

Characteristics of Unextendible Product Bases

Thomas B. Pedersen

May 16, 2002

Preface

Unextendible Product Bases have close relations to entanglement and indistinguishability, two phenomena unique to quantum mechanics. As entanglement is a central resource in quantum-algorithms and quantum-communication, the hope is that UPBs can lead to important results in understanding entanglement. Indistinguishability is a rather new concept which seems promising. In this thesis we focus on UPBs themselves and reveal some of their structures and their relations to entanglement and indistinguishability.

Acknowledgements

I would like to express my gratitude to Jan Neerbek for good discussions and comments. I also thank Barbara Terhal and David DiVincenzo for suggestions for subjects and for comments on my work, and to David for letting me use some of the figures from their paper. Thanks to Mikkel Bjerg, Rasmus Haubro Rohde, and Ole Friis Østergaard for help on L^AT_EX and suggestions on wording, and Thomas Ljungberg and Erik Olsen for corrections. Louis Salvail has been a helpful source of technical support. I am grateful to Ivan Damgård for being my supervisor. Finally I wish to thank my external supervisor Peter Høyer for giving the best support anyone could wish for.

I also want to thank the QAIP research programme for financial support to my participation in the QIP2001 workshop, and BRICS and QAIP for financial support to my participation in the ESF Euresco Conference on Quantum Information.

Contents

Preface	iii
Acknowledgements	v
1 Introduction	1
1.1 A Short History of Quantum Computing	1
1.2 Structure of this Thesis	2
2 Basic Definitions	5
2.1 Quantum State	5
2.2 Entanglement	7
2.3 Dynamics	8
2.4 Measurement	9
3 Local Operations and Classical Communication	13
3.1 LOCC Protocols	13
3.2 Bound Entanglement	14
3.3 Distinguishability	16
4 Product Bases	19
4.1 PB and UPB	19
4.2 UPBs and Bound Entanglement	20
4.3 Uncompletable Product Bases	21
5 Relations to Graph Theory	25
5.1 The Counting Lemma	25
5.2 Orthogonality Graphs	26
5.3 Dependency Graphs	35
5.4 Symmetric UPBs and Alternating UPBs	37
6 Bounds on Cardinality	41
6.1 Lower Bounds	41
6.2 A Lower Bound UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$	44
6.3 Graph Characterisation of Minimal UPBs	47

6.4	Upper Bounds	47
7	Generic UPBs	49
7.1	GenShifts	49
7.2	GenTiles1	52
7.3	GenTiles2	56
7.4	GenPyramid	59
7.5	QuadRes	64
8	Morphologic UPBs	69
8.1	Constructing a Morphologic UPB	69
8.2	Graph Equivalence of UPBs	73
9	Concluding Comments	77
9.1	Achievements	77
9.2	Open Questions	77
A	Legend	79
B	List of UPBs	81
C	Dependencies of Results	83
	Bibliography	85

List of Figures

4.1	The hierachy of the different classes of product bases	23
5.1	Orthogonality graph for the Tiles UPB	27
5.2	One step in a LOCC protocol, as viewed by Alice.	34
5.3	If we only know the orthogonality graph, we risk loosing the orthogonality information about two projected states after a measurement.	35
6.1	Lower bounds for complex vector spaces of dimension at most 35. Vector spaces not listed here has no UPBs.	45
6.2	Orthogonality graph for the Min4x4 UPB	46
7.1	Parameters for the GenShifts UPB	50
7.2	The tiles representation of the four first states of Tiles [DMS ⁺ 99]. This figure is printed with permission from David DiVincenzo.	53
7.3	The tiles representation of GenTiles1 for $\mathbb{C}^6 \otimes \mathbb{C}^6$ [DMS ⁺ 99]. This figure is printed with permission from David DiVincenzo.	54
7.4	Parameters for the GenTiles1 UPB	54
7.5	The tiles representation of GenTiles2 for $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, leaving out the <i>stopper</i> state [DMS ⁺ 99]. This figure is printed with permission from David DiVincenzo.	56
7.6	Parameters for the GenTiles2 UPB	57
7.7	Parameters for the GenPyramid UPB	60
7.8	Parameters for the QuadRes UPB	65
8.1	Orthogonality graph for the Tiles and Pyramid UPBs.	70
8.2	The orthogonality graphs of two nonequivalent symmetric UPBs in $\mathbb{C}^4 \otimes \mathbb{C}^5$	75
B.1	All generic and specific UPBs in this Thesis	81
C.1	All results in this thesis, and their dependencies.	83

Chapter 1

Introduction

1.1 A Short History of Quantum Computing

A central concept in computer science is the notion of computational complexity. In the nineteen-twenties Alan Turing introduced the Turing machine formalism, and conjectured that all problems which can be solved by *some algorithm* can be solved with no more than a polynomial penalty on a Turing machine. This conjecture is referred to as the Church-Turing thesis. With the advent of randomised algorithms in the seventies the Church-Turing thesis met its first challenge: Are randomised algorithms stronger than deterministic algorithms?

While Turings notion of *algorithm* is founded on rather philosophical considerations David Deutsch introduced the notion of the universal quantum computer in 1985, to make a “...physically more reasonable definition of complexity...” [Deu85]. The quantum computer presented yet another challenge to the Church-Turing thesis. In 1994 Peter Shor constructed a quantum algorithm for factorisation which has polynomial complexity. In the Turing machine formalism it is unknown whether factoring is of polynomial complexity. In 1995 Lov Grover constructed a quantum algorithm which can find elements in an unsorted list which has squared improvement over the best known algorithm on a Turing machine.

While it is still an open question whether the Universal Quantum Machine is stronger than the universal turing machine significant results has been obtained in the area of quantum communication. In 1984 Charles Bennett and Gilles Brassard presented the BB84 quantum key distribution protocol, which offers security based on the physical properties of the communication. In 1993 Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters presented quantum teleportation, where the quantum state of a physical system can be transferred by a classical communication channel. In 1996 Robert Calderbank and Peter Shor, and Andrew Steane presented the CSS quantum error-correcting codes which can correct for certain errors occurring in quantum communication channels.

Most of the quantum algorithms and communication protocols mentioned above get their power from a quantum mechanical phenomenon, namely entanglement. Entanglement is a correlation between the quantum states of physical systems which arises from the quantum mechanical formalism. Entanglement violates at least one of two fundamental assumptions of classical physics: Realism and locality. Realism refers to the assumption that any physical object has properties with definite values which can be observed. Locality refers to the assumption that the outcome of simultaneous measurements on two distinct physical objects does not interfere with each other.

Entanglement was first discovered by Einstein, Podolsky, and Rosen in 1935 [EPR35]. In 1994 Popescu and Vaidman discovered indistinguishability, another quantum mechanical phenomenon which violates either realism, locality or both [BDF⁺98]. In classical physics it is always possible to know the collective state of a collection of physical objects by deciding the states of the individual objects. With indistinguishable quantum states no measurement on the individual objects can reveal the collective state, though a measurement on the whole collection can.

Unextendible product bases (UPBs) were first presented by Bennett, DiVincenzo, Mor, Shor, Smolin, and Terhal [BDM⁺98]. For a vector space which is given as a direct product of complex vector spaces, a UPB is a basis of some proper subspace of that vector space. Each vector of the UPB has to be a direct product of vectors from the individual complex vector spaces. In quantum mechanics a UPB is interpreted as a collection of quantum states. A primary motivation for the study of UPBs are their relationships to entanglement and indistinguishability.

1.2 Structure of this Thesis

This thesis is centred around the articles “Unextendible Product Bases and Bound Entanglement” [BDM⁺98], and “Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement” by DiVincenzo, Mor, Shor, Smolin, and Terhal [DMS⁺99].

In Chapter 2 we introduce the quantum mechanical model used in this thesis. We define the mathematical objects used to represent the state of a quantum system. We see how a quantum state can change in time, and how we can decide the state of a quantum system. We also see the mathematical definition of entanglement.

In Chapter 3 we present the formalism of local operations and classical communication which is a class of communication protocols important to indistinguishability and the creation of entanglement.

In Chapter 4 we define product bases. A subset of the product bases are the UPBs. We also present other product bases, namely uncompletable product bases and strongly uncompletable product bases, and we investigate how these

sets relate to one another. We also present the two important theorems relating UPBs to entanglement and indistinguishability.

In Chapter 5 we introduce a graph representation of UPBs, orthogonality graphs. We demonstrate how orthogonality graphs can be used to find an explicit way to distinguish the states of a product basis. This we use to show that, in certain complex vector spaces, no UPBs exists. We then discuss how well orthogonality graphs represents protocols used for distinguishing states. We present the Counting Lemma, which is a useful lemma stating a necessary and sufficient criterion for a product basis to be a UPB. We also introduce another graph representation of UPBs, dependency graphs. Dependency graphs are only used little in this thesis as most results obtained from dependency graphs can be translated into slightly weaker, but sufficient, results about orthogonality graphs. One theorem using dependency graphs is, however, not translated into a theorem about orthogonality graphs. This theorem guarantees the existence of UPB in some vector spaces. Motivated by some characteristics of the UPBs guaranteed to exist by this theorem the author has divided the UPBs into two classes: Symmetric and alternating.

In Chapter 6 we study the lower and upper bounds on the possible number of vectors in a UPB. First we give an example of a vector space where no UPB exists. Then we present the Simple Lower Bound first proven in [BDM⁺98]. This bound is, however, not a tight bound, but we shall study a criterion, the Alon-Lovász Criterion, which tells us when the bound is tight. The original proof of the Alon-Lovász Criterion is rather cumbersome so we split it up into two smaller lemmas which are more intuitive. The first of these lemmas states that no alternating UPB can reach the Simple Lower Bound. The other lemma states that all UPBs which conforms to the Alon-Lovász Criterion are symmetric. To further classify UPBs achieving the Simple Lower Bound we prove that all symmetric UPBs conform to the Alon-Lovász Criterion, and thus achieve the Simple Lower Bound. After the study of lower bounds, we present a UPB which is minimal in a vector space where the Alon-Lovász Criterion states that the Simple Lower Bound is not tight. Finally we present an upper bound based on a limitation on the entanglement related to UPBs.

In Chapter 7 we study a family of UPBs which the author has denoted generic UPBs. Generic UPBs are parameterised UPBs, or more formally functions from some parameter space which map to UPBs of different vector spaces. This gives us an arsenal of UPBs and improve our intuition on UPBs.

In Chapter 8 we study another family of UPBs which the author has denoted morphologic UPBs. A morphologic UPB is a function which map from some parameter space to all possible UPBs which has the same orthogonality graph representation. These UPBs all live in the same vector space. We first see how we can construct morphologic UPBs. We then define an equivalence relation of UPBs where UPBs with the similar orthogonality graphs are equivalent. Equivalent UPBs correspond to particular instances of the same morphologic UPB.

Chapter 2

Basic Definitions

2.1 Quantum State

Definition 2.1.1 (Quantum state) [Pre98] *Let \mathcal{H} be a complex vector space of finite dimension with an inner product $\langle\psi|\phi\rangle$. Then any vector $\psi \in \mathcal{H}$ of unit norm is a quantum state.*

A quantum state ψ is written as $|\psi\rangle$ (pronounced “ket ψ ”). In this definition of a quantum state we require that a quantum state is a vector of unit norm in a complex vector space. This is a simplification of the quantum model, where any vector from a Hilbert space represents a quantum state. A Hilbert space is a, possibly infinite dimensional, complex vector space with an inner product which is complete in the norm. In this thesis, though, only finite dimensional vector spaces are used. As we shall see in Chapter 2.4, an implication of the definition of measurements is that we cannot tell the difference between states $|\psi\rangle$ and $e^{i\alpha}|\psi\rangle$ with physical experiments. This means that states that differs by a global scalar factor, called a phase factor, are identical.

Then how is the physical interpretation of this definition? Imagine that you have a physical object (an electron, for example) that can be in one of d discrete states (ground state, 1. excited state, etc.). Then the possible states of the object is described by the d -dimensional complex vector space \mathbb{C}^d . One *usually* chooses the standard basis ($\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$) for the complex vector space to be these discrete states. A particular object $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \dots + \alpha_{d-1}|d-1\rangle$ in this complex vector space is interpreted as being partly in the state $|0\rangle$, partly in state $|1\rangle$, and so forth, where the amplitudes $\alpha_1, \dots, \alpha_{d-1}$ describes *how much* the object is in each of the basis states respectively. We return to the notion of “*how much*” shortly. An object which is a linear combination of several basic states at the same time is said to be in a *superposition* of these states.

In quantum computing the smallest units are objects with two discrete states, as one such object resembles a classical bit. A state from a 2-dimensional complex

vector space is thus called a *qubit* (quantum-bit). When talking about qubits we denote the two basis vectors as $|0\rangle$ and $|1\rangle$.

The complex conjugate, $|\psi\rangle^\dagger$, of a quantum state $|\psi\rangle$ is also written $\langle\psi|$, and so we have the *outer product* $|\psi\rangle\langle\phi|$. Notice that in the case where $|\psi\rangle = |\phi\rangle$ the outer product is the projection matrix for the vector $|\psi\rangle$ [Bea95].

We are often observing or working with several objects at the same time. We then have the possibility of describing the collective state of these objects. The state of the collection is then a vector in a larger complex vector space.

As an example imagine you have 2 qubits (vectors from two-dimensional complex vector spaces). The two qubits can be joined in one of 4 states: $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, where $|ab\rangle$ represents the state where the first qubit is $|a\rangle$ and the second qubit is $|b\rangle$. So when joining a state from a d_1 -dimensional complex vector space with a state from a d_2 -dimensional complex vector space we obtain a state from a d_1d_2 -dimensional complex vector space. Here it is important to notice that we multiply the dimensions. The joining operation is called the *tensor product*, and is defined as follows.

Definition 2.1.2 (Tensor product) [Bra00] *Let A be an $m \times n$ matrix with entries a_{ij} and let B be a $q \times p$ matrix. The tensor product of A and B is the $mq \times np$ matrix*

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}. \quad (2.1)$$

A d -dimensional vector is treated as $d \times 1$ matrix.

Those familiar with the *Kronecker product* might have noticed that the tensor product and the Kronecker product are the same.

Let us see this definition expressed in the quantum model.

Definition 2.1.3 (Tensor product of quantum states) [Bra00] *Let \mathbb{C}^{d_1} , \mathbb{C}^{d_2} be complex vector spaces of dimensions d_1 and d_2 , respectively. Let $(|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_{d_1}\rangle)$ be an ordered basis for \mathbb{C}^{d_1} , and $(|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_{d_2}\rangle)$ be an ordered basis for \mathbb{C}^{d_2} . Let $|\psi\rangle = \sum_{i=1}^{d_1} a_i |\alpha_i\rangle \in \mathbb{C}^{d_1}$ and $|\phi\rangle = \sum_{i=1}^{d_2} b_i |\beta_i\rangle \in \mathbb{C}^{d_2}$. The tensor product of $|\psi\rangle$ and $|\phi\rangle$ is*

$$|\psi\rangle \otimes |\phi\rangle = \sum_{i=1}^{d_1} \sum_{j=1}^{d_2} a_i b_j |\alpha_i \beta_j\rangle, \quad (2.2)$$

where $|\alpha_i \beta_j\rangle$ denotes the basis vector $|\alpha_i\rangle \otimes |\beta_j\rangle$ of the d_1d_2 -dimensional complex vector space $\mathbb{C}^{d_1d_2}$.

The tensor product is associative but *not* commutative. We now state some useful properties of the tensor product and the inner product.

Proposition 2.1.4 *Let $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle \in \mathbb{C}^{d_1}$ and $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{C}^{d_2}$ be quantum states, and let $\alpha \in \mathbb{C}$ be a complex scalar. Then the following holds*

$$\langle \psi_1 | (|\psi_2\rangle + |\psi_3\rangle) = \langle \psi_1 | \psi_2\rangle + \langle \psi_1 | \psi_3\rangle, \quad (2.3)$$

$$\begin{aligned} (|\psi_1\rangle \otimes |\phi_1\rangle)^\dagger (|\psi_2\rangle \otimes |\phi_2\rangle) &= (\langle \psi_1 | \otimes \langle \phi_1 |) (|\psi_2\rangle \otimes |\phi_2\rangle) \\ &= \langle \psi_1 | \psi_2\rangle \langle \phi_1 | \phi_2\rangle, \end{aligned} \quad (2.4)$$

$$\alpha (|\psi_1\rangle \otimes |\phi_1\rangle) = \alpha |\psi_1\rangle \otimes |\phi_1\rangle \quad (2.5)$$

$$= |\psi_1\rangle \otimes \alpha |\phi_1\rangle. \quad (2.6)$$

Let us introduce some notation that we will frequently use throughout this thesis. Let $S = \{|\psi_1\rangle, |\psi_2\rangle, \dots\}$ be a set of vectors from some vector space \mathbb{C}^d , then we denote the subspace spanned by S as $\mathbb{C}_S^d \subseteq \mathbb{C}^d$. We use $\mathbb{C}_S^{d\perp}$ to denote the orthogonal complement of \mathbb{C}_S^d in \mathbb{C}^d .

2.2 Entanglement

One of the concepts that makes quantum-mechanics and quantum-computing interesting, is the notion of *entanglement*. When you have a given multiparticle quantum state $|\psi\rangle$ it is not always possible to write the state as a tensor product of the states of the individual particles. Consider the state

$$|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (2.7)$$

The state $|\text{EPR}\rangle$ cannot be written as a tensor product of the form $(\alpha_1|0\rangle + \alpha_2|1\rangle) \otimes (\beta_1|0\rangle + \beta_2|1\rangle)$ in any manner. This state is named after Einstein, Podolsky, and Rosen that used this state in their famous EPR paradox [EPR35] when they thought to have proven the incompleteness of the quantum theory. But the properties of the $|\text{EPR}\rangle$ pair they saw as a paradox, gives rise to some of the central methods in modern quantum computing [RP98].

Definition 2.2.1 (Multipartite vector space) *Let \mathbb{C}^d be a vector space that can be expressed as a tensor product of m other vector spaces $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$. Then $\{\mathbb{C}^{d_1}, \dots, \mathbb{C}^{d_m}\}$ is a partition of the m -partite vector space \mathbb{C}^d between m parties.*

When talking about a multipartite vector space, it is important to specify the desired partition of the vector space, as several partitions might be possible. Consider for instance these possible partitions of \mathbb{C}^8 .

$$\begin{aligned}\mathbb{C}^8 &= \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \\ &= \mathbb{C}^4 \otimes \mathbb{C}^2 \\ &= \mathbb{C}^2 \otimes \mathbb{C}^4.\end{aligned}\tag{2.8}$$

When we consider a quantum system as a mathematical object any one of these partitions of \mathbb{C}^8 are equally valid. But in real life the possible partitions are constrained by the actual physical objects representing the state. The first of the above partitions, for instance, could be represented by three photons each with two different possible states (their polarisation).

Definition 2.2.2 (Separability and Entanglement) [RP98]

Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. A quantum state $|\psi\rangle \in \mathbb{C}^d$ is separable, if and only if it can be written in the form

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_m\rangle,\tag{2.9}$$

where $|\psi_k\rangle \in \mathbb{C}^{d_k}$. A quantum state $|\phi\rangle \in \mathbb{C}^d$ which is not separable is said to be entangled.

Entanglement has no counterpart in the classical physics, and it is more subtle than it might seem at first glance. Notice that entanglement depends on the partition considered. Thus, you might have a three-partite state $|\psi\rangle$ which have entanglement over some partition of the state (for instance between the first and the two other parties), and no entanglement over other partitions. In entanglement over several parties we find one of the subtle properties about entanglement. As we shall see in Chapter 7 it is possible to have a state in a three-partite vector space which is separable over any partition of the state into two parties, but has entanglement when partitioned into three parties. The reader may wish to pause for a moment and consider this strange fact.

2.3 Dynamics

We have now specified the states of a quantum system (a quantum computer, for example), and are ready to describe the way in which quantum states evolve. In quantum mechanics operations on quantum systems have to be reversible.

Definition 2.3.1 (Quantum Transformation) [Bra00] Let U be a $d \times d$ matrix (over complex numbers). U is unitary if and only if $U^\dagger U = \mathbb{I}$. Any unitary $d \times d$ matrix is a possible quantum transformation for any d -dimensional quantum state.

An interesting, and frequently used, transformation is the Walsh-Hadamard transformation

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (2.10)$$

When the Walsh-Hadamard transformation is applied to, say, state $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ the result is

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (2.11)$$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad (2.12)$$

$$= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \quad (2.13)$$

So the Walsh-Hadamard transformation takes a “classical” bit and puts it in a superposition.

2.4 Measurement

Finally the last part of defining the mathematical model of quantum mechanics, as used in this thesis, is to describe how we measure quantum states. Measurements can be described in several possible ways. The most important descriptions are the von Neumann measurements and the positive operator-valued measurements (POVMs). Although the different types of measurements have different mathematical formulations, they are known to have the same expressive power [NC00].

Let us first consider the general quantum measurement. In quantum mechanics the term *operator* is usually used instead of *linear transformation matrix*, or simply *matrix*.

Definition 2.4.1 (General Measurement) [NC00] *Let $\{M_1, \dots, M_n\}$ be operators of the complex vector space \mathbb{C}^d , such that $\sum_{i=1}^n M_i^\dagger M_i = \mathbb{I}$. The outcome of a measurement on a state $|\psi\rangle \in \mathbb{C}^d$ is an index of one of the operators, where the outcome i occurs with probability*

$$\text{Prob}[i] = \|M_i|\psi\rangle\|^2 = \langle\psi|M_i^\dagger M_i|\psi\rangle. \quad (2.14)$$

After the measurement the state $|\psi\rangle$ becomes

$$|\psi'\rangle = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}. \quad (2.15)$$

We refer to the operators of a general measurement as measurement operators.

Note that by the above definition measurements are in general irreversible.

In order for the sum of the probabilities of the n different outcomes has to be 1 the state $|\psi\rangle$ has to have norm 1. This is the reason why we defined quantum states to be unit vectors.

Von Neumann measurements are the most used measurement in this thesis.

A matrix A is said to be *hermitian* if $A = A^\dagger$. A hermitian matrix is also sometimes referred to as *self-adjoint*.

