**Definition 8** [133] Let \( \mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i \). Let \( \mathcal{H}' = \bigotimes_{i=1}^{n} \mathcal{H}'_i \). A TCP map \( S : B(\mathcal{H}) \to B(\mathcal{H}') \) is separable iff one can write the action of \( S \) on an arbitrary density matrix \( \rho \in B(\mathcal{H}) \) as

\[
S(\rho) = \sum_i A_{1,i} \otimes A_{2,i} \otimes \ldots \otimes A_{n,i} \rho A_{1,i}^\dagger \otimes A_{2,i}^\dagger \otimes \ldots \otimes A_{n,i}^\dagger,
\]

(5.4.39)

where \( A_{k,i} \) is a \( \dim \mathcal{H}_i' \times \dim \mathcal{H}_i \) matrix and

\[
\sum_i A_{1,i}^\dagger A_{1,i} \otimes A_{2,i}^\dagger A_{2,i} \otimes \ldots \otimes A_{n,i}^\dagger A_{n,i} = 1.
\]

(5.4.40)
Similarly, a quantum measurement (Chap. 3, sec. 3.2) on a multipartite Hilbert space is separable iff for each outcome \( m \), the operation elements \( A_i^m \) for all \( i \) are of a separable form:

\[
A_i^m = A_{1,i}^m \otimes A_{2,i}^m \otimes \ldots \otimes A_{n,i}^m.
\]  

(5.4.41)

The results of [125] show that separable superoperators are not equivalent to local quantum operations and classical communication. There is a separable measurement for the nine states of Eq. (5.4.1); it is the measurement whose operation elements are the projectors onto the nine states. The nine states are not locally distinguishable by LO+CC.

The following theorem gives a sufficient condition under which a bipartite set of orthogonal product states is distinguishable with the use of separable measurements. Unfortunately, it is not known what entanglement resources are needed to implement such separable measurements. They do however form a rather restricted class of operations. It is for example not possible to use them to create entanglement where previously none existed.

**Theorem 9** Let \( S \) be a set of bipartite orthogonal product states in \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \) with \( k \) members. If \( S \) has the property that it is completable in \( \mathcal{H} \) or local extensions of \( \mathcal{H} \) (\( \mathcal{H}_{\text{ext}} \)) when any single member is removed from \( S \), then the members of \( S \) are distinguishable by means of a separable measurement.

**Proof** Denote by \( \{ \pi_i \}_{i=1}^k \) the orthogonal rank 1 product projectors onto the states in \( S \). Let \( S_i \) be the set \( S \) without a state \( i \). As \( S_i \) is completable, the projectors

\[
\pi_{S_i^\perp} = 1 - \sum_{m \neq i} \pi_m,
\]  

(5.4.42)

for all \( i = 1, \ldots, k \), are separable. Note that \( \pi_{S_i^\perp} = \pi_{S_i^\perp}^\perp \). The projectors \( \pi_{S_i^\perp} \) and \( \pi_i \) for \( i = 1, \ldots, k \) with the right coefficients sum up to 1:

\[
\frac{1}{k} \sum_{i=1}^k \pi_{S_i^\perp}^\perp \pi_{S_i^\perp} + \frac{k-1}{k} \sum_{i=1}^k \pi_i^\perp \pi_i = 1,
\]  

(5.4.43)

using \( \pi^2 = \pi \) for projectors. As the projectors \( \pi_{S_i^\perp} \) are separable, one can decompose them into a set of \( N_i \) rank 1 product projectors, \( \pi_{(S_i^\perp,m_i)} \) labeled by an index \( m_i = 1, \ldots, N_i \). Note that one can choose mutually orthogonal projectors (for a given \( i \)) \( \pi_{(S_i^\perp,m_i)} \) when \( S_i \) is completable in the given Hilbert space \( \mathcal{H} \). When \( S_i \) is completable only in a local extension of \( \mathcal{H} \), these projectors will be non-orthogonal. In both cases the set of product projectors

\[
\left\{ \frac{1}{\sqrt{k}} \pi_{(S_i^\perp,m_i)}, \sqrt{\frac{k-1}{k}} \pi_i \right\}_{i=1,m_i=1}^{k,N_i},
\]  