If A is a hermitian matrix on the complex vector space \mathbb{C}^d , and $\lambda_1, \dots, \lambda_n$ are eigenvalues of A then we can write A on the form $A = \sum_{i=1}^n \lambda_i P_i$, where P_i is the projection onto the eigenspace corresponding to eigenvalue λ_i . This can always be done because of the spectral theorem of hermitian matrices, which states that for all hermitian matrices A there exists an unitary matrix U such that $U^{-1}AU$ is a diagonal matrix. Furthermore, all eigenvalues of A are real [Bea95].

A projection matrix P is Hermitian, and furthermore $PP = P$ [NC00].

Definition 2.4.2 (von Neumann Measurement) [NC00] *Let A be a hermitian matrix with unique eigenvalues $\lambda_1, \dots, \lambda_n$. Then A describes a von Neumann measurement corresponding to a general measurement with the measurement operators $\{P_1, \dots, P_n\}$, where P_i is the projection onto the eigenspace of eigenvalue λ_i . The hermitian matrix A is called the observable of the measurement.*

Notice that because eigenvectors corresponding to different eigenvalues are orthogonal the projection matrices divide the complex vector space into orthogonal subspaces [Bea95]. Each subspace represents a possible outcome of a measurement on a quantum state defined in that quantum system. Thus an observable can be understood as asking about what subspace (state) the system is in.

When the hermitian matrix describing a von Neumann measurement is not explicitly states we are measuring with the matrix defined by the operators $\{|\psi_1\rangle\langle\psi_1|, \dots, |\psi_d\rangle\langle\psi_d|\}$, where $\{|\psi_1\rangle, \dots, |\psi_d\rangle\}$ is the standard basis of the complex vector space in which we work. We sometimes say that we are measuring in the standard basis.

In general a measurement of a quantum state only gains partial information about the original state. Thus, if the state is in a superposition then after measurement the state is projected down on one of the eigenspaces of the observable. As the measurement is irreversible we have lost all information about the original state, except that it was partly in the resulting eigenspace. We say that the state has *collapsed*.

Measurements show us the first implication of entanglement. Reconsider the state $|\text{EPR}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ first presented on page 7. The state may be seen as an element from the tensor product of two 2-dimensional vector spaces, $\mathbb{C}^2 \otimes \mathbb{C}^2$, that is, $|\text{EPR}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$. In accordance with definition 2.2.1 we perceive the vector space $\mathbb{C}^2 \otimes \mathbb{C}^2$ as being partitioned between two parties, Alice and Bob say. Now if Alice measures her part of the $|\text{EPR}\rangle$ state with an observable

with eigenvectors $|0\rangle, |1\rangle$. By Definition 2.4.2 Alice can obtain one of two possible outcomes: $|0\rangle$ or $|1\rangle$ each with probability $1/2$. If Alice obtains the outcome $|0\rangle$ the EPR state collapses to $|00\rangle$, and so if Bob subsequently measures his state, he obtains the outcome $|0\rangle$ with probability 1. Thus a measurement by Alice may alter the outcome of a measurement done subsequently by Bob. Suppose two parties each with a part of an entangled EPR pair travel in each their direction. After a while one of the parties measures his part of the state. This means that the actual state of the second party is fixed! This *non-locality* led Einstein to talk about “Spooky action on a distance”, and to his belief that the quantum theory was incomplete [RP98].

We now turn to the POVM measurement. Notice from the definition of the general measurement that all we need to know to calculate the probabilities of the outcome of a measurement is the expression $M_i^\dagger M_i$ for each measurement operator. If we do not care about the projection of the state, if, for instance, we throw away the object that we measure after measurement, we may define a measurement only knowing the expressions $M_i^\dagger M_i$.

We stated that projection matrices are Hermitian. Another subclass of the Hermitian matrices are the *positive operators*. A *positive operator* is a matrix P such that for all possible states $|\psi\rangle$, $\langle\psi|P|\psi\rangle \geq 0$ [NC00].

In the case of general measurements we are given n operators $\{M_1, \dots, M_n\}$. The probability of outcome i when measuring a state $|\psi\rangle$ is defined as $\langle\psi|M_i^\dagger M_i|\psi\rangle$. As a probability is always nonnegative the matrix $M_i^\dagger M_i$ is a positive operator.

Definition 2.4.3 (POVM Measurements) [NC00] *Let $\{E_1, \dots, E_n\}$ be positive operators such that $\sum_{i=1}^n E_i = \mathbb{I}$. Then $\{E_1, \dots, E_n\}$ describes an POVM measurement. The outcome of a measurement on a state $|\psi\rangle \in \mathbb{C}^d$ is an index of one of the positive operators, where the outcome i occurs with probability*

$$\text{Prob}[i] = \langle\psi|M_i|\psi\rangle. \quad (2.16)$$

Notice that we do not consider the state of the object, that we are measuring, after the measurement.

Chapter 3

Local Operations and Classical Communication

3.1 LOCC Protocols

In several quantum communication protocols two or more parties each hold a part of a multipartite quantum state. Furthermore they have the possibility to communicate via a classical communication channel. A classical communication channel is a channel by which only classical bits of information can be sent (0 or 1). The parties performing the communication protocol may only perform quantum operations on their own part of the shared quantum state and may only communicate by the classical channel. This, for instance, is the case in quantum teleportation [NC00].

Definition 3.1.1 (LOCC protocol) *Any protocol involving two or more parties each holding one part of a given multipartite quantum state is a LOCC protocol (Local Operations and Classical Communications Protocol), if and only if*

- *The protocol only involves a finite number of quantum operations (unitary operations and measurements) done individually by each party on the local part of the system.*
- *The protocol only involves exchange of a finite number of classical bits between the parties. And no exchange of quantum states.*

Two problems defined in terms of LOCC protocols are important to the subject of this thesis. Distillation is the problem of creating entangled states shared between parties by an LOCC protocol. Distinguishability is the ability to distinguish shared states by LOCC protocols. In both cases unextendible product bases, which are the primary concept of this thesis, relates to special cases where *neither* of these problems can be solved.

3.2 Bound Entanglement

In Chapter 2.2 we saw that quantum states can have a non-classical correlation, namely entanglement. In particular we considered the $|\text{EPR}\rangle$ state on page 7. Entanglement is a very important resource because it is used in many quantum applications such as teleportation, quantum cryptography, and quantum computing [NC00].

Imagine that two parties, Alice and Bob say, share an EPR state $1/\sqrt{2}(|00\rangle + |11\rangle)$. The outcome of a measurement performed by either Alice or Bob on his/her part of the state can be described as $1/\sqrt{2}(|0\rangle + |1\rangle)$. Now imagine that Alice performs a measurement on her part of the state without revealing the outcome to Bob. Any subsequent measurement by Bob is affected by Alice's measurement, so it would not be correct of Bob to keep the original description of his state. Rather than having the superposition $1/\sqrt{2}(|0\rangle + |1\rangle)$, he has a probability distribution $\{(1/2, |0\rangle), (1/2, |1\rangle)\}$ with probability $1/2$ of being the state $|0\rangle$ or $|1\rangle$ respectively. Such a probability distribution is called a *mixed state* or *mixture*. To distinguish the states that we have seen so far from mixed states, we denote the former as *pure states*.

Definition 3.2.1 (Mixed State) *A mixed state is a probability distribution $\{(p_1, |\psi_1\rangle), \dots, (p_n, |\psi_n\rangle)\}$ with probability p_i of having state $|\psi_i\rangle$, $\sum_{i=1}^n p_i = 1$.*

We sometimes say that a mixed state is a mixture of given states.

Notice that a pure state is a special case of a mixed state where one of the probabilities is 1.

In physics pure states are rarely observed and thus in practice only mixtures exist.

The definition of separability and entanglement cannot be applied directly to mixed states, we therefore have to give a definition of separability of mixed states.

Definition 3.2.2 (Separability and Entanglement of Mixed States) *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^k$ be an m -partite complex vector space. A mixture*

$$\{(p_1, |\psi_1\rangle), \dots, (p_n, |\psi_n\rangle)\}, \quad (3.1)$$

of states from \mathbb{C}^d is separable if and only if no measurement on any part of the state change the probability distribution of the outcome of a measurement on any of the other parties. A mixed state which is not separable is entangled.

Recall from Chapter 2.2 that the parties of a multipartite state may be chosen in several ways.

Entanglement of mixed states is more subtle than may be seen at first glance. Consider the following mixed state

$$\left\{ \left(\frac{1}{4}, \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \right), \left(\frac{1}{4}, \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \right), \right. \\ \left. \left(\frac{1}{4}, \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \right), \left(\frac{1}{4}, \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \right) \right\}, \quad (3.2)$$

shared between Alice and Bob. Notice that all the states of the mixture are entangled. Now let Alice perform a measurement on her part of the mixed state. Alice will measure one of the four states each with probability $1/4$. The outcome of Alice's measurement on any of the four states is 0 or 1 each with a probability of $1/2$. So with probability $1/2$ the outcome of Alice's measurement is 0 and with probability $1/2$ the outcome is 1. Conditioned on that Alice measures 0, the mixture collapses to the mixture

$$\left\{ \left(\frac{1}{4}, |00\rangle \right), \left(\frac{1}{4}, |00\rangle \right), \left(\frac{1}{4}, |01\rangle \right), \left(\frac{1}{4}, |01\rangle \right) \right\}, \quad (3.3)$$

which we may rewrite as $\{(1/2, |00\rangle), (1/2, |01\rangle)\}$. When Bob subsequently performs a measurement on his part of the mixture the outcome of his measurement will be 0 or 1 each with probability $1/2$. Conversely, conditioned on that Alice measures 1, the mixture collapses to the mixture

$$\left\{ \left(\frac{1}{4}, |11\rangle \right), \left(\frac{1}{4}, |11\rangle \right), \left(\frac{1}{4}, |10\rangle \right), \left(\frac{1}{4}, |10\rangle \right) \right\}, \quad (3.4)$$

which we may rewrite as $\{(1/2, |11\rangle), (1/2, |10\rangle)\}$. When Bob subsequently performs a measurement on his part of the mixture the outcome of his measurement will again be 0 or 1 each with probability $1/2$.

The outcome of Bob's measurement is thus not affected by Alice's previous measurement. In either case, Bob measures 0 or 1, each with probability $1/2$.

By Definition 3.2.2 a mixed state is separable if no measurement on one part of the state changes the probability distribution of measurement on another part of the state. We have seen that a measurement in the standard basis of the mixture given by Equation 3.2 does not change the probability distribution, and it can be verified that no measurement does. The mixture of Equation 3.2 is thus, not entangled, but rather separable.

Some entangled states are not as useful as others when used in quantum applications such as teleportation, quantum cryptography, and quantum computing [NC00]. To capture the usefulness of an entangled state several measures of "usefulness" has been proposed [NC00]. In [BBP96] Bennett, Bernstein, Popescu, and Schumacher show an LOCC protocol that can be used to create useful entangled states out of a number of copies of any entangled pure state. This process of creating useful entanglement is called *distilling*.

It came as a surprise that entangled mixed states which are not distillable exists. In [HHH98] Horodecki, Horodecki, and Horodecki prove the existence of such non-distillable mixed states. These *bound entangled* states have been the center of much attention since their discovery.

Definition 3.2.3 (Bound Entanglement) *Let $\{(p_1, |\psi_1\rangle), \dots, (p_n, |\psi_n\rangle)\}$ be an entangled mixed quantum state. Then $\{(p_1, |\psi_1\rangle), \dots, (p_n, |\psi_n\rangle)\}$ is bound entangled if and only if no LOCC protocol exists by which an entangled pure state can be created from a finite number of copies of $\{(p_1, |\psi_1\rangle), \dots, (p_n, |\psi_n\rangle)\}$.*

As all pure states are distillable all bound entangled states are mixed states.

Bound entangled states are interesting for us, because they have a relationship with unextendible product bases. We return to this relationship in Chapter 4.2.

3.3 Distinguishability

In some cases we may be interested in deciding which state of a predefined set of states we are given. This could for instance be the case if we have a mixed state.

In the case where a person is given one state of a set of mutual orthogonal states he can make a measurement which decides which state he is given by a von Neumann measurement.

The case of nonorthogonal states is more interesting. Suppose you are given one of the two states

$$\begin{aligned} |\psi_1\rangle &= \sin\theta|0\rangle + \cos\theta|1\rangle, \\ |\psi_2\rangle &= \sin\theta|0\rangle - \cos\theta|1\rangle, \end{aligned} \tag{3.5}$$

where $0 < \theta < \frac{\pi}{2}$ is some angle. Because the states are nonorthogonal no measurement exists which, with certainty, can tell you which of these two states you have [NC00]. And after measurement the state collapses. The best you can do is to use the measurement of the observable

$$A = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) + \frac{-1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|). \tag{3.6}$$

If the outcome of the measurement is 1 your best guess is that the given state was $|\psi_1\rangle$, and conversely if the outcome is -1 you guess that the state was $|\psi_2\rangle$. Your guess is then correct with probability $(1 + \cos\theta \sin\theta)/4$ [Bra00].

Surprisingly a number of parties, as given by Definition 2.2.1, sharing a multipartite state from a given set of mutually orthogonal multipartite states cannot always find an LOCC protocol to decide which one of the possible states they are given. Notice since the set of multipartite states are mutually orthogonal it is a simple matter to tell them apart if a measurement can be performed on the whole state.

Definition 3.3.1 (Indistinguishability) *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. And let S be a set of states from \mathbb{C}^d . The set S is indistinguishable if and only if no LOCC protocol exists by which m parties sharing an arbitrary state from S can decide with certainty which one of the states of S they are given.*

Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, and Wootters first demonstrated indistinguishability in [BDF⁺98], where the following full orthonormal basis of $\mathbb{C}^3 \otimes \mathbb{C}^3$ is shown to be indistinguishable

$$\begin{aligned}
& |1\rangle \otimes |1\rangle, \\
& |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\
& |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\
& |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \\
& |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\
& \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \otimes |0\rangle, \\
& \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle, \\
& \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |2\rangle, \\
& \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle.
\end{aligned} \tag{3.7}$$

Until now we have only seen one nonlocal property of quantum mechanics, namely entanglement. Entanglement is one of the cornerstones in quantum mechanics, and as mentioned in the previous chapter has been the center of much discussion. Indistinguishability is, however, a recent discovery of a nonlocal property of quantum systems.

In Chapter 4.3 we state the relationship between indistinguishability and unextendible product bases.

Chapter 4

Product Bases

4.1 PB and UPB

One of the central concepts of this thesis is the concept of *Unextendible Product Basis*. Unextendible product bases are first mentioned by Bennett, DiVincenzo, Mor, Shor, Smolin, and Terhal in [BDM⁺98]. A Product Basis is just a, possibly incomplete, basis for a multipartite complex vector space (See Chapter 2.2), where each basis vector is separable between all parties. The basis vectors of a product basis are referred to as *product states*. If, for instance, you have a state composed of two qubits, $|1\rangle \otimes |0\rangle$ say, then this is a product state of a 4-dimensional, bipartite, complex vector space.

Definition 4.1.1 (Product State) *Let $\otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. A state $|\psi\rangle \in \otimes_{k=1}^m \mathbb{C}^{d_k}$ is a product state if and only if it has the form $|\psi\rangle = \otimes_{k=1}^m |\phi_k\rangle$ where $|\phi_k\rangle \in \mathbb{C}^{d_k}$.*

Notice that a product state *might* have entanglement with respect to some choices of the partition of the complex vector space if more are possible. Take for instance the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |111\rangle)$. Then $|\psi\rangle$ is a 3 qubit state which is separable between the first two qubits and the third qubit as it can be written $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |1\rangle$. However, there is entanglement between the first (or second) qubit and the other two. The state $|\psi\rangle$ is a product state in the bipartite complex vector space $\mathbb{C}^4 \otimes \mathbb{C}^2$, where $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ belongs to the first complex vector space and $|1\rangle$ belongs to the second vector space. But the state $|\psi\rangle$ is not a product state in the three-partite complex vector space $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$.

Definition 4.1.2 (Product Basis) [BDM⁺98] *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. A product basis is a set S of orthogonal product states spanning a subspace $\mathbb{C}_S^d \subseteq \mathbb{C}^d$. Henceforth we denote this a PB.*

The states $|0\rangle \otimes |0\rangle$, and $|0\rangle \otimes |1\rangle$ form a, product basis spanning a two dimensional subspace of the complex vector space $\mathbb{C}^2 \otimes \mathbb{C}^2$ (of dimension 4).

This example shows a product basis which does not span all of $\mathbb{C}^2 \otimes \mathbb{C}^2$. As we shall now see it is sometimes possible to make such an incomplete product basis, such that no other product state exists which is orthogonal to the states of the product basis. Such a product basis, referred to as an *unextendible product basis*, cannot be extended to a product basis spanning the whole complex vector space.

Definition 4.1.3 (Unextendible Product Basis) [BDM⁺98]

Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space, and let S be a product basis which spans a proper subspace $\mathbb{C}_S^d \subset \mathbb{C}^d$. If the orthogonal complement, $\mathbb{C}_S^{d\perp}$, contains no product state, then S is said to be an unextendible product basis of \mathbb{C}^d , henceforth denoted a UPB.

Consider the following example of a UPB from [BDM⁺98]. Thus UPB, called **Tiles**, span a 5-dimensional subspace of $\mathbb{C}^9 = \mathbb{C}^3 \otimes \mathbb{C}^3$, and there is no other product state in $\mathbb{C}^3 \otimes \mathbb{C}^3$ which is orthogonal to the five states of **Tiles**.

$$\begin{aligned} |\psi_1\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle, \\ |\psi_3\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\ |\psi_4\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle, \\ |\psi_5\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \otimes \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle). \end{aligned} \tag{4.1}$$

In Chapter 5 we return to the question of unextendability.

4.2 UPBs and Bound Entanglement

In Chapter 1 we mentioned that one of the reasons why UPBs are interesting is their relation to bound entanglement. The following theorem is therefore one of the important theorems when motivating the study of UPBs.

Theorem 4.2.1 [BDM⁺98] Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space, and let S be a UPB of \mathbb{C}^d that spans a proper subspace $\mathbb{C}_S^d \subset \mathbb{C}^d$. Let $B = \{|\psi_{n+1}\rangle, |\psi_{n+2}\rangle, \dots, |\psi_d\rangle\}$ be any basis of the orthogonal complement $\mathbb{C}_S^{d\perp}$. Then the state corresponding to the uniform mixture of the states of B

$$\left\{ \left(\frac{1}{d-n}, |\psi_{n+1}\rangle \right), \left(\frac{1}{d-n}, |\psi_{n+2}\rangle \right), \dots, \left(\frac{1}{d-n}, |\psi_d\rangle \right) \right\} \tag{4.2}$$

is a bound entangled state, partitioned between the m parties of \mathbb{C}^d .

This provides a method of constructing states with bound entanglement.

The above theorem states that all UPBs have an associated bound entangled state. The converse, however, is not true as a bound entangled state in $\mathbb{C}^2 \otimes \mathbb{C}^4$ is demonstrated by Paweł Horodecki in [Hor97], and as we shall see in Chapter 6 no UPB exists in $\mathbb{C}^2 \otimes \mathbb{C}^4$.

4.3 Uncompletable Product Bases

Per definition we cannot extend a UPB to a full product basis of the complex vector space in which it resides. The definition of UPBs, Definition 4.1.3, even implies that we cannot add another product state to a UPB. Yet some product bases are extendible to a full product basis. The question arises whether product bases exists which can be extended, but never to a full basis. As shown by DiVincenzo, Mor, Shor, Smolin, and Terhal in [DMS⁺99] the answer to this question is yes. Product bases that cannot be extended to a full basis are called *uncompletable*.

Definition 4.3.1 (Uncompletable Product Basis) [DMS⁺99]

Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space, and let S be a product basis which spans a proper subspace $\mathbb{C}_S^d \subset \mathbb{C}^d$. If the orthogonal complement, $\mathbb{C}_S^{d\perp}$, contains fewer mutual orthogonal product states than the dimension of $\mathbb{C}_S^{d\perp}$, then the product basis is said to be an uncompletable product basis, henceforth denoted an UCPB.

Even though an UCPB is uncompletable in the complex vector space where it has been defined, it is sometimes possible to extend the UCPB to be a full basis of a larger complex vector space, thus making it a complete basis for the extended complex vector space.

Definition 4.3.2 (Strongly Uncompletable Product Basis) [DMS⁺99]

Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. A product basis, S , of \mathbb{C}^d is strongly uncompletable if for all locally extended complex vector spaces, $\mathbb{C}^{d'} = \otimes_{k=1}^m (\mathbb{C}^{d_k+d'_k})$, where S also spans a proper subspace $\mathbb{C}_S^{d'} \subset \mathbb{C}^{d'}$, the orthogonal complement $\mathbb{C}_S^{d'\perp}$ contains fewer mutually orthogonal product states than its dimension. We henceforth denote this a SUCPB.

As an example of uncompletability consider the UPB of Equation 4.1. As **Tiles** is a UPB it cannot be extended, but if we remove the state $|\psi_5\rangle$ then $S' = \{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, |\psi_4\rangle\}$ is an extendible product basis. As **Tiles** is a UPB it follows that S' is a product basis, that S' is an extendible product basis may be seen from the following equation, which is an extension of S' to a full basis of $\mathbb{C}^3 \otimes \mathbb{C}^3$.

$$\begin{aligned}
|\psi_1\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle, \\
|\psi_3\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\
|\psi_4\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle, \\
|\psi_5\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\
|\psi_6\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |2\rangle, \\
|\psi_7\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \\
|\psi_8\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \otimes |0\rangle, \\
|\psi_9\rangle &= |1\rangle \otimes |1\rangle,
\end{aligned} \tag{4.3}$$

where $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, |\psi_4\rangle\} = S'$. It is easy, but tedious, to verify that Equation 4.3 is a full product basis for $\mathbb{C}^3 \otimes \mathbb{C}^3$.

If we remove any other state of Equation 4.1 we get an uncompletable product basis. For this reason the fifth state of **Tiles** has been referred to as the *stopper* in the literature [BDM⁺98].

It turns out there is a relation between strong uncompleteness and indistinguishability. This relationship is characterised by the following theorem.

Theorem 4.3.3 [BDM⁺98] *Let S be a product basis of $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$. If the states of S are distinguishable by an LOCC protocol involving only von Neumann measurements then S is completable in \mathbb{C}^d . If the states of S are distinguishable by an LOCC protocol involving POVMs measurements then S can be completed in some extended complex vector space $\mathbb{C}^{d'} = \otimes_{k=1}^m \mathbb{C}^{d_k+d'_k}$.*

The relationship between uncompleteness, distinguishability and UPBs is expressed in the following two results.

Lemma 4.3.4 [BDM⁺98] *An unextendible product basis is strongly uncompletable.*

This lemma together with Theorem 4.3.3 implies that UPBs are indistinguishable.

Theorem 4.3.5 [BDM⁺98] *An unextendible product basis is indistinguishable.*

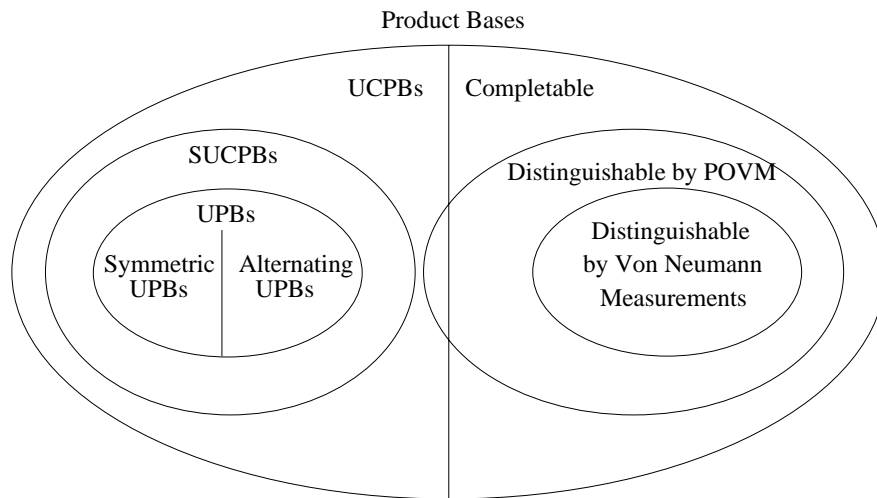


Figure 4.1: The hierarchy of the different classes of product bases

The relationship between the different product bases can be seen in Figure 4.1.

Completable product bases can be extended such that they span the full complex vector space. *Distinguishable product bases* are product bases where the states can be distinguished by local operations and classical communication. *Uncompletable product bases* (UCPBs), are product bases that might be extended with more orthogonal product states, but never to a full basis. *Strongly uncompletable product bases* (SUCPBs) cannot be completed even in a larger vector space. Finally *unextendible product bases* (UPBs) fall into two categories, symmetric and alternating which relates to minimality of unextendible product bases. We return to symmetric and alternating UPBs in Chapter 5.4.

Chapter 5

Relations to Graph Theory

5.1 The Counting Lemma

Before presenting the graph theoretic aspects of UPBs, let us consider a lemma which plays an important role in many proofs of the unextendability of UPBs.

The *Counting Lemma* by Bennett, DiVincenzo, Mor, Shor, Smolin, and Terhal [BDM⁺98] is based on the observation that for a PB, S , which is not a UPB some product state exists which is orthogonal to all the states of S . In particular it is orthogonal to each state in at least one of the parties¹. Conversely, if S is to be unextendible, Thus we know that the new state is orthogonal to some of the states of S , $S_1 \subseteq S$ say, in the first party, some of the states of S , $S_2 \subseteq S$, in the second party, e.t.c. Because all states of S are orthogonal to the new state, all states of S are in at least one of the sets S_1, \dots, S_m .

Lemma 5.1.1 (Counting Lemma) [BDM⁺98] *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite vector space. And let $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, 2, \dots, n\} \subset \mathbb{C}^d$ be a product basis of \mathbb{C}^d with n states. Then S is extendible if and only if there exists m disjoint subsets $S = S_1 \cup S_2 \cup \dots \cup S_m$ of S such that for all $k = 1, \dots, m$ $\text{rank}(\{|\phi_{ik}\rangle \mid |\psi_i\rangle \in S_k\}) < d_k$.*

Proof. First we prove that if $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, 2, \dots, n\}$ is extendible then subsets $S = S_1 \cup S_2 \cup \dots \cup S_m$ of S exists such that for all $k \in \{1, 2, \dots, m\}$, the local rank $r_k = \text{rank}(\{|\phi_{ik}\rangle \mid |\psi_i\rangle \in S_k\}) < d_k$ of the k th subset is strictly less than the dimension d_k of the k th party's vector space.

As S is extendible then, by Definition 4.1.3, some product state, $|\psi\rangle$, exists which is orthogonal to all states of S . In particular, because of Equation 2.4, S can be divided into subsets $S_1 \cup S_2 \cup \dots \cup S_m = S$ such that $|\psi\rangle$ is orthogonal to all states of S_k in the k th party, for all $k \in \{1, 2, \dots, m\}$. If the sets S_1, \dots, S_k are not disjoint we make them disjoint, by removing repeated states from one of

¹Because the inner product splits into the product of the inner products on each party: $\langle \psi_1 \otimes \psi_2 | \phi_1 \otimes \phi_2 \rangle = \langle \psi_1 | \phi_1 \rangle \langle \psi_2 | \phi_2 \rangle$. See Equation 2.4 on page 7.

the sets where they occur. As $|\psi\rangle$ is orthogonal to all the states of S_k in the k th party for all $k \in \{1, 2, \dots, m\}$ the states of S_k cannot span the full vector space, thus $r_k < d_k$.

Now assume that subsets $S_1 \cup S_2 \cup \dots \cup S_m = S$ are given, such that $r_k < d_k$. Then for each $k \in \{1, 2, \dots, m\}$ we can use Gram-Schmidt orthogonalisation to find a state $|\phi_k\rangle$ which is orthogonal to the states of S_k in the k th party [Bea95]. Then the state $|\psi\rangle = \otimes_{k=1}^m |\phi_k\rangle$ is a product state which is orthogonal to all states of S , making S extendible. \square

Consider the **Tiles** UPB on page 20. To find a product state which is orthogonal to all the states of **Tiles** the Counting Lemma states that we have to find two subsets each of rank 2 or less. Notice that any three given states from any party has rank 3. As there is no way we can find two subsets both with less than three states, we conclude that **Tiles** is unextendible. This proves the claim on page 20 as promised.

5.2 Orthogonality Graphs

We first introduce some concepts from graph theory.

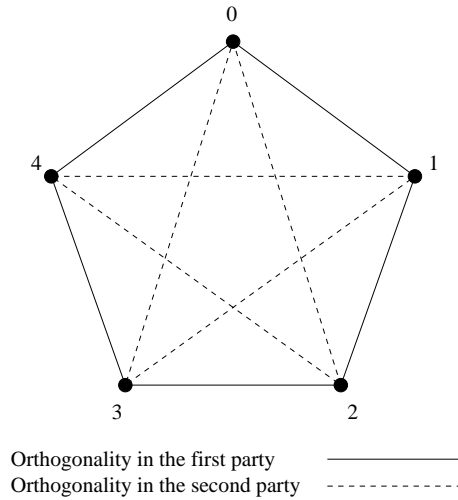
Definition 5.2.1 (Graph) A graph G is a tuple $G = (V, E)$, where V is a set of vertices, and $E \subseteq V \times V$ is a set of edges connecting the vertices of G , such that $(v, w) \in E \Rightarrow (w, v) \in E$. Two vertices $v, w \in V$ are connected if and only if $(v, w) \in E$. A graph where all vertices are connected, $K_n = (V, V \times V)$, is called the complete n -graph.

Definition 5.2.2 (Vertex Degree) Let $G = (V, E)$ be a graph, and let $v \in V$ be a vertex. The degree of v is number of vertices connected to v in G $\text{degree}(v) = \|\{w \in V \mid (v, w) \in E\}\|$.

Definition 5.2.3 (Connected Component) Let $G = (V, E)$ be a graph. The connected components of G are a sets of vertices such that

- A vertex $v \in V$ is in the same connected component as itself.
- Two connected vertices $(v, w) \in E$ are in the same connected component.
- If two connected vertices $(v, w) \in E$ are in the same connected component, and vertices $(w, u) \in E$ are in the same connected component, then v and u are in the same connected component.

Definition 5.2.4 (Graph Connectivity) Let $G = (V, E)$ be a graph. The connectivity of G is the cardinality of the smallest set of vertices $S \subseteq V$ such that the graph $(V \setminus S, E \setminus S \times S)$ has at least two connected components.

Figure 5.1: Orthogonality graph for the **Tiles** UPB

By Definition 4.1.2 the states of a PB are mutual orthogonal. From Equation 2.4 we know that the inner product on a multipartite vector space splits up as a product of the inner products on each party, therefore all the states has to be mutually orthogonal in at least one, but not necessarily all, of the parties. These orthogonality relations between the states can be captured in graphs.

Inspired by work from information theory, DiVincenzo, Mor, Shor, Smolin, and Terhal [DMS⁺99] introduces orthogonality graphs to analyse the orthogonality relations between the states of a PB. An orthogonality graph of a PB with n states is the complete n -graph. Each vertex of the graph represents a state of the PB. An edge connecting two vertices has labels or colours denoting the parties for which the represented states are orthogonal.

Definition 5.2.5 (Orthogonality Graph) [DMS⁺99] Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. And let S be a product basis of \mathbb{C}^d with n states, $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, \dots, n\}$. Then the orthogonality graph of S is the triple $(S, S \times S, c)$, where $(S, S \times S) = K_n$ is the complete n -graph, and $c : S \times S \rightarrow \mathcal{P}(\{1, 2, \dots, m\})$ is a colouring of the edges of K_n defined by $c(|\psi_i\rangle, |\psi_j\rangle) = \{k \mid |\phi_{ik}\rangle \perp |\phi_{jk}\rangle\}$.

As an example of an orthogonality graph, Figure 5.1 shows the graph for the **Tiles** UPB from Chapter 4.1.

Sometimes it is useful to consider the orthogonality relations on one party at a time. To facilitate this we define the orthogonality graph of one party.

Definition 5.2.6 (Orthogonality Graph of the k th Party) Let $G = (S, S \times S, c)$ be an orthogonality graph. The orthogonality graph of the k th party is the graph $G_k = (S, E_k)$, where $E_k = \{e \in S \times S \mid k \in c(e)\}$.

We use $\text{degree}_k(v)$ to denote the degree of vertex v in the orthogonality graph of the k th party.

In [DMS⁺99] orthogonality graphs are used to argue that UPBs with certain orthogonality relations cannot exist. In particular they prove the following result.

Proposition 5.2.7 [DMS⁺99] *The states of any multipartite product basis, S , with three or fewer states are distinguishable by an LOCC protocol.*

See the definition of LOCC protocols on page 13.

This proof is different than the one given in [DMS⁺99].

Proof. Let $G = (S, S \times S, c)$ be some given orthogonality graph. We prove that for any PB, $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, 2, 3\}$, with the orthogonality graph G an LOCC protocol exists which distinguishes the states of S .

First assume that all edges share some colour c_1 , then the states are mutual orthogonal in the c_1 th party and can be distinguished by a local von Neumann measurement by that party.

Now assume that two edges share some colour. Without loss of generality, let edges $(|\psi_1\rangle, |\psi_2\rangle)$, and $(|\psi_1\rangle, |\psi_3\rangle)$ share colour 1. Then the first party can perform a local von Neumann measurement with eigenspaces $|\phi_{11}\rangle\langle\phi_{11}|$ and $\mathbb{I} - |\phi_{11}\rangle\langle\phi_{11}|$, with eigenvalues λ_1 and λ_2 , respectively. If the outcome of the measurement is λ_1 , we know with certainty that the state is $|\psi_1\rangle$. The first party announces so to the other parties, and the protocol is over.

If the outcome of the measurement is λ_2 , we know that the given state is either $|\psi_2\rangle$ or $|\psi_3\rangle$, and the actual state is projected onto $\mathbb{I} - |\phi_{11}\rangle\langle\phi_{11}|$ after measurement², which does not alter the state in any of the two cases. As G is an orthogonality graph the edge $(|\psi_2\rangle, |\psi_3\rangle)$ has some colour, c_2 . As the two states are not altered by the first measurement they are still orthogonal in the c_2 th party. The first party now informs the c_2 th party of the outcome of the measurement, and the c_2 th party can then distinguish between the last two states.

Finally assume that no two edges share a colour. Without loss of generality, let $1 \in c(|\psi_1\rangle, |\psi_2\rangle)$, $2 \in c(|\psi_2\rangle, |\psi_3\rangle)$, and $3 \in c(|\psi_1\rangle, |\psi_3\rangle)$. First we let the first party perform a local von Neumann measurement with the eigenspaces $|\phi_{11}\rangle\langle\phi_{11}|$ and $\mathbb{I} - |\phi_{11}\rangle\langle\phi_{11}|$, with eigenvalues λ_1 and λ_2 respectively. If the outcome of the measurement is λ_1 the given state is either $|\phi_{11}\rangle$ or $|\phi_{31}\rangle$. If the outcome is λ_2 the given state is either $|\phi_{21}\rangle$ or $|\phi_{31}\rangle$. As only the local states are collapsed the orthogonality of the three states do not change for the other two parties. So if the outcome is λ_1 the measured state is known to be either $|\psi_1\rangle$ or $|\psi_3\rangle$, in this case the first party informs the third party of the outcome, and the third party can distinguish the two states. If the outcome is λ_2 the measured state is known to be either $|\psi_2\rangle$ or $|\psi_3\rangle$, in this case the first party informs the second party of the outcome, and the second party can distinguish the two states. \square

²See Definition 2.4.2

This proof provides an explicit LOCC protocol in the three different cases. Notice in the last case that there need not be three different parties. One party may play the role of two parties. This observation will simplify our proof of Theorem 5.2.8 below.

Proposition 5.2.7 together with Theorem 4.3.3 implies that no UPB with three or fewer states exists.

The proof of Proposition 5.2.7 and the above argument is a typical use of orthogonality graphs. First the orthogonality graph is used to show that some LOCC protocol exists which distinguishes the states represented by the vertices, and then Theorem 4.3.3 is applied to argue that no UPB exists with such orthogonality graph.

Let us take a look at the two other results from [DMS⁺99] which are based on orthogonality graphs.

Theorem 5.2.8 [DMS⁺99] *Let S be any bipartite PB with four or fewer states. Then the states of S are completable.*

This proof is different than the one given in [DMS⁺99].

Proof. Let $G = (S, S \times S, c)$ be the two-coloured orthogonality graph of the bipartite PB, $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, 2\}$.

First assume that some vertex, $|\psi_i\rangle$, exists which is connected to all other vertices with some colour, c say. Then the c th party can distinguish this state from the other three states in his local system by a local von Neumann measurement which does not alter any of the states. If the outcome of the measurement tells him that the state is $|\psi_i\rangle$ the protocol is done. If the outcome of the measurement tells him that the measured state is one of the three other states Proposition 5.2.7 gives us an LOCC protocol which distinguishes these states.

Now assume that no vertex is connected to all other vertices by the same colour. That is: All vertices are connected to one other vertex with one colour and the two last vertices with the other colour. Without loss of generality, let the edges $(|\psi_1\rangle, |\psi_2\rangle)$ and $(|\psi_1\rangle, |\psi_3\rangle)$ have colour 1 and the edge $(|\psi_1\rangle, |\psi_4\rangle)$ have colour 2.

First we observe that since $\langle \phi_{41} | \phi_{11} \rangle \neq 0$, we have $|\phi_{41}\rangle = |\phi_{11}\rangle + |\phi'\rangle$, for some state $|\phi'\rangle$. If $|\phi_{41}\rangle$ is orthogonal to some other state $|\phi''\rangle$ which is also orthogonal to $|\phi_{11}\rangle$ then $\langle \phi_{41} | \phi'' \rangle = \langle \phi_{11} | \phi'' \rangle + \langle \phi' | \phi'' \rangle = \langle \phi' | \phi'' \rangle = 0$, and so $|\phi'\rangle$ and $|\phi''\rangle$ are also orthogonal.

Let the first party make a local von Neumann measurement with the two eigenspaces $|\phi_{11}\rangle\langle\phi_{11}|$ and $\mathbb{I} - |\phi_{11}\rangle\langle\phi_{11}|$, with eigenvalues λ_1 and λ_2 respectively. If the state $|\phi_{11}\rangle$ is measured the outcome is λ_1 with certainty, and the state is not altered after measurement. If one of the states $|\phi_{21}\rangle$ or $|\phi_{31}\rangle$ is measured the outcome is λ_2 and the state is not altered neither. If, on the other hand, state $|\phi_{41}\rangle$ is measured the outcome is either λ_1 or λ_2 each with a positive probability.

If the outcome is λ_1 then we know that the original state was either $|\phi_{41}\rangle$ or $|\phi_{11}\rangle$ and $|\phi_{41}\rangle$ is collapsed to $|\phi_{11}\rangle$. But as only the local state collapses, the

states $|\phi_{12}\rangle$ and $|\phi_{42}\rangle$ are still orthogonal in the second party, which can then distinguish them.

If the outcome is λ_2 then we know that the original state was either $|\phi_{21}\rangle$, $|\phi_{31}\rangle$, or $|\phi_{41}\rangle$ and $|\phi_{41}\rangle$ is collapsed to $|\phi'\rangle$. As $|\phi_{11}\rangle$ is orthogonal to both $|\phi_{21}\rangle$ and $|\phi_{31}\rangle$ the observation above gives us that $|\phi'\rangle$ is orthogonal to the same states as is $|\phi_{41}\rangle$. Thus the outcome λ_2 tells us that the measured state is one of $|\phi_{21}\rangle$, $|\phi_{31}\rangle$, or $|\phi_{41}\rangle$, and then Proposition 5.2.7 gives us an LOCC protocol which distinguishes these states. \square

Theorem 5.2.9 [DMS⁺99] *All UPBs in $\mathbb{C}^3 \otimes \mathbb{C}^3$ have the orthogonality graph of Figure 5.1.*

This proof is different than the one given in [DMS⁺99].

Proof. Let $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, 2\}$ be a bipartite PB and let $G = (S, S \times S, c)$ be the orthogonality graph of S . We prove that if G is not the graph of Figure 5.1 then S is distinguishable, which by Theorem 4.3.3 implies that S is extendible.

Assume that some vertex, $|\psi_i\rangle$, of G is connected to all other vertices of G by some colour, c . Then the c th party can distinguish this state from the other four states in his local system by a local von Neumann measurement which does not alter any of the states. If the outcome of the measurement tells him that the state is $|\psi_i\rangle$ the protocol is done. If the outcome of the measurement tells him that the measured state is one of the four other states Theorem 5.2.8 gives us an LOCC protocol which distinguishes these states.

Assume now that some vertex of G is connected to three other vertices of G by some colour, c_1 , and the last vertex by some other colour $c_2 \neq c_1$. Without loss of generality, let $c_1 \in c(|\psi_1\rangle, |\psi_2\rangle), c_1 \in c(|\psi_1\rangle, |\psi_3\rangle)$, and $c_1 \in c(|\psi_1\rangle, |\psi_4\rangle)$, and that $c_2 \in c(|\psi_1\rangle, |\psi_5\rangle)$.

First we observe that $|\phi_{51}\rangle = |\phi_{11}\rangle + |\phi'\rangle$, for some state $|\phi'\rangle$. If $|\phi_{51}\rangle$ is orthogonal to some other state $|\phi''\rangle$ which is also orthogonal to $|\phi_{11}\rangle$ then $\langle \phi_{51} | \phi'' \rangle = \langle \phi_{11} | \phi'' \rangle + \langle \phi' | \phi'' \rangle = \langle \phi' | \phi'' \rangle = 0$, and so $|\phi'\rangle$ and $|\phi''\rangle$ are also orthogonal.

Let the first party make a local von Neumann measurement with the two eigenspaces $|\phi_{11}\rangle\langle\phi_{11}|$ and $\mathbb{I} - |\phi_{11}\rangle\langle\phi_{11}|$, with eigenvalues λ_1 and λ_2 respectively. If the state $|\phi_{11}\rangle$ is measured the outcome is λ_1 with probability 1, and the state is not altered after measurement. If one of the states $|\phi_{21}\rangle$, $|\phi_{31}\rangle$, or $|\phi_{41}\rangle$ is measured the outcome is λ_2 and the state is not altered neither. If, on the other hand, state $|\phi_{51}\rangle$ is measured the outcome is either λ_1 or λ_2 each with a positive probability.

If the outcome is λ_1 then we know that the original state was either $|\phi_{11}\rangle$ or $|\phi_{51}\rangle$ and $|\phi_{51}\rangle$ is collapsed to $|\phi_{11}\rangle$. But as only the local state collapses the

states $|\phi_{12}\rangle$ and $|\phi_{52}\rangle$ are still orthogonal in the second party, which can then distinguish them.

If the outcome is λ_2 then we know that the original state was either $|\phi_{21}\rangle$, $|\phi_{31}\rangle$, $|\phi_{41}\rangle$, or $|\phi_{51}\rangle$ and $|\phi_{51}\rangle$ is collapsed to $|\phi'\rangle$. As $|\phi_{11}\rangle$ is orthogonal to $|\phi_{21}\rangle$, $|\phi_{31}\rangle$, and $|\phi_{41}\rangle$ the previous observation gives us that $|\phi'\rangle$ is orthogonal to the same states as is $|\phi_{51}\rangle$. Thus the outcome λ_2 tells us that the measured state is one of $|\phi_{21}\rangle$, $|\phi_{31}\rangle$, $|\phi_{41}\rangle$, or $|\phi_{51}\rangle$, and then Theorem 5.2.8 gives us an LOCC protocol which distinguishes these states.

Now the only case left is graphs where no vertex is connected to all other vertices by a single colour, and no vertex is connected to three other vertices by a single colour. This only leaves the case where all vertices are connected to two other vertices with each of the two colours. Which is exactly the graph of Figure 5.1, which is the orthogonality graph of the **Tiles** UPB. \square

These three proofs from [DMS⁺99] are very similar. In fact the two last proofs have identical passages in the form presented here. They are all constructive proofs, where an explicit LOCC protocol is found. The LOCC protocols of the three proofs are based on von Neumann measurements only.