(5.4.44)

are the operation elements of a separable measurement. This measurement projects onto states in \( S \) or onto separable states that are orthogonal to all but one state in \( S \). With a slight
modification of this measurement one can construct a measurement which distinguishes the states in S locally. Formally one replaces the projectors of Eq. (5.4.44) by

\[ \pi_i = |\alpha_i, \beta_i \rangle \langle \alpha_i, \beta_i | \rightarrow |i_A, i_B \rangle \langle \alpha_i, \beta_i |, \]

\[ \pi_{(S\pm, m)} = |\delta_{i, m_i}, \gamma_{i, m_i} \rangle \langle \delta_{i, m_i}, \gamma_{i, m_i} | \rightarrow |i', m_A, i', m_B \rangle \langle \delta_{i, m_i}, \gamma_{i, m_i} |, \] \tag{5.4.45}

such that the set of states \( |i_A, \rangle \), \( |i', m_A, \rangle \) is an orthonormal set and the same for B. This modification leaves Eq. (5.4.43) unchanged, so that this new set of operation elements again corresponds to a (separable) measurement. Upon this measurement, however, Alice and Bob both get a classical record of the outcome. If they perform this measurement on states in S, their outcomes will uniquely determine which state in S they were given. □

Both the Pent UPB as well as the Tiles UPB are examples of sets that are completable in 3 \( \otimes \) 3 when anyone state in the set is omitted. These sets are thus distinguishable by a separable measurement.

### 5.5 A Family of Indecomposable Positive Linear Maps

We introduce a new family of indecomposable positive linear maps based on entangled states. Central to our construction is the notion of an unextendible product basis. The construction lets us create and conjecture indecomposable positive linear maps in matrix algebras of arbitrary high dimension.

#### 5.5.1 Introduction

One of the central problems in the emergent field of quantum information theory [37] is the classification and characterization of the entanglement of quantum states. Entangled quantum states have been shown to be valuable resources in (quantum) communication and computation protocols. In this context it has been shown [112] that there exists a strong connection between the classification of the entanglement of quantum states and the structure of positive linear maps. Very little is known about the structure of positive linear maps even on low dimensional matrix algebras, in particular the structure of indecomposable positive linear maps. We denote the \( n \times n \) matrix algebra as \( M_n(\mathbb{C}) \). The first example of an indecomposable positive linear map in \( M_3(\mathbb{C}) \) was found by Choi [134]. There have been only a couple of other examples of indecomposable positive linear maps (see Ref. [135] for some recent literature); they seem to be hard to find and no general construction method is available. In this section we make use of the connection with quantum states to develop a method to create indecomposable positive linear maps on matrix algebras \( M_n(\mathbb{C}) \) for any \( n > 2 \). This construction exhibits some of the structure of positive linear maps which is present in almost any dimension. In section 5.5.2 we present the general construction. In section 5.5.3 we present two examples and discuss various open problems.
5.5.2 Unextendible Product Bases and Indecomposable Maps

The more complicated structure of the positive linear maps in higher dimensional matrix algebras, namely the existence of indecomposable positive maps (see the introductory section 5.2.3) is reflected in the existence of entangled density matrices $\rho$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ for which $(\text{id}_A \otimes T)(\rho)$ is positive semidefinite.

In Ref. [136] a method was discovered to construct entangled density matrices $\rho$ with positive semidefinite $(\text{id}_A \otimes T)(\rho)$ in various dimensions $\dim \mathcal{H}_A > 2$ and $\dim \mathcal{H}_B > 2$. The construction was based on the notion of an unextendible product basis.