Let us examine how well orthogonality graphs can describe distinguishability.

When describing an explicit LOCC protocol von Neumann measurement are generally used as the measurements of the LOCC protocol. The reason for this is that we do not know the state of a quantum system after measuring with a POVM measurement. We can therefore in general not use this state in a subsequent step of the LOCC protocol.

The three previous proofs build on the fact that a von Neumann measurement corresponds to projecting the measured state down on one of a number of orthogonal eigenspaces of the measurement.

Let us see what happens with the colour of the edge connecting two vertices when a von Neumann measurement is performed.

Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be states which reside entirely in, possibly different, eigenspaces. By definition of the von Neumann Measurement (Definition 2.4.2) the state are not altered after measurement. Therefore the edges connecting these states do not alter colours after measurement.

Let $|\psi_1\rangle$ be a state that resides in more than one eigenspace, and let $|\psi_2\rangle$ be a state which resides entirely in one eigenspace. By Definition 2.4.2 $|\psi_1\rangle$ is projected down on one of the eigenspaces in which it resides. If $|\psi_2\rangle$ resides in the resulting eigenspace the orthogonality between $|\psi_1\rangle$ and $|\psi_2\rangle$ is unchanged. Therefore the edges connecting the resulting state to $|\psi_2\rangle$ is not altered. If, however, $|\psi_2\rangle$ resides in an eigenspace different to the resulting eigenspace the resulting state is, of course, orthogonal to $|\psi_2\rangle$. This, however, is no problem, as we, at this point of the LOCC protocol, are only interested in the resulting eigenspace.

Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two states which do not reside entirely in one eigenspace are both altered when projected. As the orthogonality graph cannot tell whether the two states are orthogonal in the resulting eigenspace or another eigenspace before measurement, we do not know whether they remain orthogonal after measurement. Therefore the edges between two states become colourless.

We have not seen the last case in any of the three proofs from [DMS⁺99].

An LOCC protocol also permits local unitary operations on each party. But unitary operations preserve angles [NC00], and therefore they do not alter the orthogonality graph.

We can now see that a measurement corresponds to *dissecting* the graph into smaller graphs each representing the states which are non-null when projected down on a certain eigenspace of the measurement, that is, states which can have the same outcome of the measurement. Edges between states which each has a non-null projection on more than one eigenspace lose their colour after this *dissection*.

We see from the argument above that one limitation when representing LOCC protocols only by orthogonality graphs is that we lose all information about the orthogonality of two states which resides in more than one eigenspace. We return to this limitation later in this chapter. Another limitation is that we cannot represent POVM measurements, as the spaces to which the results are projected need not be orthogonal in a POVM measurement.

Let us now turn our attention to the construction of an LOCC protocol when only given an orthogonality graph.

When only given an orthogonality graph, we express the eigenspaces of the von Neumann measurements of an LOCC protocol in terms of the vertices of the graph.

As measurements can only be done locally by each party, and as a local measurement can only distinguish vertices which are connected with the colour of that party, a measurement can only *dissect* the graph into subsets such that all edges between vertices of different subsets have the colour of that party. The outcome is the vertices of one of the subsets, with the same colours on edges connecting them, plus all vertices not in any of the subsets with the same colour on edges going into the subset and no colour on edges between the vertices outside the subset.

The process is repeated for each new orthogonality graphs separately until the graphs are *dissected* into individual vertices.

If a *dissection* of an orthogonality graph into individual vertices can be found we have an explicit construction of an LOCC protocol which can distinguish the states of any PB with that orthogonality graph. This, by Theorem 4.3.3, further implies that all PBs with such orthogonality graph are completable, which by definition is equivalent to saying that no UPB exists with that orthogonality graph.

One could be led to hope that the converse of the implication of *dissection* is also true. This would imply that *dissection* of orthogonality graphs is equivalent to an LOCC protocol, based on von Neumann measurements, that distinguish the states of all PBs with that orthogonality graph.

If, furthermore, the converse of Theorem 4.3.3 holds, that is to say that all completable product bases are distinguishable, *dissection* would characterise UCPBs. This, unfortunately, is not true. Completable, indistinguishable PBs exist. One such PB is

$$\begin{aligned}
|\psi_1\rangle &= |1\rangle \otimes |1\rangle \\
|\psi_2\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\
|\psi_3\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\
|\psi_4\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \\
|\psi_5\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\
|\psi_6\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \otimes |0\rangle, \\
|\psi_7\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle, \\
|\psi_8\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |2\rangle, \\
|\psi_9\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle.
\end{aligned} \tag{5.1}$$

In [BDF⁺98] Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, and Wootters show that this product basis is indistinguishable. And since it is a full basis of $\mathbb{C}^3 \otimes \mathbb{C}^3$ it is indeed completable.

So even though all PBs with a certain orthogonality graph are completable we might not be able to find a *dissection* of that orthogonality graph.

To the author it is unknown whether *dissection* is equivalent to LOCC protocols based on von Neumann measurements. There are indications that this is not true neither. Consider the states of the orthogonality graph of Figure 5.2, which is an orthogonality graph of a bipartite PB with 6 states. Alice's part of the states is explicitly represented in the figure. One way these states can be distinguished by an LOCC protocol is if Alice measures whether the given state is in one of the two subspaces

$$\begin{aligned}
&\{|0\rangle, |1\rangle\}, \\
&\{|2\rangle, |3\rangle\}.
\end{aligned} \tag{5.2}$$

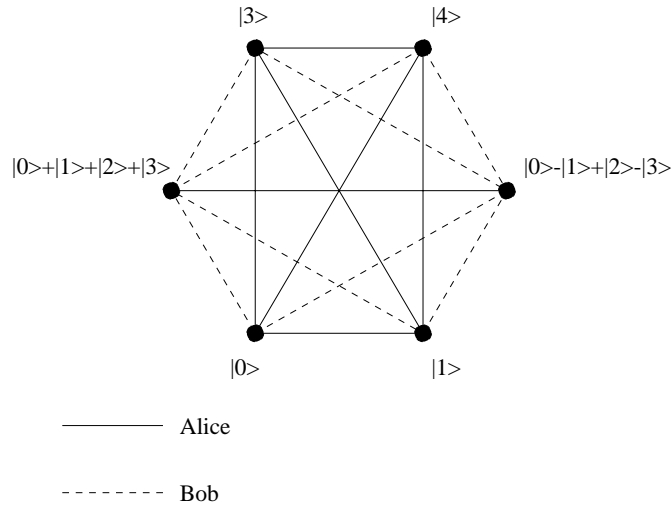


Figure 5.2: One step in a LOCC protocol, as viewed by Alice.

If the outcome is $\{|0\rangle, |1\rangle\}$ we know that Alice's part of the given state is one of

$$\begin{aligned}
 &|0\rangle, \\
 &|1\rangle, \\
 &\frac{1}{\sqrt{4}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle), \\
 &\frac{1}{\sqrt{4}}(|0\rangle - |1\rangle + |2\rangle - |3\rangle)..
 \end{aligned} \tag{5.3}$$

The states $\frac{1}{\sqrt{4}}(|0\rangle+|1\rangle+|2\rangle+|3\rangle)$ and $\frac{1}{\sqrt{4}}(|0\rangle-|1\rangle+|2\rangle-|3\rangle)$ collapse to $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ respectively, which means they are still orthogonal, and so the resulting orthogonality graph has colours on all edges. If, however, we only know the orthogonality graph and not the actual states, we will lose the information of the orthogonality of two states which are outside the subset onto which we project, leaving us with the graph of Figure 5.3, which cannot be *dissected*.

This is no proof that *dissection* does not characterise LOCC protocols based on von Neumann measurements, it is merely an example of the limitation of *dissection* stated above. We have neither shown that a situation like the one given here can ever occur, nor that, in the case such situation does occur, there is no alternative ways to *dissect* the orthogonality graph. In particular in Figure 5.2 Bob can make a measurement which distinguishes the two superposition states from the four simple states, and so in this case an alternative LOCC protocol can be found by *dissection*.

Because of this difficulty orthogonality graphs are only useful in cases where we want to prove distinguishability. This is useful to prove the inexistence of UPBs with certain orthogonality structures.

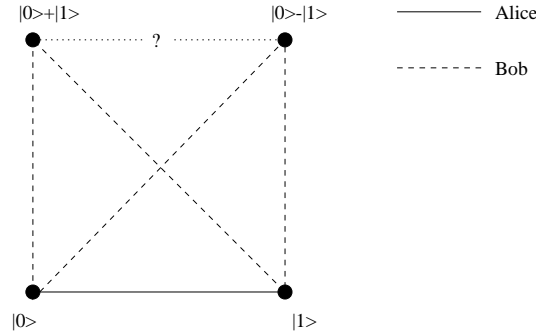


Figure 5.3: If we only know the orthogonality graph, we risk losing the orthogonality information about two projected states after a measurement.

5.3 Dependency Graphs

Another graph representation of PBs is presented by Alon and Lovász [AL00] and Lovász, Saks, and Schrijver [LSS89]. In [AL00] and [LSS89] these graphs are called orthogonality graphs, as the graphs we have studied so far. But to avoid confusion we denote the graphs presented in [AL00] as *dependency graphs* in this thesis.

In dependency graphs we only consider one of the parties at a time. This makes the definition more simple. Despite their simplicity dependency graphs are very powerful, and are the basis of many results.

The definition of dependency graphs is similar to that of orthogonality graphs. Instead of representing that two states are orthogonal, an edge in a dependency graph represent that two states are *not* orthogonal.

Definition 5.3.1 (Dependency Graph) [LSS89] *Let S be a set of vectors from a complex vector space, \mathbb{C}^d . Then the dependency graph of S is the graph $G = (S, E)$, where $E = \{(|\psi\rangle, |\phi\rangle) \in S \times S \mid \langle \psi | \phi \rangle \neq 0\}$.*

Thus a PB from an m -partite complex vector space has m dependency graphs, one for each party.

In the following we use graph-connectivity in the following form.

Definition 5.3.2 (Graph Connectivity) *Let $G = (V, E)$ be a graph. G is c -connected if and only if a subset $S_c \subseteq V$ of c vertices exists such that the graph $(V \setminus S_c, E)$ is not connected, and such that no subset of less than c vertices exists which separates G .*

The following theorem is what makes dependency graphs powerful.

Theorem 5.3.3 (LSS Bound on Spanning Subsets) [LSS89]

Let $G = (V, E)$ be a graph with n vertices. Then G is c -connected if and only if some set of n vectors, S , from \mathbb{C}^{n-c} can be assigned to the vertices V such that G is the dependency graph of S and such that every set of $n - c$ vectors from S are linearly independent.

This theorem together with the Counting Lemma (Lemma 5.1.1) guarantees the existence of UPBs with certain dependency graphs. If the dependency graph of every party, k , of a multipartite PB, S , has connectivity $n - d_k$ then, by Theorem 5.3.3 the states of S can be chosen such that any d_k states spans the complex vector space of the k th party. If n is big enough to guarantee that every time we split S into m subsets, at least one subset S_k has d_k states, then, by the Counting Lemma, S is unextendible. It is important to realise that even though at least one of the subsets, S_k , has rank d_k not necessarily all subsets of d_k states from the k th party has rank d_k .

Let us recapture this in a lemma.

Lemma 5.3.4 Let $G_k = (V_k, E_k), k = 1, \dots, m$, be graphs with each n vertices. If, for all $k = 1, \dots, m$, G_k is c_k -connected and $n \leq \frac{\sum_{k=1}^m c_k}{m-1} + 1$ then a UPB with n states exists in $\otimes_{k=1}^m \mathbb{C}^{n-c_k}$.

This lemma is a special case of a theorem by Alon and Lovász [AL00].

Proof. Let graphs $G_k = (V_k, E_k), k = 1, \dots, m$, of each n vertices be given, such that for all $k = 1, \dots, m$ G_k is c_k -connected, and $n \leq \frac{\sum_{k=1}^m c_k}{m-1} + 1$.

As for all $k = 1, \dots, m$ the graph G_k is c_k -connected and has n vertices, Theorem 5.3.3 implies that we can define sets $P_k = \{|\phi_{ik}\rangle \mid i = 1, \dots, n\}$ of vectors from $\mathbb{C}^{d_k}, d_k = n - c_k$, such that any d_k vectors from P_k spans \mathbb{C}^{d_k} .

Define the PB S as $S = \{|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik}\rangle \mid i = 1, \dots, n\}$.

Now we rewrite the condition $n \leq \frac{\sum_{k=1}^m c_k}{m-1} + 1$ as

$$\begin{aligned}
n &\leq \frac{\sum_{k=1}^m c_k}{m-1} + 1 \\
\Leftrightarrow n(m-1) &\leq \left(\sum_{k=1}^m c_k \right) + m - 1 \\
\Leftrightarrow mn - m - \left(\sum_{k=1}^m c_k \right) + 1 &\leq n \tag{5.4} \\
\Leftrightarrow \left(\sum_{k=1}^m n - c_k - 1 \right) + 1 &\leq n \\
\Leftrightarrow \left(\sum_{k=1}^m d_k - 1 \right) + 1 &\leq n.
\end{aligned}$$

To prove that S is unextendible consider any m disjoint subsets $S_1 \cup S_2 \cup \dots \cup S_m = S$. Because $n \geq (\sum_{k=1}^m d_k - 1) + 1$ at least one of the subsets S_k must have at least d_k states, and thus spans \mathbb{C}^{d_k} . This, by the Counting Lemma, implies that S is unextendible, which is what we required. \square

Where orthogonality graphs can be used to show the inexistence of UPBs, dependency graphs can be used to guarantee existence. Even though it might seem confusing to have two graph-representations of PBs, the reason why we keep both definitions is that Theorem 5.3.3 and Lemma 5.3.4 cannot be translated directly into statements about orthogonality graphs. To the best knowledge of the author, there is no direct relationship between the connectivity of a graph and the connectivity of the complementary graph.

Though we are not able to translate Theorem 5.3.3 and Lemma 5.3.4 directly into statements about orthogonality graphs we can still do almost without dependency graphs. From now on all uses of dependency graphs will be stated on terms of orthogonality graphs.

5.4 Symmetric UPBs and Alternating UPBs

As we saw in Chapter 5.2, orthogonality graphs does not seem to be a full characterisation of distinguishability. Neither do dependency graphs characterise UPBs, as the converse implication of Lemma 5.3.4 is not true. In Chapter 6 we shall see a UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$ with 8 states³ whose dependency graphs are *not* 4-connected. And in Chapter 7 we shall see several other examples of UPBs which demonstrates that the converse of Lemma 5.3.4 is not true.

Motivated by the fact that Lemma 5.3.4 can guarantee the existence of some UPBs the author has defined two classes of UPBs. These classes have a close connection to the Simple Lower Bound of the cardinality of UPBs which we examine in Chapter 6.

Before defining the two classes of UPBs let us take a look at a lemma which is of great use. This lemma is a generalised version of the Simple Lower Bound mentioned above.

Lemma 5.4.1 (Partition Lemma) *Let S be a BP with $\sum_{k=1}^m (d_k - 1) + 1$ states of the m -partite complex vector space $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$. Then S is a UPB if and only if for all $k = 1, \dots, m$ and all subsets, S' , of S of cardinality d_k the states of S' spans \mathbb{C}^{d_k} .*

Proof. Let $S = \{|\psi_i\rangle = \sum_{k=1}^m |\phi_{ik}\rangle \mid i = 1, \dots, n\}$ be a BP with $n = \sum_{k=1}^m (d_k - 1) + 1$ states of the m -partite complex vector space $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$

³In terms of Lemma 5.3.4 we have $n = 8$ and $c_1 = c_2 = 4$.

We first prove that if S is a UPB then for any party $l \in \{1, 2, \dots, m\}$ the states of any subset, S' , of S of cardinality d_l spans \mathbb{C}^{d_l} .

Let l be given, and let $S_l \subset S$ be a subset of S of cardinality d_l . As S consists of $n = \sum_{k=1}^m (d_k - 1) + 1$ states, $S \setminus S_l$ has

$$\begin{aligned} n - d_l &= \sum_{k=1}^m (d_k - 1) + 1 - d_l \\ &= \sum_{\substack{k=1 \\ k \neq l}}^m (d_k - 1) \end{aligned} \tag{5.5}$$

states. As $d_k \geq 1$ for all k we can define $m - 1$ disjoint nonempty subsets, $S_1, \dots, S_{l-1}, S_{l+1}, \dots, S_m$, such that for all $k \in \{1, \dots, l-1, l+1, \dots, m\}$, S_k has $d_k - 1$ states, S_k is disjoint to S_l , and $S = S_1 \cup \dots \cup S_{l-1} \cup S_l \cup S_{l+1} \cup \dots \cup S_m$. As S is unextendible the Counting Lemma states that for all m disjoint subsets the local rank of at least one of the subsets is greater than or equal to the local dimension. In particular we have that for at least one of the subsets $S_1, \dots, S_{l-1}, S_l, S_{l+1}, \dots, S_m$, S_k say, $\text{rank}(\{|\phi_{ik}\rangle \mid |\psi_i\rangle \in S_k\}) \geq d_k$. As the subsets S_1, \dots, S_{l-1} , and S_{l+1}, \dots, S_m all have less states than the dimension of their local party, S_l has to be the subset with $\text{rank}(\{|\phi_{il}\rangle \mid |\psi_i\rangle \in S_l\}) \geq d_l$, which is what we required.

Now we prove that if, for all subsets S_k of S of cardinality d_k , the states of S_k spans \mathbb{C}^{d_k} then S is unextendible.

Assume that for all subsets S_k of S of cardinality d_k , the states of S_k spans \mathbb{C}^{d_k} . Let $S_1 \cup \dots \cup S_m = S$ be any m disjoint subsets of S . As S consists of $n = \sum_{k=1}^m (d_k - 1) + 1$ states at least one of the subsets, S_l say, has d_l or more states. Then, by assumption, d_l of the states of S_l spans \mathbb{C}^{d_l} and thus, by the Counting Lemma, S must be unextendible. \square

The Partition Lemma tells us about the structure of UPBs with a certain cardinality. Consider a UPB from $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ with $\sum_{k=1}^m (d_k - 1) + 1$ states. The Partition Lemma then tells us that whenever the k th party considers k random states of his part of the UPB these states span the whole of his subsystem \mathbb{C}^{d_k} . This give us a symmetry of this type of UPBs. And since the Partition Lemma is a bijection it also give us a way to verify that a PB of this cardinality is unextendible.

Definition 5.4.2 (Symmetric UPB) *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. An UPB, S , of \mathbb{C}^d is a symmetric UPB if and only if for all $k = 1, \dots, m$ and all subsets S' of S of cardinality d_k the states of the k th party of S' spans \mathbb{C}^{d_k} .*

Symmetric UPBs enable us able to translate part of the results we have on dependency graphs to similar results on orthogonality graphs.

Lemma 5.4.3 *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. And let S be a symmetric UPB of \mathbb{C}^d with orthogonality graph G . Then any vertex of G is connected to exactly $(d_k - 1)$ other vertices by colour k , for $k = 1, \dots, m$.*

Proof. Let S be a given symmetric UPB with n states and with orthogonality graph G , such that G is c -connected.

By definition of symmetric UPBs any d_k states of S span \mathbb{C}^{d_k} on the k th party. Thus by Theorem 5.3.3 the dependency graph of S is $(n - d_k)$ -connected.

As the dependency graph of S is $(n - d_k)$ -connected all vertices of the dependency graph are connected to at least $(n - d_k)$ other vertices. And thus a vertex of the orthogonality graph of the k th party cannot be connected to more than $(n - 1) - (n - d_k) = (d_k - 1)$ other states. We write

$$\text{degree}_k(v) \leq d_k - 1 \quad (5.6)$$

Furthermore, by definition, any vertex v of G is connected to all other $n - 1 = \sum_{k=1}^m (d_k - 1)$ vertices with at least one colour. So

$$\sum_{k=1}^m \text{degree}_k(v) \geq \sum_{k=1}^m (d_k - 1) \quad (5.7)$$

Comparing the two inequalities gives us that each vertex of G_k must have degree exactly $d_k - 1$. \square

If S is a UPB and we can find some subsets S_1, \dots, S_m such that one of the subsets S_k has local rank less than the dimension of the local system, \mathbb{C}^{d_k} , then the Counting Lemma implies that there must be some other subset $S_{k'}$ for which the local rank is equal to or greater than the dimension of the local system $\mathbb{C}^{d_{k'}}$. One might say the job of blocking for a potential orthogonal product state alternates between the parties.

Any UPB which is not symmetric is alternating, but let us write out the negation explicitly.

Definition 5.4.4 (Alternating UPB) *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. An UPB, S , of \mathbb{C}^d is an alternating UPB if and only if for some $k \in \{1, \dots, m\}$ some subset S' of S of cardinality d_k exists such that the states of the k th party do not span \mathbb{C}^{d_k} .*

The **Tiles** UPB on page 20 is an example of a symmetric UPB. The **GenTiles1** and **GenTiles2** UPBs in Chapter 7 are examples of alternating UPBs.

Chapter 6

Bounds on Cardinality

In this chapter we present results achieved with respect to the possible sizes of UPBs.

6.1 Lower Bounds

We start out by proving that no UPBs exists in a bipartite complex vector space if the vector space of one of the parties has dimension 2.

Lemma 6.1.1 (No UPB in $\mathbb{C}^2 \otimes \mathbb{C}^d$) [BDM⁺98] *No unextendible product basis exists in a bipartite complex vector space, $\mathbb{C}^d = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, where either $d_1 = 2$ or $d_2 = 2$.*

In this thesis we give an alternative proof to this lemma, using orthogonality graphs. The LOCC protocol used in this proof is the same as the one used by Bennett, DiVincenzo, Mor, Shor, Smolin, and Terhal in [BDM⁺98], but in [BDM⁺98] orthogonality graphs are not used as an aid.

Proof. Let S be a PB in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. And let $G = (V, E, c)$ be the orthogonality graph of S . Let some state of S be given which is shared between two parties, Alice and Bob. We prove that an LOCC protocol exists by which Alice and Bob can decide which state they share, thus proving that S cannot be a UPB.