We will present our results relating these density matrices obtained from the construction in Proposition 6 to indecomposable positive linear maps. We will need the definition of a maximally entangled pure state:

**Definition 9** Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Let $|\psi\rangle$ be a normalized state $(\langle \psi | \psi \rangle = 1)$ in $\mathcal{H}$ and

$$\rho_{A,\psi} = \text{Tr}_B |\psi\rangle \langle \psi|,$$  \hspace{1cm} (5.5.1)

where $\text{Tr}_B$ indicates that the trace is taken with respect to Hilbert space $\mathcal{H}_B$ only. The state $|\psi\rangle \in \mathcal{H}$ is maximally entangled if

$$S(\rho_{A,\psi}) = -\text{Tr} \rho_{A,\psi} \log_2 \rho_{A,\psi} = \log_2 \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B)$$ \hspace{1cm} (5.5.2)

The function $S(\rho_{A,\psi})$ is the von Neumann entropy of the density matrix $\rho_{A,\psi}$.

**Remarks** For pure states $|\psi\rangle$ the von Neumann entropy of $\rho_{A,\psi}$ is always less than or equal to $d \equiv \log_2 \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B)$. For maximally entangled states we will have $\rho_{A,\psi} = \text{diag}(1/d, \ldots, 1/d, 0, \ldots, 0)$ so that the maximum von Neumann entropy, Eq. (5.5.2), is achieved. When $\dim \mathcal{H}_A = \dim \mathcal{H}_B$ one can always make an orthonormal basis for $\mathcal{H}$ with maximally entangled states [137]. For pure states $|\psi\rangle$ we always have $S(\rho_{A,\psi}) = S(\rho_{B,\psi})$.

The following lemma bounds the innerproduct between a maximally entangled state and any product state.

**Lemma 7** Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Let $|\Phi\rangle \in \mathcal{H}$ be a maximally entangled state. Let $d = \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B)$. For all product states $|\phi_A\rangle \otimes |\phi_B\rangle$ of norm 1 we have

$$|\langle \Phi | \phi_A \rangle \otimes \langle \phi_B |\rangle|^2 \leq \frac{1}{d},$$ \hspace{1cm} (5.5.3)

**Proof** We write the maximally entangled state $|\Phi\rangle$ in the Schmidt polar form [138] as

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |a_i\rangle \otimes |b_i\rangle,$$  \hspace{1cm} (5.5.4)
where \( \langle a_i | a_j \rangle = \delta_{ij} \) and \( \langle b_i | b_j \rangle = \delta_{ij} \). Thus we can write
\[
|\langle \Phi | \phi_A \rangle \otimes | \phi_B \rangle \rangle^2 = \frac{1}{d} \sum_{i=1}^{d} |\langle \phi_A | a_i \rangle |^2 |\langle \phi_B | b_i \rangle |^2 \leq \frac{1}{d},
\]
(5.5.5)

using the Schwarz inequality and \( \sum_{i=1}^{d} |\langle \phi_A | a_i \rangle |^2 \leq 1 \) and \( \sum_{i=1}^{d} |\langle \phi_B | b_i \rangle |^2 \leq 1 \). □

We will also need the following lemma:

**Lemma 8** Let \( S \) be an unextendible product basis \( \{|\alpha_i \rangle \otimes | \beta_i \rangle \}_{i=1}^{\lvert S \rvert} \) in \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \). Let
\[
f(\langle \phi_A \rangle, | \phi_B \rangle \rangle) = \sum_{i=1}^{\lvert S \rvert} |\langle \phi_A | a_i \rangle |^2 |\langle \phi_B | \beta_i \rangle |^2.
\]
(5.5.6)
The minimum of \( f \) over all pure states \( | \phi_A \rangle \in \mathcal{H}_A \) and \( | \phi_B \rangle \in \mathcal{H}_B \) exists and is strictly larger than 0.