Without loss of generality say that the dimension of Alice's local system is $d_A = 2$. Denote by C_1, \dots, C_l the connected components of the orthogonality graph of Alice, G_A . As the states of one of these connected components have to be mutual orthogonal, and as the dimension of the Alice's complex vector space is two, there can only be four vectors in each connected component. As we do not distinguish states which differs by a global scalar factor each connected component consists of at most two states.

As no vertex from C_i is connected to vertices from C_j , for $i \neq j$, no state from C_i is orthogonal to any state of C_j . But then all states of C_i must be orthogonal

to all states of C_j in Bobs vector space. Bob can then make a von Neumann measurement which distinguishes the sets C_1, \dots, C_l without destroying the states.

After measurement Bob informs Alice of the outcome, a say. Alice now knows the given state is one of the states of C_a , since C_a at most contains two states which are known to be mutually orthogonal in Alice's vector space, thus Alice can distinguish between these states. Now Alice and Bob have identified the given state, which was our goal. \square

From the Counting Lemma (Lemma 5.1.1) we can derive a lower bound on the cardinality of any UPB.

Lemma 6.1.2 (Simple Lower Bound) [BDM⁺98] *Let S be an unextendible product basis of an m -partite complex vector space $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$. Then S consists of at least*

$$n \geq \sum_{k=1}^m (d_k - 1) + 1 \quad (6.1)$$

product states.

Proof. Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space.

Assume there is a UPB S of \mathbb{C}^d with less than $\sum_{k=1}^m (d_k - 1) + 1$ states. Then m disjoint subsets, $S_1 \cup S_2 \cup \dots \cup S_m = S$, of S exists such that $|S_k| \leq (d_k - 1)$. This implies that the local rank of all the subsets S_k , $k = 1, \dots, m$ is less than d_k , which, by the Counting Lemma, implies that S is extendible, contradicting the assumption that S is a UPB. \square

The Simple Lower Bound is, however, not tight. In some vector spaces no UPB exists which achieves the cardinality of the Simple Lower Bound. In [AL00] Alon and Lovász give a criterion for the existence of UPBs which achieves the cardinality of the Simple Lower Bound.

Theorem 6.1.3 (Alon-Lovász Criterion) [AL00] *For all $m \geq 2$ and all m -partite complex vector space $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$, there exists an unextendible product basis of \mathbb{C}^d of cardinality $\sum_{k=1}^m (d_k - 1) + 1$ if and only if none of the following is true*

- $m = 2$ and $2 \in \{d_1, d_2\}$.
- $\sum_{k=1}^m (d_k - 1) + 1$ is odd and at least one of d_k is even.

Below we state and prove two smaller lemmas which together proves the only-if part of Theorem 6.1.3.

Note, however, that the first requirement of Theorem 6.1.3 follows from Lemma 6.1.1.

The following lemma states that no alternating UPB achieves the Simple Lower Bound.

Lemma 6.1.4 *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. Then there exists no alternating UPB of cardinality $n = \sum_{k=1}^m (d_k - 1) + 1$ in \mathbb{C}^d .*

Proof. Let S be a UPB in \mathbb{C}^d with $n = \sum_{k=1}^m (d_k - 1) + 1$ states. Assume S is alternating.

By the Partition Lemma (Lemma 5.4.1) all subsets of S with d_k states has to locally span \mathbb{C}^{d_k} , but this by definition of alternating UPBs, contradicts the assumption that S is alternating. \square

So if we are to find a UPB which achieves the Simple Lower Bound, it has to be a symmetric UPB. But when does such a UPB exist?

Lemma 6.1.5 [AL00] *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. Then if $n = \sum_{k=1}^m (d_k - 1) + 1$ is odd and at least one of $d_k, k = 1, \dots, m$ is even there exist no symmetric UPB of cardinality n in \mathbb{C}^d .*

Proof. Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space, where at least one of $d_k, k = 1, \dots, m$ is even.

Assume S is a symmetric UPB of \mathbb{C}^d with $n = \sum_{k=1}^m (d_k - 1) + 1$, such that n is odd. And let G be the orthogonality graph of S with vertices $\{v_1, \dots, v_n\}$.

By Lemma 5.4.3 each vertex of the orthogonality graph of S has degree exactly $d_k - 1$ in the orthogonality graph of the k th party. Let l be the party whom has an even dimension local vector space. If we sum the degree of all vertices of the orthogonality graph of the l th party we get

$$\begin{aligned} S_l &= \sum_{i=1}^n \text{degree}_l(v_i) \\ &= n(d_l - 1), \end{aligned} \tag{6.2}$$

which is an odd number. Each time one edge is removed from the orthogonality graph of the l th party the sum S_l decrease by 2. When all edges are removed $S_l = 0$, and so S_l must be even. But from Equation 6.2 we know that S_l is odd, thus we have a contradiction to the assumption that S is a symmetric UPB. \square

The Lemmas 6.1.1, 6.1.4, and 6.1.5 together prove the only-if part of the Alon-Lovász Criterion.

When distinguishing between alternating and symmetric UPBs, we can analyse the lower bounds even further. The following theorem gives a tight lower (and upper) bound for the symmetric UPBs.

The following theorem is one of the main results in this thesis.

Theorem 6.1.6 *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space, and let S be an unextendible product basis of \mathbb{C}^d . Then S is symmetric if and only if S has cardinality $n = \sum_{k=1}^m (d_k - 1) + 1$.*

Proof. Let S be a UPB with $n = \sum_{k=1}^m (d_k - 1) + 1$ states then, by Lemma 6.1.4, S is a symmetric UPB.

Let S be a symmetric UPB of cardinality $n = \sum_{k=1}^m (d_k - 1) + 1 + s$ in \mathbb{C}^d and with orthogonality graph G . We prove that $s = 0$.

As S is symmetric Lemma 5.4.3 implies that all vertices of the local orthogonality graph G_k is connected to exactly $d_k - 1$ other states. Thus for any vertex v

$$\begin{aligned} \sum_{k=1}^m \text{degree}_k(v) &= \sum_{k=1}^m (d_k - 1) \\ &= n - 1 - s. \end{aligned} \tag{6.3}$$

Furthermore a vertex v has to be orthogonal to all other $n - 1$ vertices in at least one party. And thus

$$\sum_{k=1}^m \text{degree}_k(v) \geq n - 1 \tag{6.4}$$

Comparing Equation 6.3 and Inequality 6.4 we conclude that $s = 0$, and thus S has cardinality $\sum_{k=1}^m (d_k - 1) + 1$ as required. \square

Theorem 6.1.6 states that all UPBs achieving the Simple Lower Bound are symmetric, and all other UPBs are alternating.

The Simple Lower Bound is based on the Counting Lemma, which is also the central motivation in defining symmetric UPBs. Therefore it come as no surprise that UPBs which achieves the Simple Lower Bound are the symmetric UPBs.

To summarise, Table 6.1 shows the known lower bound for complex vector spaces of dimension less than 35, and the cardinality of the smallest known UPBs.

6.2 A Lower Bound UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$

$\mathbb{C}^4 \otimes \mathbb{C}^4$ is interesting because it is the smallest bipartite vector space for which we know that no symmetric UPB exists. The author has therefore thrived to find a minimal (alternating) UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$.

A minimal alternating UPB in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ has been found by David DiVincenzo [DT02]. In this thesis we shall refer to this UPB as the **Min2x2x2x2** UPB.

In cooperation with Peter Høyer and Jan Neerbek [HN01] a 6 state PB was found which seemed promising. Later this was extended to a 8 state UPB in cooperation with Peter Høyer.

QuadRes is a known alternating UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$ of cardinality 9. We shall see this UPB in Chapter 7.2, but here we present an even smaller UPB of

Dimension	Lower bound	Smallest known UPB	UPB name
$\mathbb{C}^9 = \mathbb{C}^3 \otimes \mathbb{C}^3$	5	5	Tiles, Pyramid
$\mathbb{C}^{12} = \mathbb{C}^3 \otimes \mathbb{C}^4$	6	7	GenTiles2
$\mathbb{C}^{15} = \mathbb{C}^3 \otimes \mathbb{C}^5$	7	10	GenTiles2
$\mathbb{C}^{18} = \mathbb{C}^3 \otimes \mathbb{C}^6$	8	13	GenTiles2
$\mathbb{C}^{21} = \mathbb{C}^3 \otimes \mathbb{C}^7$	9	16	GenTiles2
$\mathbb{C}^{24} = \mathbb{C}^3 \otimes \mathbb{C}^8$	10	19	GenTiles2
$\mathbb{C}^{27} = \mathbb{C}^3 \otimes \mathbb{C}^9$	11	22	GenTiles2
$\mathbb{C}^{30} = \mathbb{C}^3 \otimes \mathbb{C}^{10}$	12	25	GenTiles2
$\mathbb{C}^{33} = \mathbb{C}^3 \otimes \mathbb{C}^{11}$	13	28	GenTiles2
$\mathbb{C}^{16} = \mathbb{C}^4 \otimes \mathbb{C}^4$	> 7	8	Min4x4
$\mathbb{C}^{20} = \mathbb{C}^4 \otimes \mathbb{C}^5$	8	13	GenTiles2
$\mathbb{C}^{24} = \mathbb{C}^4 \otimes \mathbb{C}^6$	> 9	17	GenTiles2
$\mathbb{C}^{28} = \mathbb{C}^4 \otimes \mathbb{C}^7$	10	21	GenTiles2
$\mathbb{C}^{32} = \mathbb{C}^4 \otimes \mathbb{C}^8$	> 11	25	GenTiles2
$\mathbb{C}^{25} = \mathbb{C}^5 \otimes \mathbb{C}^5$	9	16	GenTiles1
$\mathbb{C}^{30} = \mathbb{C}^5 \otimes \mathbb{C}^6$	10	21	GenTiles2
$\mathbb{C}^{35} = \mathbb{C}^5 \otimes \mathbb{C}^7$	11	26	GenTiles2
$\mathbb{C}^8 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$	4	4	GenShifts
$\mathbb{C}^{12} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^3$	> 5	-	-
$\mathbb{C}^{16} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^4$	6	-	-
$\mathbb{C}^{20} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^5$	> 7	-	-
$\mathbb{C}^{24} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^6$	8	-	-
$\mathbb{C}^{28} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^7$	> 9	-	-
$\mathbb{C}^{32} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^8$	10	-	-
$\mathbb{C}^{18} = \mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$	6	-	-
$\mathbb{C}^{24} = \mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^4$	> 7	-	-
$\mathbb{C}^{30} = \mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^5$	8	-	-
$\mathbb{C}^{32} = \mathbb{C}^2 \otimes \mathbb{C}^4 \otimes \mathbb{C}^4$	> 7	-	-
$\mathbb{C}^{27} = \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$	7	7	Sept
$\mathbb{C}^{16} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$	> 5	6	Min2x2x2x2
$\mathbb{C}^{24} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^3$	6	-	-
$\mathbb{C}^{32} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^4$	> 7	-	-
$\mathbb{C}^{32} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$	6	6	GenShifts

Figure 6.1: Lower bounds for complex vector spaces of dimension at most 35. Vector spaces not listed here has no UPBs.

cardinality 8. By the Simple Lower Bound the smallest possible UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$ has cardinality 7, but as 7 is odd, the Alon-Lovász Criterion states that no UPB of cardinality exactly 7 exists. Thus a UPB in $\mathbb{C}^4 \otimes \mathbb{C}^4$ of cardinality 8 is minimal.

The states of the **Min4x4** UPB are the following

$$\begin{aligned}
 |\psi_0\rangle &= |0\rangle - 3|1\rangle + |2\rangle + |3\rangle \otimes |1\rangle - (3 + \sqrt{2})|2\rangle - (1 + \sqrt{2})|3\rangle \\
 |\psi_1\rangle &= |0\rangle \otimes |0\rangle \\
 |\psi_2\rangle &= |1\rangle + 2|2\rangle + |3\rangle \otimes |0\rangle + (\sqrt{2} - 1)|2\rangle + |3\rangle \\
 |\psi_3\rangle &= |0\rangle - |3\rangle \otimes |1\rangle \\
 |\psi_4\rangle &= |1\rangle \otimes -|0\rangle + (1 + \sqrt{2})|1\rangle + |3\rangle \\
 |\psi_5\rangle &= 3|0\rangle + |1\rangle - |2\rangle + |3\rangle \otimes |2\rangle \\
 |\psi_6\rangle &= |1\rangle + |2\rangle \otimes |0\rangle + |1\rangle + |2\rangle - \sqrt{2}|3\rangle \\
 |\psi_7\rangle &= |2\rangle \otimes -|0\rangle + (1 + \sqrt{2})|1\rangle + |3\rangle.
 \end{aligned} \tag{6.5}$$

For clarity we have omitted proper normalisation factors. They are not explicitly needed below.

The orthogonality graph of the **Min4x4** UPB can be seen in Figure 6.2.

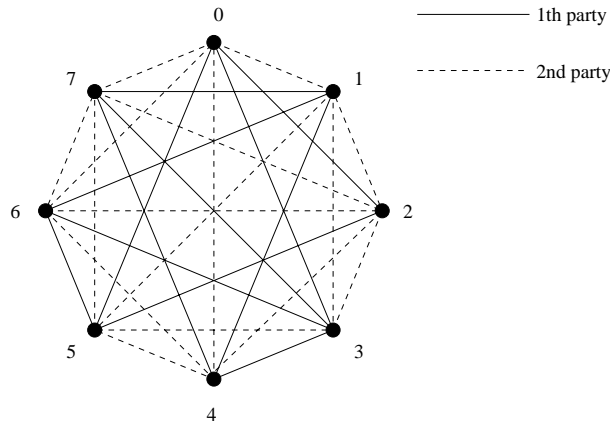


Figure 6.2: Orthogonality graph for the **Min4x4** UPB

In order to prove that **Min4x4** is unextendible the Counting Lemma (page 25) states that for all possible partitions of the states we have to show that at least one of the partitions spans the vector space of its party.

Every time we split the 8 states up in one set per party one of the parties has at least 4 states. To verify that 4 states of \mathbb{C}^4 spans \mathbb{C}^4 we can construct a 4×4 matrix with the states as columns, and calculate the determinant. If the determinant is nonzero the states span \mathbb{C}^4 [Bea95].

Whenever 4 states do not span one of the local vector spaces in **Min4x4** there are 4 other states which span the other local vector space. The 1680 determinants can be verified by a computer to see this is true.

6.3 Graph Characterisation of Minimal UPBs

Theorem 6.1.6 tells us that symmetric UPBs characterise the Simple Lower Bound of Lemma 6.1.2. This can be extended to a graph characterisation, as the orthogonality graphs of symmetric UPBs have special properties.

Theorem 6.3.1 (Orthogonality Graphs of Symmetric UPBs)

Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. And let S be an unextendible product basis of \mathbb{C}^d with orthogonality graph G . Then the following holds if and only if S is symmetric

- All edges of G have exactly one colour.
- All vertices of G_k have degree $d_k - 1$.

Proof. We first prove that all symmetric UPBs have the two properties.

Let S be a symmetric UPB of $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$.

By Theorem 6.1.6 S has $n = \sum_{k=1}^m (d_k - 1) + 1$ states.

By Lemma 5.4.3 all vertices of G_k have degree exactly $d_k - 1$. Furthermore each vertex of G has to be connected to all other $n - 1 = \sum_{k=1}^m (d_k - 1)$ vertices, and thus no edge can have more than one colour.

We now prove that any UPB with the two properties is symmetric.

Let S be a UPB of $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ with orthogonality graph G , such that G satisfies the two properties.

As each vertex by definition is connected to all other vertices by at least one colour, and as each edge of G has exactly one colour S must have cardinality $\sum_{k=1}^m (d_k - 1) + 1$. Then, by Theorem 6.1.6, S is symmetric. \square

Theorem 6.3.1 gives us a method to verify whether a UPB is symmetric (and thus minimal). First verify that no edge has more than one colour. Then check that for all colours all vertices have same degree.

6.4 Upper Bounds

Little work has been done on the upper bounds of the cardinality of UPBs. The only previously known result by Horodecki, Smolin, Terhal, and Thapliyal [HSTT99] originates from a lower bound on bound entangled states. Recall from Section 4.2 that every UPB has a bound entangled state in the orthogonal complement to the subspace spanned by the UPB.

Lemma 6.4.1 (No Rank Two Bound Entangled State) [HSTT99] *All bipartite bound entangled states are mixtures of at least three states.*

No bound entangled state of rank three is believed to exist neither, but it has not yet been proven [HSTT99].

Theorem 6.4.2 [HSTT99] *Let S be an unextendible product basis of a bipartite complex vector space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$. Then S consists of at most*

$$n \leq d_1 d_2 - 3 \tag{6.6}$$

product states.

Proof. Assume that S is a UPB from $\mathbb{C}^d = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ with n states where $n > d_1 d_2 - 3$. As all n states are orthogonal the subspace $\mathbb{C}_S^d \subset \mathbb{C}^d$ spanned by the vectors of S has dimension larger than $d_1 d_2 - 3$. Thus the orthogonal complement has dimension at most 2. As S is a UPB Theorem 4.2.1 states that the uniform mixture of any basis of the orthogonal complement is bound entangled. But this mixture only consists of 1 or 2 states which contradicts Lemma 6.4.1. Thus S cannot be a UPB. \square

The bound of Theorem 6.4.2 is the best known upper bound for alternating UPBs. But Theorem 6.1.6 is both a lower and upper bound on the cardinality of symmetric UPBs.

Chapter 7

Generic UPBs

In this chapter we present families of UPBs which we call generic UPB. A generic UPB is a parameterised UPB which is defined for vector spaces of different dimensions or which can be defined for several number of parties. All the generic UPBs presented in this chapter are constructed by DiVincenzo, Mor, Shor, Smolin, and Terhal [DMS⁺99].

Each section in this chapter is divided into five parts. First we motivate the UPB by explaining the idea which lead to its creation, this facilitates understanding the constructions. Then we define the UPB. Afterwards we prove that the construction is indeed a UPB. Then we shall see an example of an actual UPB, and finally we mention whether the UPB has any particularly interesting properties.

7.1 GenShifts

Motivation

GenShifts is a generic UPB defined for any odd number of parties (except 1), each holding a 2 dimensional complex vector space.

The idea is to define a product state in $\otimes_{k=1}^{2m-1} \mathbb{C}^2$, where all parties hold different states¹, such that shifting the states one party to the left makes the original state and the shifted state orthogonal on the $k_{(1,2)}$ th party, for some $k_{(1,2)} = 1, \dots, 2m - 1$. When shifting i parties, the original state and the shifted state are orthogonal on the $k_{(1,i+1)}$ th party. In this way, by symmetry, all states are orthogonal. And as any two states of the k th party are different (the original state shifted 1 through k places), they span \mathbb{C}^2 which, by the Counting Lemma, implies that we have a UPB.

¹Recall that we cannot tell the difference between states which differs on a global phase factor only, so two such states are considered identical (see page 2.1.1).

Definition

For any integer m , **GenShifts** is defined on the $(2m - 1)$ -partite complex vector space $\otimes_{k=1}^{2m-1} \mathbb{C}^2$. **GenShifts** consists of $2m$ states, $n = 2m$.

GenShifts	
Parameters	$m \in \mathbb{N}$ $m \geq 2$
Vector Space	$\otimes_{k=1}^{2m-1} \mathbb{C}^2$
Parties	$2m - 1$
Cardinality	$2m$
Minimal	Yes
Originally from	[DMS ⁺ 99]

Figure 7.1: Parameters for the **GenShifts** UPB

The states are

$$\begin{aligned} |\psi_i\rangle &= \otimes_{k=1}^{2m-1} |\phi_{k+i \bmod 2m-1}\rangle, \\ |\psi_{2m}\rangle &= \otimes_{k=1}^{2m-1} |0\rangle, \end{aligned} \quad (7.1)$$

where $i = 1, \dots, 2m - 2$ and for all $a, b = 1, \dots, 2m - 1$, $|\phi_0\rangle = |1\rangle$, $|\phi_a\rangle \neq |\phi_b\rangle$ for $a \neq b$ and $|\phi_a\rangle \perp |\phi_{-a \bmod 2m-1}\rangle$.

Proof

Lemma 7.1.1 *The states of **GenShifts** form a UPB.*

The proof given here is different from the one given in [DMS⁺99].

Proof. We first prove that all states are orthogonal. Given a state $|\psi_i\rangle$, $i = 1, \dots, 2m - 1$, $|\psi_i\rangle$ is orthogonal to the state $|\psi_{2m}\rangle$ on the $(2m - 1 - i)$ th party, as $|\phi_{i+2m-1-i \bmod 2m-1}\rangle = |\phi_0\rangle = |1\rangle$, and $|\psi_{2m}\rangle = \otimes_{j=1}^{2m-1} |0\rangle$.

Let two states $|\psi_i\rangle$ and $|\psi_j\rangle$, $i, j \in \{1, \dots, 2m - 1\}$ be given. Without loss of generality let $i < j$. Define $p = (m(j - i) - j)$. Then $|\psi_i\rangle$ and $|\psi_j\rangle$ are orthogonal on the p th party, since the p th party of $|\psi_i\rangle$, $|\phi_{i+p \bmod 2m-1}\rangle$, is orthogonal to $|\phi_{-(i+p) \bmod 2m-1}\rangle$, and

$$\begin{aligned} |\phi_{-(i+p) \bmod 2m-1}\rangle &= |\phi_{-i-(m(j-i)-j) \bmod 2m-1}\rangle \\ &= |\phi_{-m(j-i)+(j-i) \bmod 2m-1}\rangle \\ &= |\phi_{(1-m)(j-i) \bmod 2m-1}\rangle \\ &= |\phi_{-(m-1)(j-i) \bmod 2m-1}\rangle \\ &= |\phi_{m(j-i) \bmod 2m-1}\rangle \\ &= |\phi_{j+p \bmod 2m-1}\rangle, \end{aligned} \quad (7.2)$$

which is the p th party of the state $|\psi_j\rangle$. This proves that **GenShifts** is a PB. The second to last equation follows from the fact that $-mx \equiv (2m - 1 - m)x \equiv (m - 1)x \pmod{2m - 1}$ for any m and x .