**Proof** The set of all pure product states \( | \phi_A \rangle \otimes | \phi_B \rangle \rangle \) on \( \mathcal{H} \) is a compact set. The function \( f \) is a continuous function on this set. Therefore, if there exists a set of states \( | \phi_A \rangle \otimes | \phi_B \rangle \rangle \) for which \( f \) is arbitrarily small then there would also exist a pair \( | \phi'_A \rangle \otimes | \phi'_B \rangle \rangle \) for which \( f = 0 \). This contradicts the fact that \( S \) is an unextendible product basis. □

The following two theorems contain the main result of this section.

**Theorem 10** Let \( S \) be an unextendible product basis \( \{|\alpha_i \rangle \otimes | \beta_i \rangle \}_{i=1}^{\lvert S \rvert} \) in \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \). Let \( \rho \) be the density matrix
\[
\rho = \frac{1}{\dim \mathcal{H} - \lvert S \rvert} \left( I_{AB} - \sum_{i=1}^{\lvert S \rvert} |\langle \alpha_i \rangle |^2 |\langle \beta_i \rangle | \otimes |\langle \beta_i \rangle | \right),
\]
(5.5.7)

Let \( d = \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B) \). Let \( | \Phi \rangle \rangle \) be a maximally entangled state on \( d \otimes d \) such that
\[
| \langle \Phi | \rho | \Phi \rangle \rangle > 0,
\]
(5.5.8)

and
\[
\epsilon = \min_{| \phi_A \rangle \otimes | \phi_B \rangle \rangle} \sum_{i=1}^{\lvert S \rvert} |\langle \phi_A | a_i \rangle |^2 |\langle \phi_B | \beta_i \rangle |^2,
\]
(5.5.9)

where the minimum is taken over all pure states \( | \phi_A \rangle \in \mathcal{H}_A \) and \( | \phi_B \rangle \in \mathcal{H}_B \). Let \( \Pi \) be a Hermitian operator given by
\[
\Pi = \sum_{i=1}^{\lvert S \rvert} |\langle \alpha_i | \otimes | \beta_i \rangle | \langle \beta_i | \rangle = d| \langle \Phi \rangle \rangle | \langle \Phi \rangle |.
\]

(5.5.10)

For every unextendible product basis \( S \) there is a maximally entangled state \( | \Phi \rangle \rangle \) such that Eq. (5.5.8) holds. Moreover \( \Pi \) has the following properties:
\[
\text{Tr} \Pi \rho < 0,
\]
(5.5.11)
and for all product states $|\phi_A\rangle \otimes |\phi_B\rangle \in \mathcal{H}$,

$$\text{Tr} H |\phi_A\rangle \langle \phi_A| \otimes |\phi_B\rangle \langle \phi_B| \geq 0. \quad (5.5.12)$$

**Proof** Eq. (5.5.12) follows from the definition of $\varepsilon$, Eq. (5.5.9), and Lemma 7. Consider Eq. (5.5.11). Since the density matrix $\rho$ is proportional to the projector on $\mathcal{H}_A^\perp$, one has

$$\text{Tr} \rho = -d \varepsilon \langle \Phi | \rho | \Phi \rangle, \quad (5.5.13)$$

which is strictly smaller than zero by Lemma 8 and the choice of the maximally entangled state, Eq. (5.5.8). When $\dim \mathcal{H}_A = \dim \mathcal{H}_B$ there exists a basis of maximally entangled states and thus there will be a basis vector $|\Phi\rangle$ for which $\langle \Phi | \rho | \Phi \rangle$ is nonzero. In case, say, $\dim \mathcal{H}_A > \dim \mathcal{H}_B = d$, there exists a basis of maximally entangled states for every subspace $\mathcal{H}' = \mathcal{H}_A \otimes \mathcal{H}_B$ with $\mathcal{H}' \subset \mathcal{H}_A$ and $\dim \mathcal{H}' = d$. Therefore there will be a maximally entangled state $|\Phi\rangle$ such that $\langle \Phi | \rho | \Phi \rangle$ is nonzero. This completes the proof. □