We now prove that **GenShifts** is unextendible. Let $S_1 \cup S_2 \cup \dots \cup S_{2m-1} = S$ be any $2m - 1$ given disjoint subsets of **GenShifts**. As **GenShifts** consists of $2m$ states at least one of the subsets S_k must contain 2 or more states. Then, as no party repeats states the states of this set has rank 2 on the k th party, which by the Counting Lemma (Lemma 5.1.1) implies that **GenShifts** is unextendible.

Thus **GenShifts** is a UPB. \square

Example

The following is the **GenShifts** for $m = 2$. This UPB is called **Shifts** and is introduced by Bennett, DiVincenzo, Mor, Shor, Smolin, and Terhal in [BDM⁺98].

$$\begin{aligned} |\psi_0\rangle &= |\phi\rangle \otimes |\phi^\perp\rangle \otimes |1\rangle, \\ |\psi_1\rangle &= |\phi^\perp\rangle \otimes |1\rangle \otimes |\phi\rangle, \\ |\psi_2\rangle &= |1\rangle \otimes |\phi\rangle \otimes |\phi^\perp\rangle, \\ |\psi_3\rangle &= |0\rangle \otimes |0\rangle \otimes |0\rangle, \end{aligned} \tag{7.3}$$

where $|\phi\rangle$ is an arbitrary state not equal to $|0\rangle$ nor $|1\rangle$. $|\phi\rangle$ could for instance be chosen as the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Properties

By definition of UPBs (Definition 4.1.3) any state in the orthogonal complement to the subspace spanned by a UPB is entangled. In the case of the **Shifts** UPB this entanglement has the curious property that it is not two-way entangled.

A state from the orthogonal complement to **Shifts** shared by three parties has entanglement between the three parties. That is: A measurement done by one of the parties alter the probabilities of outcome of subsequent measurements done by the other parties.

If Alice and Bob share one of these states, such that Alice holds two parts of the state and Bob holds the remaining part then this bipartite state is separable [BDM⁺98]. That is: If a measurement is done on one part of the state it does not alter the probabilities of outcome of subsequent measurements done on both the remaining parts simultaneously and vice versa.

7.2 GenTiles1

Motivation

GenTiles1 is a UPB defined for all bipartite complex vector spaces $\mathbb{C}^d \otimes \mathbb{C}^d$, where d is an even number greater than 4.

Though the name might suggest it the **Tiles** UPB from page 20 is not a **GenTiles1** UPB. But the name is not a coincidence as **Tiles** and **GenTiles1** are based on the same idea.

In [BDF⁺98] Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, and Wootters use a graphical representation of bipartite quantum states. When drawing a state from $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ one draws a $d_1 \times d_2$ grid. Columns represent the basis states from the first party, and the rows represent the basis states from the second party. A state which is the tensor product of two basis states, say $|a\rangle \otimes |b\rangle$ is drawn as a tile in the grid (a, b) . If one part of a state is a superposition, the tile covers more grids. In Figure 7.2 the tile representation of the 4 states

$$\begin{aligned}
 |\psi_1\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\
 |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle, \\
 |\psi_3\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\
 |\psi_4\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle,
 \end{aligned} \tag{7.4}$$

are shown. These states are the first four states of the **Tiles** UPB. The last state $|\psi_5\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \otimes \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$ would cover the whole figure, so it is not drawn explicitly.

When considering the following observations, the tiles representations can aid in constructing a UPB.

- Two tiles which has an overlap of just one grid cannot be orthogonal.
- Two tiles which overlap in several grids should be orthogonal in the overlapping subspace for at least one of the parties.
- If a tiles drawing has an empty grid, a product state can be found which is orthogonal to all existing states. Thus Figure 7.2 does not represent a UPB.

The tiles representation of **GenTiles1** for $\mathbb{C}^6 \otimes \mathbb{C}^6$ can be seen in Figure 7.3. The idea is that it is not possible to add a tile without having a 1,2 or 3 grid overlap with existing tiles. If a one grid overlap occurs, the two states are not

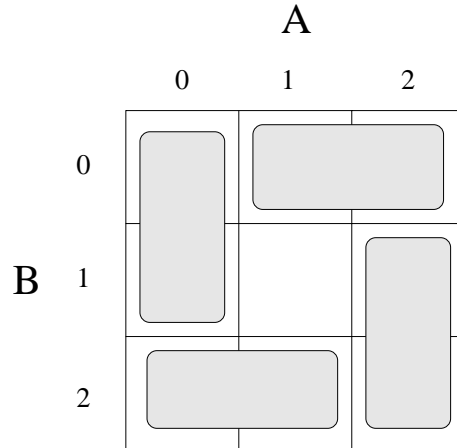


Figure 7.2: The tiles representation of the four first states of **Tiles** [DMS⁺99]. This figure is printed with permission from David DiVincenzo.

orthogonal. Now we just have to define the states corresponding to 1×3 grids in a way that no 2 or 3 overlap can be made orthogonal. Notice that one tile might represent several states. In particular the tiles of figure 7.3 each represents 2 states. The 2 states represented by one tile corresponds to the 2 last rows of the Fourier Transform F_3 , defined on page 65. And finally a 6×6 state, corresponding to the last state of the **Tiles** UPB, is added. This state, called the stopper, is an equal superposition of the 6 basis states of each party, thus corresponding to the first row of F_3 on the overlap with any of the 1×3 states. The properties of F_3 guarantees that 2 overlapping states plus the stopper are orthogonal in any subspace of the 3 dimensional space they span. So no new 2 overlap can be made orthogonal to these 3 states.

Definition

For any even integer $d > 4$, **GenTiles1** is defined for the complex vector space $\mathbb{C}^d \otimes \mathbb{C}^d$, and consists of $d^2 - 2d + 1$ states.

For a given d the states of **GenTiles1** are

$$\begin{aligned}
 |V_{ij}\rangle &= |\phi_j\rangle \otimes \frac{1}{\sqrt{d/2}} \sum_{s=0}^{d/2-1} \omega^{si} |\phi_{s+j+1 \bmod d}\rangle, \\
 |H_{ij}\rangle &= \frac{1}{\sqrt{d/2}} \sum_{s=0}^{d/2-1} \omega^{si} |\phi_{s+j \bmod d}\rangle \otimes |\phi_j\rangle, \\
 |F\rangle &= \frac{1}{d} \sum_{s=0}^{d-1} |\phi_s\rangle \otimes \frac{1}{d} \sum_{s=0}^{d-1} |\phi_s\rangle,
 \end{aligned} \tag{7.5}$$

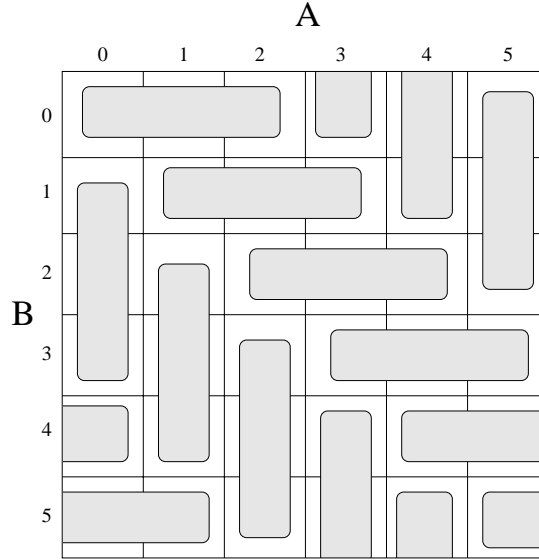


Figure 7.3: The tiles representation of **GenTiles1** for $\mathbb{C}^6 \otimes \mathbb{C}^6$ [DMS⁺99]. This figure is printed with permission from David DiVincenzo.

GenTiles1	
Parameters	$d \in \mathbb{N}$ $d \geq 4$, and d even.
Vector Space	$\mathbb{C}^d \otimes \mathbb{C}^d$
Parties	2
Cardinality	$d^2 - 2d + 1$
Minimal	No
Originally from	[DMS ⁺ 99]

Figure 7.4: Parameters for the **GenTiles1** UPB

where $i = 1, 2, \dots, d/2 - 1, j = 0, 1, \dots, d - 1, \omega = e^{i4\pi/d}$, and $|\phi_a\rangle$ are states such that for $a \neq b$ we have $\langle \phi_a | \phi_b \rangle = 0$.

There are $\frac{d^2}{2} - d$ states of each vertical states, $|V_{mk}\rangle$, and horizontal states, $|H_{mk}\rangle$.

Proof

In [DMS⁺99] no proof that **GenTiles1** is a UPB is given. But in [DT00] David DiVincenzo and Barbara Terhal give a cumbersome proof by contradiction. To prove the unextendibility of **GenTiles1** the determinant method used to prove unextendibility of the **Min4x4** UPB on page 46 can be used.

Example

The smallest **GenTiles1** UPB is obtained with the parameter $d = 4$, and has the following 9 states

$$\begin{aligned}
|V_{10}\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\
|V_{11}\rangle &= |1\rangle \otimes \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle), \\
|V_{12}\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|3\rangle - |0\rangle), \\
|V_{13}\rangle &= |3\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\
|H_{10}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle, \\
|H_{11}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |1\rangle, \\
|H_{12}\rangle &= \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle) \otimes |2\rangle, \\
|H_{13}\rangle &= \frac{1}{\sqrt{2}}(|3\rangle - |0\rangle) \otimes |3\rangle, \\
|F\rangle &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) \otimes \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle),
\end{aligned} \tag{7.6}$$

where $|\phi_i\rangle$ from the definitions is set to $|\phi_i\rangle = |i\rangle$.

Properties

7.3 GenTiles2

Motivation

GenShifts1 is only defined for bipartite vector spaces where the two parties have the same dimension. The **GenTiles2** UPB is an asymmetrical variation of the **Tiles** type of UPBs. **GenTiles2** is defined for $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, for any $d_1, d_2 \in \mathbb{N}$ where $d_1 \geq 3$, $d_2 > 3$, and $d_1 \leq d_2$.

The idea of **GenTiles2** is the same as for **GenTiles1**, except that we fix the horizontal tiles to be of size 1×2 , and the vertical tiles then fills out. The tiles representation of a **GenTiles2** UPB can be seen in Figure 7.5.

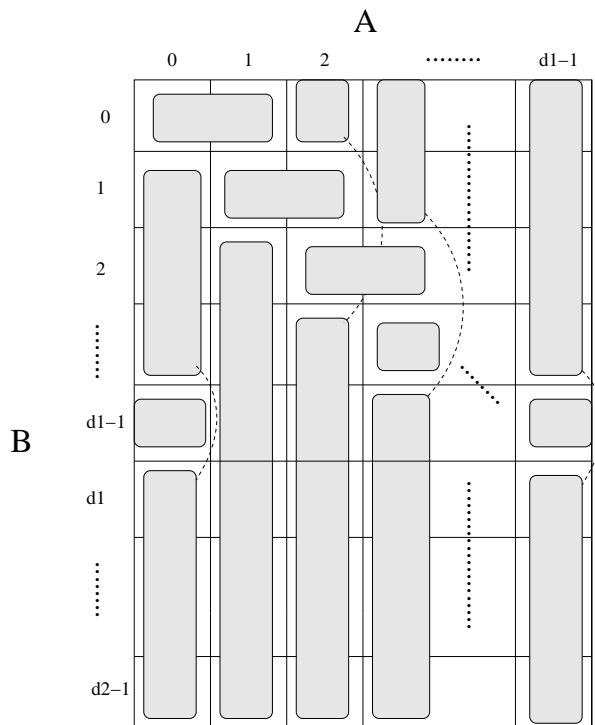


Figure 7.5: The tiles representation of **GenTiles2** for $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, leaving out the *stopper* state [DMS⁺99]. This figure is printed with permission from David DiVincenzo.

Definition

For any integers $d_1, d_2 \in \mathbb{N}$ where $d_1 \geq 3$, $d_2 > 3$, and $d_1 \leq d_2$, **GenTiles2** is defined for the complex vector space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, and consists of $d_1 d_2 - 2d_1 + 1$ states.

GenTiles2	
Parameters	$d_1, d_2 \in \mathbb{N}$ $d_1 \geq 3, d_2 > 3, \text{ and } d_1 \leq d_2$
Vector Space	$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$
Parties	2
Cardinality	$d_1 d_2 - 2d_1 + 1$
Minimal	No
Originally from	[DMS ⁺ 99]

Figure 7.6: Parameters for the **GenTiles2** UPB

For given d_1, d_2 the states of **GenTiles2** are

$$\begin{aligned}
|H_i\rangle &= \frac{1}{\sqrt{2}} (|\phi_i\rangle - |\phi_{i+1 \bmod d_1}\rangle) \otimes |\phi_i\rangle, \\
|V_{ij}\rangle &= |\phi_i\rangle \otimes \frac{1}{\sqrt{d_2-2}} \left(\sum_{s=0}^{d_1-3} \omega^{sj} |\phi_{s+i+1 \bmod d_1}\rangle + \sum_{s=d_1-2}^{d_2-3} \omega^{sj} |\phi_{s+2}\rangle \right), \\
|F\rangle &= \frac{1}{\sqrt{d_1}} \sum_{s=0}^{d_1-1} |\phi_s\rangle \otimes \frac{1}{\sqrt{d_2}} \sum_{s=0}^{d_2-1} |\phi_s\rangle,
\end{aligned} \tag{7.7}$$

where $0 \leq i \leq d_1 - 1$, $1 \leq j \leq d_2 - 3$, and $\omega = e^{i\frac{2\pi}{n-2}}$.

Proof

As for **GenTiles1** there is no proof in [DMS⁺99] that **GenTiles2** is a UPB. The proof is given in [DT00]. To prove the unextendibility of **GenTiles2** the determinant method used to prove unextendibility of the **Min4x4** UPB on page 46 can be used.

Example

The smallest **GenTiles2** UPB, which is obtained with parameters $d_1 = 3$ and $d_2 = 4$, is the following

$$\begin{aligned}
|H_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle, \\
|H_1\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |1\rangle, \\
|H_2\rangle &= \frac{1}{\sqrt{2}}(|2\rangle - |0\rangle) \otimes |2\rangle, \\
|V_{01}\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |3\rangle), \\
|V_{11}\rangle &= |1\rangle \otimes \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle), \\
|V_{21}\rangle &= |2\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |3\rangle), \\
|F\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \otimes \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle),
\end{aligned} \tag{7.8}$$

where $|\phi_i\rangle$ from the definitions is set to $|\phi_i\rangle = |i\rangle$.

Properties

GenTiles2 UPBs where both parties have the same dimensions exist. When $d = d_1 = d_2$, **GenTiles1** and **GenTiles2** have the same cardinality, and resides in the same vector space, but they are, except from the case $d_1 = d_2 = d = 4$, not identical. The $|H_j\rangle$ states of the **GenTiles2** have a superposition of two basic states on their first party, whereas all states of **GenTiles1** UPBs are superpositions of $d/2$ basis states. In the case $d_1 = d_2 = d = 4$ **GenTiles1** and **GenTiles2** are identical. This case is the example of the smallest **GenTiles1** on page 55.

7.4 GenPyramid

Motivation

The **GenPyramid** UPB, like the **GenShift** UPB, is defined for several parties. The dimension of the vector space of each party is 3. The **GenPyramid** UPB is defined for m parties, where $p = 2m + 1$ is a prime. **GenPyramid** has p states, which achieves the Simple Lower Bound (see page 42).

If we want a UPB which achieves the Simple Lower Bound, we know it has to be symmetric (Theorem 6.1.4). By definition any set of three states from a symmetric UPB with m parties each with a 3 dimensional complex vector space, should span the local three-dimensional vector space of all the parties.

The idea of the **GenPyramid** UPB is to define some vectors, such that any three of the vectors span a three dimensional space, and then combine these vectors to the states of a UPB. A way to ensure that any three vectors out of p , span a three dimensional space is to let them be the edges of a pyramid with a p -polygon base, thus the name **GenPyramid**. If we adjust the height of the pyramid such that, for some t , each vector $|\phi_i\rangle$ is orthogonal to $|\phi_{i\pm t}\rangle$ then we can combine the vectors into states $|\psi_i\rangle$ such that $\langle\psi_i|\psi_{i\pm 1}\rangle = 0$ in the first party, and $\langle\psi_i|\psi_{i\pm 2}\rangle = 0$ in the second party, and so forth, thus guaranteeing that $\langle\psi_i|\psi_{i\pm k}\rangle = 0$ in the k 'th party, for $k = 1, \dots, m$.

When choosing t we might have several possibilities. Imagine a pyramid of height 0. If two edges have an angle greater than $\pi/2$ and smaller than π they can be made orthogonal by lifting the pyramid top. So any t for which $|\phi_i\rangle$ and $|\phi_{i+t}\rangle$ have an angle between $\pi/2$ and π in the height 0 pyramid works.

The reason why $2m + 1$ has to be prime, is that it gives us a fairly simple way to permute the pyramid edges from one party to the other. This is because multiplication by a number $t \in \mathbb{Z}_p$, modulo p , with all numbers of \mathbb{Z}_p is a permutation if and only if p and t are relatively prime.

Definition

For any integer $m \in \mathbb{N}$ where $2m + 1$ is a prime, and any $t \in \mathbb{N}$ where $\frac{\pi}{2} \leq \frac{2\pi t}{2m+1} \leq \pi$, **GenPyramid** is defined for the m -partite complex vector space $\otimes_{k=1}^m \mathbb{C}^3$, and consists of $2m + 1$ states.

For a given number of parties m , such that $p = 2m + 1$ is a prime, and any $t \in \mathbb{N}$ such that $\frac{\pi}{2} \leq \frac{2\pi t}{2m+1} \leq \pi$ the states of **GenPyramid** are defined as follows.

First we define p *pyramid edges* in \mathbb{C}^3 .

$$|\phi_i\rangle = N_p \left(\cos\left(\frac{2\pi i}{p}\right), \sin\left(\frac{2\pi i}{p}\right), h_p \right), \quad (7.9)$$

where $p = 2m + 1$, $i = 0, \dots, p - 1$, and $h_p = \sqrt{-\cos(\frac{2\pi t}{p})}$ is the height of the

GenPyramid	
Parameters	$m, t \in \mathbb{N}$ $2m + 1$ is a prime $\frac{\pi}{2} \leq \frac{2\pi t}{2m+1} \leq \pi$
Vector Space	$\otimes_{k=1}^m \mathbb{C}^3$
Parties	m
Cardinality	$2m + 1$
Minimal	Yes
Originally from	[DMS ⁺ 99]

Figure 7.7: Parameters for the **GenPyramid** UPB

pyramid, and $N_p = 1/\sqrt{1 + |\cos(\frac{2\pi t}{p})|}$ is a normalisation. Please note that i is not $\sqrt{-1}$ in Equation 7.9 above.

Then $|\phi_i\rangle \perp |\phi_{i \pm t \bmod p}\rangle$. And so we combine the vectors into a UPB in the following manner

$$|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik \bmod p}\rangle, \quad (7.10)$$

where $i = 0, \dots, 2m$.

Proof

Lemma 7.4.1 *The states of **GenPyramid** form a UPB.*

The proof given here is different from the one given in [DMS⁺99].

Proof. We first prove the orthogonality of the *pyramid edges*. Let $|\phi_i\rangle$ be given. We prove that $|\phi_i\rangle$ is orthogonal to $|\phi_{i \pm t \bmod p}\rangle$. As $\frac{\pi}{2} \leq \frac{2\pi t}{2m+1} \leq \pi$ we have that

h_p is real.

$$\begin{aligned}
\langle \phi_i | \phi_{i+t \bmod p} \rangle &= N_p \left(\cos \left(\frac{2\pi i}{p} \right), \sin \left(\frac{2\pi i}{p} \right), h_p \right)^\dagger \cdot \\
&\quad N_p \left(\cos \left(\frac{2\pi(i+t)}{p} \right), \sin \left(\frac{2\pi(i+t)}{p} \right), h_p \right) \\
&= N_p^2 \left(\cos \left(\frac{2\pi i}{p} \right) \cos \left(\frac{2\pi(i+t)}{p} \right) + \right. \\
&\quad \left. \sin \left(\frac{2\pi i}{p} \right) \sin \left(\frac{2\pi(i+t)}{p} \right) + h_p^\dagger h_p \right) \\
&= N_p^2 \left(\cos \left(\frac{2\pi i}{p} - \frac{2\pi(i+t)}{p} \right) + h_p^2 \right) \\
&= N_p^2 \left(\cos \left(-\frac{2\pi t}{p} \right) + h_p^2 \right) \\
&= N_p^2 \left(\cos \left(\frac{2\pi t}{p} \right) - \cos \left(\frac{2\pi t}{p} \right) \right) \\
&= 0.
\end{aligned} \tag{7.11}$$

And same argument for $\langle \phi_i | \phi_{i-t \bmod p} \rangle = 0$.

Now let states $|\psi_i\rangle = \otimes_{k=1}^m |\phi_{ik \bmod p}\rangle$ and $|\psi_j\rangle = \otimes_{k=1}^m |\phi_{jk \bmod p}\rangle$ be given. Without loss of generality let $i > j$. The $k/(i-j)$ th party of the two states are $|\phi_{ik/(i-j) \bmod p}\rangle$ and $|\phi_{jk/(i-j) \bmod p}\rangle$. And as $ik/(i-j) - jk/(i-j) = k$, the two vectors are orthogonal by the previous argument, thus making the two states orthogonal. This proves that **GenPyramid** is a PB.

As **GenPyramid** is a PB with $\sum_{k=1}^m (d_k - 1) + 1 = 2m + 1$ states, the Partition Lemma (page 37) states that it is a UPB if and only if any 3 states spans the local vector spaces of all parties.

Consider the vectors of the k th party which are the vectors $|\phi_{ik \bmod 2m+1}\rangle, i = 0, \dots, 2m$. \mathbb{Z}_p is a cyclic group. And as p is a prime any element $k \neq 0$ is a generator. So $ik, k = 0, \dots, 2m$ is just a permutation of the elements of \mathbb{Z}_p . This implies that no vector is repeated on the k th party. As, by construction, any three different vectors spans \mathbb{C}^3 , **GenPyramid** is unextendible and thus a UPB. \square

Example

Some examples of parameters which allows a **GenPyramid** UPB are: $(m, t) = (2, 2), (3, 2), (3, 3), (5, 5)$.

The 2-party **GenPyramid** is called the **Pyramid** UPB, and has the param-

eters $(m, t) = (2, 2)$.

$$\begin{aligned}
|\psi_0\rangle &= N(|0\rangle + h|2\rangle) \otimes N(|0\rangle + h|2\rangle), \\
|\psi_1\rangle &= N(\cos \frac{2\pi}{5}|0\rangle + \sin \frac{2\pi}{5}|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos \frac{4\pi}{5}|0\rangle + \sin \frac{4\pi}{5}|1\rangle + h|2\rangle), \\
|\psi_2\rangle &= N(\cos \frac{4\pi}{5}|0\rangle + \sin \frac{4\pi}{5}|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos \frac{3\pi}{5}|0\rangle + \sin \frac{3\pi}{5}|1\rangle + h|2\rangle), \\
|\psi_3\rangle &= N(\cos \frac{\pi}{5}|0\rangle + \sin \frac{\pi}{5}|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos \frac{2\pi}{5}|0\rangle + \sin \frac{2\pi}{5}|1\rangle + h|2\rangle), \\
|\psi_4\rangle &= N(\cos \frac{3\pi}{5}|0\rangle + \sin \frac{3\pi}{5}|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos \frac{\pi}{5}|0\rangle + \sin \frac{\pi}{5}|1\rangle + h|2\rangle),
\end{aligned} \tag{7.12}$$

where $h = \sqrt{-\cos \pi/5}$ and $N = 1/\sqrt{1 + \cos 4\pi/5}$.

The following 3-party **GenPyramid** is called **Sept**, and has the parameters

$(m, t) = (3, 2)$.

$$\begin{aligned}
|\psi_0\rangle &= N(|0\rangle + h|2\rangle) \otimes N(|0\rangle + h|2\rangle) \otimes N(|0\rangle + h|2\rangle) \\
|\psi_1\rangle &= N(\cos(2\pi/7)|0\rangle + \sin(2\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(4\pi/7)|0\rangle + \sin(4\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(6\pi/7)|0\rangle + \sin(6\pi/7)|1\rangle + h|2\rangle) \\
|\psi_2\rangle &= N(\cos(4\pi/7)|0\rangle + \sin(4\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(8\pi/7)|0\rangle + \sin(8\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(12\pi/7)|0\rangle + \sin(12\pi/7)|1\rangle + h|2\rangle) \\
|\psi_3\rangle &= N(\cos(6\pi/7)|0\rangle + \sin(6\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(12\pi/7)|0\rangle + \sin(12\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(4\pi/7)|0\rangle + \sin(4\pi/7)|1\rangle + h|2\rangle) \\
|\psi_4\rangle &= N(\cos(8\pi/7)|0\rangle + \sin(8\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(2\pi/7)|0\rangle + \sin(2\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(10\pi/7)|0\rangle + \sin(10\pi/7)|1\rangle + h|2\rangle) \\
|\psi_5\rangle &= N(\cos(10\pi/7)|0\rangle + \sin(10\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(6\pi/7)|0\rangle + \sin(6\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(2\pi/7)|0\rangle + \sin(2\pi/7)|1\rangle + h|2\rangle) \\
|\psi_6\rangle &= N(\cos(12\pi/7)|0\rangle + \sin(12\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(10\pi/7)|0\rangle + \sin(10\pi/7)|1\rangle + h|2\rangle) \\
&\quad \otimes N(\cos(8\pi/7)|0\rangle + \sin(8\pi/7)|1\rangle + h|2\rangle)
\end{aligned} \tag{7.13}$$

where $h = \sqrt{-\cos(4\pi/7)}$, and $N = 1/\sqrt{1 + |\cos(4\pi/7)|}$.

7.5 QuadRes

Motivation

The **QuadRes** UPB, as the name suggests, is based on properties of quadric residues. But it also bases on the following theorem by Čebotarev.

Theorem 7.5.1 (Čebotarev’s Theorem) [New76] *No sub-matrix of the $p \times p$ matrix*

$$F_p = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{p-1} & \dots & \omega^{(p-1)^2} \end{bmatrix} \quad (7.14)$$

is singular, where ω is a primitive p th root of unity and p is a prime.

The matrix F_p is sometimes referred to as the Fourier Matrix, as it is the discrete Fourier Transform [NC00].

Čebotarev’s Theorem states that whenever you remove n rows and n columns from the matrix F_p the $p-n$ columns (or rows) of the reminding matrix are vectors which spans \mathbb{C}^{p-n} . This is an obvious advantage when trying to construct a UPB according to the Partition Lemma (Lemma 5.4.1).

QuadRes is a bipartite UPB where each party holds p states corresponding to rows of F_p with the same $(p+1)/2$ columns removed for both parties. We know from Čebotarev’s Theorem that whenever we take out $(p+1)/2$ vectors on either party they span $\mathbb{C}^{(p+1)/2}$, we only need to ensure that all states are orthogonal. This is where the quadric residues come to play. When choosing the columns removed from F_p with care, namely all columns whose number is not a quadric residue of \mathbb{Z}_p , we can make all states orthogonal.

Let us first recall some properties of quadric residues.

Definition 7.5.2 (Quadric Residues) [DMS⁺99] *Let p be some integer. And let \mathbb{Z}_p be the group of integers modulo p . Define $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Then the set of quadric residues*

$$Q_p = \{q \in \mathbb{Z}_p^* \mid \exists x \in \mathbb{Z}. q \equiv x^2 \pmod{p}\} \quad (7.15)$$

is a group.

We need a few observations from [DMS⁺99] about quadric residues to be able to analyse **QuadRes**. Let p be a prime, and let $q_1 \in Q_p$, and $p_1, p_2 \in \mathbb{Z}_p^* \setminus Q_p$, then

$$q_1 p_1 \notin Q_p, \quad (7.16)$$

$$p_1 p_2 \in Q_p. \quad (7.17)$$

Moreover, as p is an odd prime,

$$|Q_p| = \frac{p-1}{2}, \quad (7.18)$$

$$|\mathbb{Z}_p^* \setminus Q_p| = \frac{p-1}{2}. \quad (7.19)$$

These observations imply

$$x \in \mathbb{Z}_p^* \setminus Q_p \Rightarrow \{qx \mid q \in Q_p\} = \mathbb{Z}_p^* \setminus Q_p, \quad (7.20)$$

$$x \in Q_p \Rightarrow \{qx \mid q \in Q_p\} = Q_p. \quad (7.21)$$

Definition

For any integer $d \in \mathbb{N}$, where $2d - 1$ is a prime of the form $4t - 1$, **QuadRes** is defined for the bipartite complex vector space $\mathbb{C}^d \otimes \mathbb{C}^d$, and consists of $2d - 1$ states.

QuadRes	
Parameters	$d \in \mathbb{N}$ $x \in \mathbb{Z}_{2d-1}^* \setminus Q_{2d-1}$ $\exists t \in \mathbb{N} : 4t + 1 = 2d - 1$ is a prime
Vector Space	$\mathbb{C}^d \otimes \mathbb{C}^d$
Parties	2
Cardinality	$2d - 1$
Minimal	Yes
Originally from	[DMS ⁺ 99]

Figure 7.8: Parameters for the **QuadRes** UPB

For any given $d \in \mathbb{N}$ and $x \in \mathbb{Z}_{2d-1}^* \setminus Q_{2d-1}$ such that, for some t , $p = 2d - 1 = 4t - 1$ is a prime the states of **QuadRes** are defined as follows.

Define the function $Q : \mathbb{Z}_p \rightarrow \mathbb{C}^d$ as

$$Q(a) = \sqrt{N}|0\rangle + \sum_{q \in Q_p} e^{i2\pi qa/p} |2^q\rangle \quad (7.22)$$

where $N = \max(-\sum_{q \in Q_p} e^{i2\pi q/p}, 1 + \sum_{q \in Q_p} e^{i2\pi q/p})$ is a normalisation. Then the states of **QuadRes** are the following

$$|\psi_i\rangle = Q(i) \otimes Q(ix), \quad (7.23)$$

for all $i \in \mathbb{Z}_p$.

Proof

Lemma 7.5.3 *The states of **QuadRes** form a UPB.*

The proof given here is different from the one given in [DMS⁺99].

Proof. We first prove that N is a well defined real number. As $-1 \in Q_p$, when $p = 4t + 1$ is a prime [DMS⁺99], Equation 7.21 implies that

$$\begin{aligned} \left(\sum_{q \in Q_p} e^{i2\pi q/p} \right)^\dagger &= \left(\sum_{q \in Q_p} e^{-i2\pi q/p} \right) \\ &= \left(\sum_{q \in Q_p} e^{i2\pi q/p} \right). \end{aligned} \quad (7.24)$$

Thus $\sum_{q \in Q_p} e^{i2\pi q/p}$ is indeed a real number. And as $N = \max(-\sum_{q \in Q_p} e^{i2\pi q/p}, 1 + \sum_{q \in Q_p} e^{i2\pi q/p})$, N is a positive real number.

We now prove the orthogonality of the states. Let $|\psi_a\rangle, |\psi_b\rangle$ be given. Then

$$\begin{aligned} \langle \psi_a | \psi_b \rangle &= (Q(a) \otimes Q(ax))^\dagger \cdot (Q(b) \otimes Q(bx)) \\ &= (Q(a)^\dagger \cdot Q(b))(Q(ax)^\dagger \cdot Q(bx)) \\ &= \left(N + \sum_{q \in Q_p} e^{i2\pi q(b-a)/p} \right) \left(N + \sum_{q \in Q_p} e^{i2\pi qx(b-a)/p} \right). \end{aligned} \quad (7.25)$$

From Observations 7.20 and 7.21 we have that

$$\sum_{q \in Q_p} e^{i2\pi qz/p} = \begin{cases} \sum_{q \in Q_p} e^{i2\pi q/p} & z \in Q_p \\ \sum_{q \in \mathbb{Z}_p^* \setminus Q_p} e^{i2\pi q/p} & z \in \mathbb{Z}_p^* \setminus Q_p \end{cases}. \quad (7.26)$$

So 7.25 can be written as

$$\langle \psi_a | \psi_b \rangle = \left(N + \sum_{q \in Q_p} e^{i2\pi q/p} \right) \left(N + \sum_{q \in \mathbb{Z}_p^* \setminus Q_p} e^{i2\pi q/p} \right). \quad (7.27)$$

Furthermore

$$\begin{aligned} \sum_{q \in Q_p} e^{i2\pi q/p} + \sum_{q \in \mathbb{Z}_p^* \setminus Q_p} e^{i2\pi q/p} &= \sum_{z \in \mathbb{Z}_p^*} e^{i2\pi z/p} \\ &= -1 \end{aligned} \quad (7.28)$$

The last equality holds as we sum over all p th roots of unity except 1. Now Equation 7.27 can be rewritten as

$$\begin{aligned} \langle \psi_a | \psi_b \rangle &= \left(N + \sum_{q \in Q_p} e^{i2\pi q/p} \right) \left(N - 1 - \sum_{q \in Q_p} e^{i2\pi q/p} \right) \\ &= 0, \end{aligned} \quad (7.29)$$

by definition of N . Thus **QuadRes** is a PB.

We now prove that **QuadRes** is unextendible. The Partition Lemma (page 37) implies that it suffices to show that any d states spans \mathbb{C}^d in both parties. By definition each part of a state $|\psi_a\rangle = (N|0\rangle + \sum_{q \in Q_p} e^{i2\pi qa/p}) \otimes (N|0\rangle + \sum_{q \in Q_p} e^{i2\pi qa/p})$ corresponds to the a th row of F_p with $(p-1)/2$ columns removed plus $N|0\rangle$. So, by Čebotarev's Theorem, any $p - (p-1)/2 = (p+1)/2 = d$ states on one party spans \mathbb{C}^d . Thus proving that **QuadRes** is a UPB. \square

Example

Some examples of the dimensions for which **QuadRes** is defined are: 3, 7, 9, 11, and 19. For $(d, x) = (3, 2)$ **QuadRes** is the **Pyramid** UPB (page 61).

The **QuadRes** with $(d, x) = (3, 3)$ has the following states.

$$\begin{aligned}
 |\psi_0\rangle &= (\sqrt{N}|0\rangle + |1\rangle + |2\rangle) \otimes (\sqrt{N}|0\rangle + |1\rangle + |2\rangle) \\
 |\psi_1\rangle &= (\sqrt{N}|0\rangle + \omega|1\rangle + \omega^4|2\rangle) \otimes (\sqrt{N}|0\rangle + \omega^2|1\rangle + \omega^3|2\rangle) \\
 |\psi_2\rangle &= (\sqrt{N}|0\rangle + \omega^2|1\rangle + \omega^3|2\rangle) \otimes (\sqrt{N}|0\rangle + \omega^4|1\rangle + \omega|2\rangle) \\
 |\psi_1\rangle &= (\sqrt{N}|0\rangle + \omega^3|1\rangle + \omega^2|2\rangle) \otimes (\sqrt{N}|0\rangle + \omega|1\rangle + \omega^4|2\rangle) \\
 |\psi_1\rangle &= (\sqrt{N}|0\rangle + \omega^4|1\rangle + \omega^2|2\rangle) \otimes (\sqrt{N}|0\rangle + \omega^3|1\rangle + \omega^2|2\rangle),
 \end{aligned} \tag{7.30}$$

where $\omega = e^{i2\pi/5}$ and $N = (\sqrt{5} + 1)/2$.

Properties

Recall from Chapter 7.4 that **GenPyramid** with parameters $(2, 2)$ is the **Pyramid** UPB. This is also the case for **QuadRes** with parameters $(d, x) = (3, 2)$.

Chapter 8

Morphologic UPBs

As can be seen both the **Tiles** (page 20) and **Pyramid** (page 61) UPBs have the orthogonality graph of Figure 8.1, and live in the same multipartite complex vector space. This leads to the idea of finding all UPBs with this orthogonality graph. In [DMS⁺99] DiVincenzo, Mor, Shor, Smolin, and Terhal show a parameterised UPB which expresses all possible UPBs with this orthogonality graph.

Motivated by the fact that the parameterised UPB from [DMS⁺99] can take the forms of both **Tiles** and **Pyramid** respectively we denote this type of parameterised UPB as a *morphologic UPB*.

8.1 Constructing a Morphologic UPB

When given an orthogonality graph the search for the corresponding morphologic UPB have a number of steps. We start out assigning a completely parameterised product state to each vertex, i : $|\psi_i\rangle = \otimes_{k=1}^m (\sum_{j=1}^d \alpha_{ikj} |j\rangle)$. We then refine this product basis such that it satisfies the orthogonality graph. And finally we further refine the product basis such that it is unextendible.

To make the completely parameterised product basis satisfy the orthogonality graph we solve a system of equations for each party separately. When considering the subgraph of a particular party, the equations which are to be solved have to express the following requirements:

- The inner product of the vectors represented by connected vertices have to be zero.
- The inner product of the vectors represented by non-connected vertices have to be nonzero.
- All vectors should have unit norm.

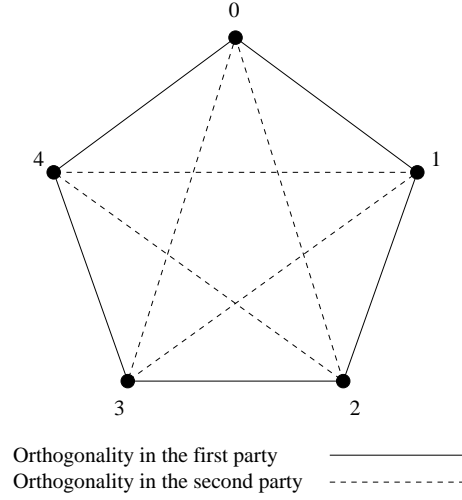


Figure 8.1: Orthogonality graph for the **Tiles** and **Pyramid** UPBs.

Consider again the graph of Figure 8.1. The equations of the two parties are the same, as the subgraphs representing the two parties are both 5-cycles. We concentrate on the subgraph represented by full lines.

As the vectors of vertices 0 and 1 are orthogonal, we can assume without loss of generality, that the state represented by vertex 0 is $|0\rangle$ and the state represented by vertex 1 is $|1\rangle$. This assumption corresponds to a possible rotation of the local subsystem.

The states of the first party can then be written as

$$\begin{aligned}
 |\phi_0\rangle &= |0\rangle, \\
 |\phi_1\rangle &= |1\rangle, \\
 |\phi_2\rangle &= \alpha_{210}|0\rangle + \alpha_{211}|1\rangle + \alpha_{212}|2\rangle, \\
 |\phi_3\rangle &= \alpha_{310}|0\rangle + \alpha_{311}|1\rangle + \alpha_{312}|2\rangle, \\
 |\phi_4\rangle &= \alpha_{410}|0\rangle + \alpha_{411}|1\rangle + \alpha_{412}|2\rangle.
 \end{aligned} \tag{8.1}$$

Using our list of requirements (page 69), we see that the first of the above requirements yields the equations $\alpha_{211} = 0, \alpha_{411} = 0, \alpha_{210}\alpha_{310} + \alpha_{212}\alpha_{312} = 0$, and $\alpha_{311}\alpha_{411} + \alpha_{312}\alpha_{412} = 0$. The second requirement yields the inequalities $\alpha_{210} \neq 0, \alpha_{310} \neq 0, \alpha_{311} \neq 0, \alpha_{411} \neq 0, \alpha_{212} \neq 0$, and $\alpha_{412} \neq 0$. And finally the normalisation requirement yields the equations $\alpha_{210}^2 + \alpha_{212}^2 = 1, \alpha_{310}^2 + \alpha_{311}^2 + \alpha_{312}^2 = 1$, and $\alpha_{411}^2 + \alpha_{412}^2 = 1$.

Solving these equations gives the solution

$$\begin{aligned}
|\phi_0\rangle &= |0\rangle, \\
|\phi_1\rangle &= |1\rangle, \\
|\phi_2\rangle &= a_1 \frac{\alpha_{312}}{\sqrt{\alpha_{310}^2 + \alpha_{312}^2}} |0\rangle - a_1 \frac{\alpha_{310}}{\sqrt{\alpha_{310}^2 + \alpha_{312}^2}} |2\rangle, \\
|\phi_3\rangle &= \alpha_{310} |0\rangle + a_2 i \sqrt{\alpha_{310}^2 - 1} \sqrt{1 + \frac{\alpha_{312}^2}{\alpha_{310}^2 - 1}} |1\rangle + \alpha_{312} |2\rangle, \\
|\phi_4\rangle &= a_2 a_3 i \frac{\alpha_{312}}{\sqrt{\alpha_{310}^2 - 1}} |1\rangle + a_3 \sqrt{1 + \frac{\alpha_{312}^2}{\alpha_{310}^2 - 1}} |2\rangle,
\end{aligned} \tag{8.2}$$

where $\alpha_{310} \notin \{-1, 0, 1\}$ and α_{312} are complex variables. And each of a_1, a_2 , and a_3 are either 1 or -1 . As the overall phase factor has no impact¹ a_1 and a_3 can be assumed to be 1.

When solving the equations for the second party the same solution is achieved except for a permutation, such that we obtain the product basis

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle \otimes |0\rangle, \\
|\psi_1\rangle &= |1\rangle \otimes \alpha_{320} |0\rangle + b_2 i \sqrt{\alpha_{320}^2 - 1} \sqrt{1 + \frac{\alpha_{322}^2}{\alpha_{320}^2 - 1}} |1\rangle + \alpha_{322} |2\rangle, \\
|\psi_2\rangle &= \frac{\alpha_{312}}{\sqrt{\alpha_{310}^2 + \alpha_{312}^2}} |0\rangle - \frac{\alpha_{310}}{\sqrt{\alpha_{310}^2 + \alpha_{312}^2}} |2\rangle \otimes |1\rangle, \\
|\psi_3\rangle &= \alpha_{310} |0\rangle + a_2 i \sqrt{\alpha_{310}^2 - 1} \sqrt{1 + \frac{\alpha_{312}^2}{\alpha_{310}^2 - 1}} |1\rangle + \alpha_{312} |2\rangle, \\
&\otimes b_2 i \frac{\alpha_{322}}{\sqrt{\alpha_{320}^2 - 1}} |1\rangle + \sqrt{1 + \frac{\alpha_{322}^2}{\alpha_{320}^2 - 1}} |2\rangle, \\
|\psi_4\rangle &= a_2 i \frac{\alpha_{312}}{\sqrt{\alpha_{310}^2 - 1}} |1\rangle + \sqrt{1 + \frac{\alpha_{312}^2}{\alpha_{310}^2 - 1}} |2\rangle, \\
&\otimes \frac{\alpha_{322}}{\sqrt{\alpha_{320}^2 + \alpha_{322}^2}} |0\rangle - \frac{\alpha_{320}}{\sqrt{\alpha_{320}^2 + \alpha_{322}^2}} |2\rangle,
\end{aligned} \tag{8.3}$$

where $\alpha_{310}, \alpha_{312}, \alpha_{320}$, and α_{322} are complex numbers with $\alpha_{310}, \alpha_{320} \notin \{-1, 0, 1\}$, and each of a_2, b_2 are either 1 or -1 .

We now have a product basis. The last step is to further restrict the variables such that the product basis is unextendible. According to the Counting Lemma (page 25) we have to guarantee that for all possible partitions of the states, at least one of the partitions spans the vector space of its party.

¹See page 5.

In order for d d -dimensional states to span \mathbb{C}^d , the determinant of the matrix with the d states as columns has to be different from 0 [Bea95]. In order for $D > d$ d -dimensional states to span \mathbb{C}^d , some subset of size d of the D states has to span \mathbb{C}^d . To verify that a PB is unextendible we can verify that in any partition at least one of the subsets spans its local vector space.