**Remark** Note that $H$ is the entanglement witness that was introduced in Lemma 3, section 5.3.

**Theorem 11** Let $S$ be an unextendible product basis $\{|\alpha_i\rangle \otimes |\beta_i\rangle\}_{i=1}^{|S|}$ in $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Let $H$ be defined as in Theorem 10, Eq. (5.5.10). Choose an orthonormal basis $\{|i\rangle\}_{i=1}^{\dim \mathcal{H}_A}$ for $\mathcal{H}_A$. Let $S: B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ be a linear map defined by

$$S(|i\rangle \langle j|) = \langle i| H |j\rangle. \quad (5.5.14)$$

Then $S$ is positive but not completely positive. Moreover, $S$ is indecomposable.

**Proof** The relation between $S$ and $H$, Eq. (5.5.14), follows from the isomorphism between Hermitian operators on $\mathcal{H}_A \otimes \mathcal{H}_B$ with the property of Eq. (5.5.12) and linear positive maps, see Refs. [112, 139]. In particular, iff a Hermitian $H$ operator on $\mathcal{H}_A \otimes \mathcal{H}_B$ has the property of Eq. (5.5.12) then the linear map $R: B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ defined by

$$H = \sum_{i,j} \langle i| \langle j| \otimes R(|i\rangle \langle j|), \quad (5.5.15)$$

is positive for any choice of the orthonormal basis $\{|i\rangle\}_{i=1}^{\dim \mathcal{H}_A}$. The map $S = R \circ T$, where $T$ is matrix transposition in the basis $\{|i\rangle\}_{i=1}^{\dim \mathcal{H}_A}$, in Eq. (5.5.14) is then positive as well.

Using the density matrix $\rho$ that is derived from the unextendible product basis, Eq. (5.5.7), we will show that $S$ is not completely positive. At the same time we will prove that the assumption that $S$ is decomposable leads to a contradiction. We can rewrite Eq. (5.5.14) as

$$H = (\text{id}_A \otimes S)(|\Phi^+\rangle \langle \Phi^+|), \quad (5.5.16)$$

where $|\Phi^+\rangle = \sum_i |\alpha_i\rangle |\beta_i\rangle$.

$$\text{Tr} H |\phi_A\rangle \langle \phi_A| \otimes |\phi_B\rangle \langle \phi_B| \geq 0. \quad (5.5.17)$$

This completes the proof. □
where \( |\Phi^+\rangle \) is equal to the (unnormalized) maximally entangled state \( \sum_{i=1}^{\dim \mathcal{H}_A} |i\rangle \otimes |i\rangle \). Let \( S^\dagger: B(\mathcal{H}_B) \to B(\mathcal{H}_A) \) be the Hermitian conjugate of the map \( S \). We use the definition of \( S^\dagger \)

\[
\text{Tr} \ S^\dagger (A^\dagger) B = \text{Tr} A^\dagger S(B),
\]

and Eq. (5.5.16) to derive that Eq. (5.5.11) can be rewritten as

\[
\text{Tr} \ H \rho = \langle \Phi^+ | (\text{id}_A \otimes S^\dagger) (\rho) | \Phi^+ \rangle < 0. \tag{5.5.18}
\]

Thus \( S^\dagger \) cannot be completely positive and therefore \( S \) itself is not completely positive. If \( S \) were decomposable, then \( S^\dagger \) would be of the form \( S_1 + T \circ S_2 \) where \( S_1 \) and \( S_2 \) are completely positive maps. The density matrix \( \rho \) is positive semidefinite under any positive linear map of the form \( S_1 + T \circ S_2 \) by Proposition 6. This is in contradiction with Eq. (5.5.18) and therefore \( S \) cannot be decomposable. \( \Box \)

### 5.5.3 Examples and Discussion

As we have shown the structure of unextendible product bases carries over to indecomposable positive linear maps. The results on unextendible product bases that we presented in sections 5.4.2-5.4.3 give us many examples of these indecomposable positive linear maps. In this section we will take two examples of unextendible product bases and demonstrate the construction of Theorem 10 and Theorem 11.

**Example 1:** Consider the Pent UPB, Eq. (5.4.3). Let \( \rho_{\text{Pent}} \) be the bound entangled state derived from Pent as in Eq. (5.4.6), Proposition 6. We choose a maximally entangled state \( |\Phi\rangle \), here named \( |\Phi^+\rangle \),

\[
|\Phi^+\rangle = \frac{1}{\sqrt{3}} (|11\rangle + |22\rangle + |33\rangle). \tag{5.5.19}
\]

One can easily compute that

\[
\langle \Phi^+ | \rho_{\text{Pent}} | \Phi^+ \rangle = \frac{1}{4} \left( 1 - \frac{7 + \sqrt{5}}{3 + \sqrt{5}} \right) > 0. \tag{5.5.20}
\]

The map \( S \) as defined in Eq. (5.5.14) Theorem 11, follows directly:

\[
S(|i\rangle \langle j|) = \sum_{k=0}^4 |i\rangle \langle v_k| \langle v_k | \langle j| \langle v_{2k \mod 5}| - \epsilon |i\rangle \langle j| . \tag{5.5.21}
\]

A positive linear map \( S: B(\mathcal{H}_n) \to B(\mathcal{H}_m) \) is called unital if \( S(1_n) = 1_m \). We will demonstrate that \( S \) is not unital. One can write

\[
S(1_A) = \text{Tr}_A \ H = \sum_{k=0}^4 |v_{2k \mod 5}| \langle v_{2k \mod 5}| - 3 \epsilon \text{ Tr}_A |\Phi^+\rangle \langle \Phi^+| . \tag{5.5.22}
\]
5.5 A Family of Indecomposable Positive Linear Maps

which in turn is equal to

$$S(1_A) = \text{diag} \left( \frac{10}{5 + \sqrt{5}}, \frac{10}{5 + \sqrt{5}}, \sqrt{5} \right) - \epsilon 1_B. \quad (5.5.23)$$

A numerical approximation of $\epsilon$ as defined in Eq. (5.5.9) Theorem 10, gives the value

$$\epsilon \approx 0.037911, \quad (5.5.24)$$

but we don’t know whether this is the minimum of the function in Eq. (5.5.9).

The next example is based on a more general unextendible product bases that was presented in Ref. [129].

**Example 2:** The states of $S$, $\text{Tiles3n}$ in $\mathcal{H}_3 \otimes \mathcal{H}_n$ are

$$|F_{k}^0\rangle = \frac{1}{\sqrt{n-2}} |0\rangle \otimes (|1\rangle + \sum_{l=3}^{n-1} \omega^{k(l-2)} |l\rangle), \quad 1 \leq k \leq n-3, \quad (5.5.25)$$

$$|F_{k}^1\rangle = \frac{1}{\sqrt{n-2}} |1\rangle \otimes (|2\rangle + \sum_{l=3}^{n-1} \omega^{k(l-2)} |l\rangle), \quad 1 \leq k \leq n-3, \quad (5.5.26)$$

$$|F_{k}^2\rangle = \frac{1}{\sqrt{n-2}} |2\rangle \otimes (|0\rangle + \sum_{l=3}^{n-1} \omega^{k(l-2)} |l\rangle), \quad 1 \leq k \leq n-3, \quad (5.5.27)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes |0\rangle, \quad (5.5.28)$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}} (|1\rangle - |2\rangle) \otimes |1\rangle, \quad (5.5.29)$$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}} (|2\rangle - |0\rangle) \otimes |2\rangle, \quad (5.5.30)$$