In the case of Equation 8.3 we can just verify that any three of the states of Equation 8.1 spans \mathbb{C}^3 . This is clearly true in all cases but $\{|\phi_0\rangle, |\phi_3\rangle, |\phi_4\rangle\}$, $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$, and $\{|\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle\}$, as

$$\begin{aligned} \det(|\phi_0\rangle, |\phi_3\rangle, |\phi_4\rangle) &= i\sqrt{\alpha_{310}^2 - 1}, \\ \det(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle) &= -\frac{\alpha_{310}^2 + \alpha_{312}^2}{\sqrt{\alpha_{310}^2 + \alpha_{312}^2}}, \\ \det(|\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle) &= \frac{i\alpha_{312}}{\sqrt{(\alpha_{310}^2 - 1)(\alpha_{310}^2 + \alpha_{312}^2)}}. \end{aligned} \tag{8.4}$$

For the PB of Equation 8.3 to be unextendible, we have to require that these three determinants are nonzero. As we are already requiring that $\alpha_{310} \notin \{-1, 0, 1\}$ the first determinant is different from zero. But for the last two determinants to be nonzero we have to further require that $\alpha_{310} \neq \pm i\alpha_{312}$, and that $\alpha_{310} \neq 0$. The same is true for the second party.

Thus the product basis of Equation 8.3 is a UPB if and only if $\alpha_{310}, \alpha_{320} \notin \{-1, 0, 1\}$, $\alpha_{310} \neq \pm i\alpha_{312}$, $\alpha_{320} \neq \pm i\alpha_{322}$, $\alpha_{310}, \alpha_{320} \neq 0$, and $a_2, b_2 \in \{-1, 1\}$. Furthermore the UPBs defined by Equation 8.3 constitute the only UPBs having the orthogonality graph given in Figure 8.1.

In Theorem 5.2.9 we saw that all UPBs in $\mathbb{C}^3 \otimes \mathbb{C}^3$ have the same orthogonality graph, namely the graph of Figure 8.1. We have now constructed a 6 parameter UPB which can take the form of any other UPB with that orthogonality graph, possibly after a rotation, which therefore can take the form of any UPB in $\mathbb{C}^3 \otimes \mathbb{C}^3$.

Let us summarise this in a lemma.

Lemma 8.1.1 *The states of Equation 8.3 represents all product bases in $\mathbb{C}^3 \otimes \mathbb{C}^3$ having the orthogonality graph of Figure 8.1. Furthermore if $\alpha_{310}, \alpha_{320} \notin \{-1, 0, 1\}$, $\alpha_{310} \neq \pm i\alpha_{312}$, $\alpha_{320} \neq \pm i\alpha_{322}$, $\alpha_{310}, \alpha_{320} \neq 0$, and $a_2, b_2 \in \{-1, 1\}$, the states of Equation 8.3 is an unextendible product basis.*

When using the PB of Equation 8.3 with the parameters $a_2 = b_2 = -1$, $\alpha_{310} = \alpha_{320} = \frac{1}{\sqrt{3}}$, and $\alpha_{312} = \alpha_{322} = \frac{1}{\sqrt{6}}$ we obtain the **Tiles** UPB when rotated by the rotation-matrix

$$\begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & -\sqrt{\frac{2}{3}} \end{pmatrix} \tag{8.5}$$

The morphologic UPB in Equation 8.3 is a bit different than the one in [DMS⁺99], though, by construction, they are equivalent.

8.2 Graph Equivalence of UPBs

If we define an equivalence relation on UPBs by their orthogonality graph such that two UPBs which resides in the same complex multipartite vector space and have the same orthogonality graph are *graph equivalent* then, by Theorem 5.2.9, all UPBs in $\mathbb{C}^3 \otimes \mathbb{C}^3$ are *graph equivalent*.

Definition 8.2.1 (Graph Equivalence) *Let $\mathbb{C}^d = \otimes_{k=1}^m \mathbb{C}^{d_k}$ be an m -partite complex vector space. And let S_1 and S_2 be two unextendible product bases from \mathbb{C}^d with orthogonality graphs $(S_1, S_1 \times S_1, c_1)$ and $(S_2, S_2 \times S_2, c_2)$, respectively. Then $S_1 \sim S_2$ if and only if there exists some permutation $\Pi : S_1 \rightarrow S_2$ such that*

$$c_1(u, v) = c_2(\Pi(u), \Pi(v)) \quad (8.6)$$

for all $u, v \in S_1$. We say S_1 and S_2 are graph equivalent.

In Chapter 7.3 we saw that in $\mathbb{C}^4 \otimes \mathbb{C}^4$ the **GenTiles1** and **GenTiles2** UPBs are identical, but we realised that in other dimensions they are not identical. In particular they have different orthogonality graphs. This tells us that there may be more than one equivalence class in a particular complex vector space.

In some cases, however, we can prove that only one equivalence class exists. To do this we need the following lemma.

Lemma 8.2.2 *Let G be a graphs with $n \geq 3$ vertices and connectivity 2, such that all vertices have degree exactly 2. Then G is an n -cycle.*

Proof. We prove the lemma by induction in the size of the graph.

For the basis case we realise that if G consists of 3 vertices each with degree two, then the graph is a 3-cycle.

Now assume that for graphs of size n the lemma holds.

Let a graph G' with $n + 1$ vertices be given, such that each vertex has degree exactly 2, and that the connectivity of the graph is 2. Denote by S_v the set consisting of a vertex v and the two vertices, u, w , to which v is connected (v has degree two). As the connectivity of the graph is 2, and each vertex is connected to exactly two other vertices the two vertices u and w must be connected to vertices outside S_v . Now remove v from the graph G' , and connect u and w , then u and w each have degree 2, and the connectivity of the new graph is still 2. As this graph is of size n it must, by the induction hypothesis, be an n -cycle. But then G' must be an $(n + 1)$ -cycle, which completes the proof. \square

We can use this lemma to prove that all minimal UPBs in $\mathbb{C}^3 \otimes \mathbb{C}^{d_2}$, for some integer d_2 , belong to the same equivalence class. First notice that for $\mathbb{C}^3 \otimes \mathbb{C}^{d_2}$ the lower bound of Lemma 6.1.2 is $d_2 + 2$. When d_2 is odd the Alon-Lovász Criterion (page 42) implies that a UPB of this cardinality exists. By Theorem 6.1.6 a UPB of cardinality $d_2 + 2$ in $\mathbb{C}^3 \otimes \mathbb{C}^{d_2}$ is symmetric.

Theorem 8.2.3 *Let $\mathbb{C}^d = \mathbb{C}^3 \otimes \mathbb{C}^{d_2}$ be a bipartite complex vector space, where d_2 is odd. And let S_1 and S_2 be minimal UPBs of \mathbb{C}^d . Then $S_1 \sim S_2$.*

Proof. When d_2 is odd, $2 + d_2$ is also odd, and thus the Alon-Lovász Criterion (Theorem 6.1.3) implies that a UPB of cardinality $2 + d_2$ exists. By The Simple Lower Bound (Lemma 6.1.2) no UPB of cardinality less than $2 + d_2$ exists in $\mathbb{C}^3 \otimes \mathbb{C}^{d_2}$, and so S_1 and S_2 must have cardinality $2 + d_2$ to be minimal.

By Theorem 6.1.6 a UPB of cardinality $d_2 + 2$ in $\mathbb{C}^3 \otimes \mathbb{C}^{d_2}$ is symmetric, so both S_1 and S_2 are symmetric.

By Theorem 6.3.1 each vertex of the two orthogonality graphs is connected to 2 vertices on the first party and $d_2 - 1$ vertices on the second party.

By Lemma 8.2.2 this implies that the orthogonality graph of the first party of both S_1 and S_2 are n -cycles.

We can now define a permutation $\Pi : S_1 \rightarrow S_2$ which permutes the n -cycle of S_1 to the n -cycle of S_2 as follows: Let $u_1 \in S_1$ and $u_2 \in S_2$ be given, and define

$$\begin{aligned} \Pi(u_1) &= u_2 \\ \Pi(w_1) &= w_2 \text{ if } c_1(v_1, w_1) = c_2(v_2, w_2) = \{1\} \wedge \Pi(v_1) = v_2 \end{aligned} \tag{8.7}$$

By Theorem 6.3.1 all edges have exactly one colour, and thus we either have $c_1(u, v) = c_2(\Pi(u), \Pi(v)) = \{1\}$ or $c_1(u, v) = c_2(\Pi(u), \Pi(v)) = \{2\}$. And thus $S_1 \sim S_2$. \square

Unfortunately not all symmetric UPBs from identical vector spaces are equivalent. Consider the two orthogonality graphs of Figure 8.2. Applying Lemma 5.3.4 we can verify that both orthogonality graphs represent UPBs from $\mathbb{C}^4 \otimes \mathbb{C}^5$.

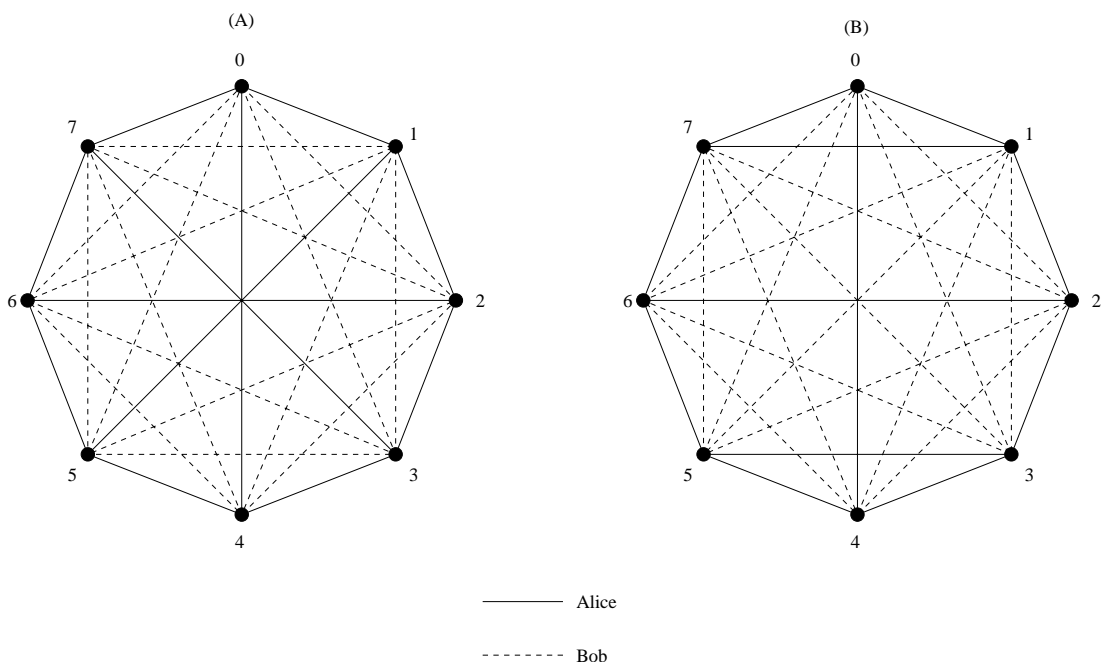


Figure 8.2: The orthogonality graphs of two nonequivalent symmetric UPBs in $\mathbb{C}^4 \otimes \mathbb{C}^5$.

Chapter 9

Concluding Comments

9.1 Achievements

In this thesis work done on unextendible product bases (UPBs) is collected and presented in a structured manner. Emphasis is on improving the reader's intuition on UPBs, and many proofs are rewritten to clarify the techniques used. Furthermore new results on UPBs are presented.

Through a discussion, in Chapter 5.2, on the use of orthogonality graphs in proofs of the existence of LOCC protocols to distinguish states of a product basis, we see that orthogonality graphs might not fully classify distinguishability. But we demonstrate several uses of orthogonality graphs.

We classify UPBs as either symmetric UPBs or alternating UPBs. We prove that UPBs that achieve the non-tight Simple Lower Bound are exactly the symmetric UPB. Furthermore, in Chapter 6.3 we prove that the orthogonality graphs of symmetric UPBs have some nice properties.

In Chapter 6.2 we present a UPB which is minimal without reaching the Simple Lower Bound. This is the first known bipartite alternating minimal UPBs.

In Chapter 8.2 we introduce an equivalence relation on UPBs and proves that all bipartite UPBs in $\mathbb{C}^3 \otimes \mathbb{C}^d$ are equivalent according to this definition.

9.2 Open Questions

Little work has been done on the upper bound on the size of UPBs. If it can be proven that the upper bound presented in Chapter 6.4 is tight it would prove that the lower bound on the rank of a bound entangled state is also tight.

No work has been done on characterising the properties of the bound entangled states related to UPBs. New insight to bound entanglement might be found in a study of the bound entangled states related to UPBs.

UPBs might be used to create a protocol for the exchange of secret keys for cryptology. To the best knowledge of the author of this thesis this is the first

practical use of UPBs. An outline of the protocol is as follows: Choose a bipartite UPB with many states. Let each state of the UPBs represent a possible key. If Alice wants to share a secret key with Bob, she randomly chooses one of the states of the UPB. Alice first sends the first part of the chosen state by a quantum channel. When Bob receives the state he announces this on a public channel. When Alice knows that Bob has received the first part of the state, she sends the second part of the state to Bob. Now Bob has the whole state, and can make a measurement to decide which state of the UPB he has been given. The security of the protocol is based on the fact that an eavesdropper cannot recognise the state by only observing one of the parts. A strict proof of the security has to be made.

Appendix A

Legend

\mathbb{C}	The complex numbers.
\mathbb{C}^d	A complex vector space of dimension d
$ \psi\rangle$	A quantum state (Usually an entire multipartite state).
$ \phi\rangle$	A quantum state (Usually part of multipartite state).
α_i, β_i	Amplitudes from the first and second part of a bipartite state.
d	Dimension of \mathbb{C}^d .
n	The cardinality of a UPB.
m	The number of parties in a multipartite vector space.
i	Iteration over the states of a UPB.
k	Iteration over the parties of a multipartite vector space.
i	$\sqrt{-1}$
A	A matrix.
U	A unitary matrix (Transformation).
A^\dagger	Complex conjugate transposed of A .
λ_i	The i 'th eigenvalue of some matrix.
I	The identity matrix.
φ_i	The eigenvector corresponding to eigenvalue λ_i .
P_i	Projection onto the eigenspace corresponding to eigenvalue λ_i .
p	A probability.
G	A graph.
V	The set of vertices of a graph.
E	The set of edges of a graph.
S	A set of quantum states. Sometimes a set of vertices.
u, v, w	Vertices.
$\mathcal{P}(S)$	The powerset of S .
Π	A permutation function.
UPB	A named UPB.

Appendix B

List of UPBs

The following table contains a list of UPBs referred to in this thesis.

Name	Dimension	Cardinality	Page
Tiles	$\mathbb{C}^3 \otimes \mathbb{C}^3$	5	20
Min4x4	$\mathbb{C}^4 \otimes \mathbb{C}^4$	7	46
GenShifts	$\otimes_{k=1}^{2m-1} \mathbb{C}^2$	$2m$	49
Shifts	$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$	4	51
GenTiles1	$\mathbb{C}^n \otimes \mathbb{C}^n, n \geq 4$ even	$n^2 - 2n + 1$	52
GenTiles2	$\mathbb{C}^n \otimes \mathbb{C}^m, m \leq n$	$mn - 2m + 1$	56
GenPyramid	$\otimes_{k=1}^m \mathbb{C}^3, 2m + 1$ prime	$2m + 1$	59
Pyramid	$\mathbb{C}^3 \otimes \mathbb{C}^3$	5	61
Sept	$\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$	7	62
QuadRes	$\mathbb{C}^n \otimes \mathbb{C}^n, 2n - 1 = 4m + 1$ prime	$2n - 1$	65
Min2x2x2x2	$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$	6	44

Figure B.1: All generic and specific UPBs in this Thesis

Appendix C

Dependencies of Results

Result	Depends on	Page
Proposition 2.1.4		7
Theorem 4.2.1	-	20
Theorem 4.3.3	-	22
Lemma 4.3.4	-	22
Theorem 4.3.5	-	22
Counting Lemma (5.1.1)	2.1.4	25
Proposition 5.2.7		28
Theorem 5.2.8	5.2.7	29
Theorem 5.2.9	4.3.3, 5.2.8	30
Theorem 5.3.3	-	36
Lemma 5.3.4	5.3.3, 5.1.1	36
Partition Lemma (5.4.1)	5.1.1	37
Lemma 5.4.3	5.3.3	39
Lemma 6.1.1	5.1.1	41
Simple Lower Bound 6.1.2	5.1.1	42
Alon-Lovász Criterion (6.1.3)	6.1.1, 6.1.4, 6.1.5	42
Lemma 6.1.4	5.4.1	43
Lemma 6.1.5		43
Theorem 6.1.6	6.1.4, 5.3.3, 5.1.1	43
Theorem 6.3.1	5.4.3, 6.1.6	47
Lemma 6.4.1,	-	47
Theorem 6.4.2	4.2.1, 6.4.1	48
Lemma 8.1.1	5.2.9	72
Lemma 8.2.2		73
Theorem 8.2.3	5.3.3, 6.3.1, 8.2.2	74

Figure C.1: All results in this thesis, and their dependencies.

Bibliography

- [AL00] N. ALON, L. LOVÁSZ, *Unextendible Product Bases*, Journal of Combinatorial Theory, Series A 95(1):169–179 (Jul 2001).
- [Bea95] FRALEIGH BEAUREGARD, *Linear Algebra*, Addison-Wesley, 1995.
- [BBP96] C. H. BENNETT, H. BERNSTEIN, S. POPESCU, B. SCHUMACHER, *Concentration Partial Entanglement by Local Operations*, Physical Review A 53:2046 (1996), <http://xxx.lanl.gov/abs/quant-ph/9511030>.
- [BDF⁺98] C. H. BENNETT, D. P. DIVINCENZO, C. A. FUCHS, T. MOR, E. RAINS, P. W. SHOR, J. A. SMOLIN, AND W. K. WOOTTERS, *Quantum Nonlocality without Entanglement*, Physical Review A 59:1070–1091 (1999), <http://xxx.lanl.gov/abs/quant-ph/9804053>.
- [BDM⁺98] C. H. BENNETT, D. P. DIVINCENZO, T. MOR, P. W. SHOR, J. A. SMOLIN, AND B. M. TERHAL, *Unextendible Product Bases and Bound Entanglement*, Physical Review Letters 82:5385–5388 (1999), <http://xxx.lanl.gov/abs/quant-ph/9808030>.
- [Bra00] GILLES BRASSARD, *Quantum Information Processing*, January 2000. Fragments of a book. To appear.
- [Deu85] DAVID DEUTSCH, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society A400:97–117 (1985).
- [DMS⁺99] D. P. DIVINCENZO, T. MOR, P. W. SHOR, J. A. SMOLIN, AND B. M. TERHAL, *Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement*, To appear in Communications in Mathematical Physics, <http://xxx.lanl.gov/abs/quant-ph/9908070>.
- [DT00] DAVID P. DIVINCENZO AND BARBARA M. TERHAL, *Product Bases in Quantum Information Theory*, To appear in Proceedings of the

- XIII International Congress on Mathematical Physics, <http://xxx.lanl.gov/abs/quant-ph/0008055>.
- [DT01] DAVID P. DIVINCENZO AND BARBARA M. TERHAL, private communication, QIP2001 in Amsterdam, Holland, January 2001.
- [DT02] DAVID P. DIVINCENZO AND BARBARA M. TERHAL, private communication, EURESCO Conference on Quantum Information, Sant Feliu de Guixols, Spain, Marts 2002.
- [EPR35] A. EINSTEIN, B. PODOLSKY, AND N. ROSEN, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Physical Review 47:777–780 (1935).
- [Hor97] PAWEŁ HORODECKI, *Seperability criterion and inseparable mixed states with positive partial transposition*, Physical Letters A 232:333 (1997), <http://xxx.lanl.gov/abs/quant-ph/9703004>.
- [HHH96] M. HORODECKI, P. HORODECKI, AND R. HORODECKI, *Separability of mixed states: necessary and sufficient conditions*, Physics Letters A 223:1–8 (1996), <http://xxx.lanl.gov/abs/quant-ph/9605038>.
- [HHH98] M. HORODECKI, P. HORODECKI, AND R. HORODECKI, *Mixed-state entanglement and distillation: is there a “bound” entanglement in nature?*, Physical Review Letter 80:5239–5242 (1998), <http://xxx.lanl.gov/abs/quant-ph/9801069>.
- [HSTT99] P. HORODECKI, J. A. SMOLIN, B. M. TERHAL, AND A. V. THAPLIYAL, *Rank Two Bipartite Entangled States Do Not Exist*. To appear in Journal of Theoretical Computer Science, <http://xxx.lanl.gov/abs/quant-ph/9910122>.
- [HN01] PETER HØYER AND JAN NEERBEK, private communication, Århus, Denmark, 2001.
- [LBC⁺00] M. LEWENSTEIN, D. BRUSS, J. I. CIRAC, B. KRAUS, M. KUŚ, J. SAMSONIWICZ, A. SANPERA, AND R. TARRACH, *Seperability and disillability in composite systems —a primer—*, Journal of Modern Optics 47:2841 (2000), <http://xxx.lanl.gov/abs/quant-ph/0006064>.
- [LSS89] L. LOVÁSZ, M. SAKS, AND A. SCHRIJVER, *Orthogonal Representations and Connectivity of Graphs*, Linear Algebra and its Applications 114/115:439–454 (1989).
- [New76] M. NEWMAN, *On a theorem of Čebotarev*, Linear and Multilinear Algebra 3:259–262 (1976).

- [NC00] MICHAEL A. NIELSEN AND ISAAC L. CHUANG, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [Per96] ASHER PERES, *Seperability Criteron for Density Matrices*, Physical Review Letter 77:1413–1415 (1996), <http://xxx.lanl.gov/abs/quant-ph/9604005>.
- [Pre98] JOHN PRESKILL, *Lecturenotes*, (Chapter 2. Foundations of Quantum Theory I: States and Ensembles), 1998, <http://www.theory.caltech.edu/people/preskill/ph219/#lecture>
- [RP98] ELEANOR RIEFFEL AND WOLFGANG POLAK, *An Introduction to Quantum Computing for Non-Physicists*, ACM Computing Surveys 32(3):300–335 (2000), <http://xxx.lanl.gov/abs/quant-ph/9809016>.