$$|\psi_6\rangle = \frac{1}{\sqrt{3n}} \sum_{i=0}^{2} \sum_{j=0}^{n-1} |i\rangle \otimes |j\rangle, \quad (5.5.31)$$

and we have $\omega = \exp(2\pi i/(n-2))$. Here the states $\{|k\rangle\}_{k=0}^{n-1}$ form an orthonormal basis. In total there are $3n-5$ states in the basis. We choose a maximally entangled state, again we take $|\Phi^+\rangle$, Eq. (5.5.19). One can show that

$$\langle \Phi^+ | \rho_{\text{Tiles3n}} | \Phi^+ \rangle = \frac{1}{5} \left( \frac{1}{2} - \frac{1}{3n} \right) > 0. \quad (5.5.32)$$

The map $S: B(\mathcal{H}_3) \rightarrow B(\mathcal{H}_n)$ is given as

$$S(|i\rangle\langle j|) = \sum_{k=1}^{n-3} \sum_{p=0}^{2} (i |F_{k}^p\rangle \langle F_{k}^p| j|) + \sum_{p=3}^{6} \langle i |\psi_p\rangle \langle \psi_p| j| - \epsilon |i\rangle\langle j|. \quad (5.5.33)$$

The following questions concerning the positive linear maps that were introduced in this paper are left open.
1. Is $S$ always non unital? We conjecture it is. As we showed, see Eq. (5.5.22), the answer to this question depends on whether
\[ \sum_{i=1}^{\|S\|} |\beta_i\rangle\langle\beta_i| = c1_B, \] (5.5.34)
where the set of states $\{|\beta_i\rangle\}_{i=1}^{\|S\|}$ are one side of the unextendible product basis and $c$ is some constant. The states $|\beta_i\rangle$ will span $\mathcal{H}_B$ but they will not be all orthogonal, nor all non-orthogonal.

2. It was shown in Theorem 11 that the new indecomposable positive linear maps $S: \mathcal{B}(\mathcal{H}_m) \rightarrow \mathcal{B}(\mathcal{H}_n)$ are not $m$-positive, as they are not completely positive. Are these maps $S$ $k$-positive for some $k$ with $1 < k < m$? The answer to this question will require a better understanding of the structure of unextendible product bases.

3. In Ref. [136] (see section 5.4.6) a single example was given of an entangled density matrix on $\mathcal{H}_3 \otimes \mathcal{H}_4$ which was positive semidefinite under the map $\text{id}_3 \otimes T$. The density matrix was based not on an unextendible product basis, but a 'barely' completable product basis $S$. We did show that the Hilbert space $\mathcal{H}_S^\perp$ had a product state deficit, i.e. the number of product states in $\mathcal{H}_S^\perp$ was less than $\dim \mathcal{H}_S^\perp$. It is open question how to generalize this example and whether these kinds of density matrices will give rise to more general family of indecomposable positive linear maps.

5.6 Discussion

Both the bound entangled states and the unextendible product bases from which we derived the bound entangled states exhibit a form of local irreversibility. A bound entangled state can be viewed as the result of a local entropy-increasing process on a pure entangled state. It is the nature of a bound entangled state that this process cannot be reversed locally; we cannot distill pure entanglement out of a bound entangled state. The states in an unextendible product basis are states that can be prepared locally. The uniform ensemble of the UPB states can be viewed as the result of an entropy-increasing process in which the local preparers forget which state was prepared. We have shown that this process cannot be reversed locally, as the preparers are not able to confidently distinguish the members of the ensemble.

The question what minimal nonlocal means are needed to undo both kinds of processes is not answered by this work. Another question that is related to this work, is the question of the use of bound entangled states. Bound entangled states are not helpful in the transmission of quantum data via a teleportation protocol; it has been shown [140] that any (attempt at) teleportation that is done with the use of bound entangled states can also be done without the use of entanglement. It is possible that bound entangled states are instrumental in the implementation of separable superoperators and measurements.