Quantum Latin squares and quantum functions: applications in quantum information



Benjamin Musto
Wolfson College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy
Michaelmas term 2019

Abstract

A central theme of this thesis is the quantization and generalization of objects from areas of mathematics such as set theory and combinatorics with application to quantum information. We represent mathematical objects such as Latin squares or functions as string diagrams over the category of finite-dimensional Hilbert spaces obeying various diagrammatic axioms. This leads to a direct understanding of how these objects arise in quantum mechanics and gives insight into how quantum analogues can be defined.

In Part I of this thesis we introduce quantum Latin squares (QLS), quantum objects which generalize the classical Latin squares from combinatorics. We present a new method for constructing a unitary error basis (UEB) from a quantum Latin square equipped with extra data, which we show simultaneously generalizes the existing shift-and-multiply and Hadamard methods. We introduce two different notions of orthogonality for QLS which we use to construct families of mutually unbiased bases and perfect tensors respectively. We also introduce a further generalization of Latin squares called quantum Latin isometry squares. We use these to produce quantum error codes and to give a new way of characterizing UEBs.

In Part II we show that maximal families of mutually unbiased bases (MUBs) are characterized in all dimensions by partitioned UEBs, up to a choice of a family of Hadamards. Furthermore, we give a new construction of partitioned UEBs, and thus maximal families of MUBs, from a finite field, which is simpler and more direct than previous proposals. We introduce new tensor diagrammatic characterizations of maximal families of MUBs, partitioned UEBs, and finite fields as algebraic structures defined over Hilbert spaces.

In Part III we introduce quantum functions and quantum sets, which quantize the classical notions. We show that these structures form a 2-category **QSet**. *We extend this framework to introduce quantum graphs and quantum homomorphisms which form a 2-category* **QGraph**. *We show that these 2-categories capture several different notions of quantum morphism and noncommutative graph from various previous papers in noncommutative topology, quantum non-local games and quantum information. We later use the correspondence between our quantum graph morphisms and those from quantum non-local games to show that pairs of quantum isomorphic graphs with multiple connected components are built up of quantum isomorphisms on those components.*

Contents

1 Preface **4**

1.1 Summary of main results . . . 8

1.2 Related work . . . 10

1.3 Outlook . . . 11

1.4 Overview . . . 13

2 Background **14**

2.1 An introduction to the graphical calculus . . . 14

2.1.1 String diagrams . . . 14

2.1.2 Representing finite-dimensional C*-Algebras graphically . . . 16

2.1.3 Finite-dimensional Gelfand duality and dagger special commutative Frobenius algebras as orthonormal bases . . . 18

2.2 Interacting algebras . . . 20

2.2.1 Abelian groups . . . 20

2.2.2 Generalizations . . . 22

2.3 Shaded graphical calculus . . . 23

I Quantum Latin squares **24**

3 Quantum shift-and-multiply bases **25**

3.1 Introduction . . . 25

3.2 Interacting algebraic structures in Hilbert space . . . 28

3.3 Quantum Latin squares from Hadamard matrices . . . 29

3.4 Unitary error bases from quantum Latin squares . . . 33

3.5 Shift-and-multiply method . . . 35

3.6 Hadamard method . . . 38

3.7 Group-theoretic method . . . 41

3.8 Lists of unitary error bases . . . 42

3.8.1 The unitary error basis $\mathcal{M}$ . . . 43

3.8.2 The unitary error basis $\mathcal{F}'$ . . . 43

4 An application to mutually unbiased bases **44**

4.1 Introduction . . . 44
4.2 New construction for square dimension MUBs . . . 47
4.3 Left orthogonality and Latin square conjugates . . . 51
4.4 Beth and Wocjan's MUB construction . . . 55
4.5 Mutually unbiased error bases . . . 58
4.6 Mutually left orthogonal quantum Latin squares . . . 60
4.7 Quantum Latin square 9×9 example MUB . . . 61

5 Orthogonality and generalizations **63**

5.1 Introduction . . . 63
5.1.1 Summary . . . 63
5.1.2 The two other notions of orthogonal quantum Latin squares . . . 64
5.1.3 Outline . . . 64
5.2 Quantum Latin squares and orthogonality . . . 65
5.2.1 First definitions . . . 65
5.2.2 Relationship to previous notion of orthogonality . . . 68
5.2.3 Equivalence and orthogonality . . . 69
5.2.4 Generalization to multiple systems . . . 70
5.2.5 Upper bounds on the number of mutually orthogonal quantum Latin squares . . . 72
5.3 Biunitaries and perfect tensors . . . 72
5.4 Quantum Latin isometry squares and quantum error detecting codes . . . 75
5.4.1 Quantum isometry Latin squares . . . 76
5.4.2 Skew projective permutation matrices . . . 78
5.4.3 Skew PPMs are biunitary . . . 79
5.4.4 Orthogonal quantum isometry Latin squares . . . 80
5.4.5 Quantum error detecting codes . . . 83
5.4.6 Orthogonal quantum Latin isometry squares from unitary error bases . . . 84

II Mutually unbiased bases and finite fields **85**

6 The correspondence between mutually unbiased bases and unitary error bases **86**

6.1 Introduction . . . 86
6.2 Background . . . 88
6.3 Diagrammatic controlled Hadamards and permutations . . . 89
6.4 Maximal families of MUBs and partitioned UEBs . . . 92
6.4.1 Diagrammatic characterizations . . . 93
6.5 Main results . . . 97

7 A new construction **103**

7.1 Introduction . . . 103

7.2 Finite fields . . . 104

7.2.1 A construction of $d+1$ MUBs . . . 108

7.3 Conclusion . . . 116

7.4 Minor lemmas . . . 117

III Quantum functions 119

8 Quantum functions **120**

8.1 Introduction . . . 120

8.1.1 Quantization . . . 121

8.1.2 Notation . . . 122

8.1.3 Related work . . . 122

8.1.4 Splitting and projecting . . . 123

8.2 Quantum sets, functions and bijections . . . 125

8.2.1 Quantum functions . . . 125

8.2.2 Quantum bijections . . . 127

8.2.3 The 2-category **QSet** . . . 129

8.2.4 Quantum bijections in noncommutative topology . . . 131

8.3 Quantum morphisms of classical sets . . . 132

8.3.1 Quantum functions on sets . . . 132

8.3.2 Quantum bijections on sets . . . 134

8.4 Quantum graph theory . . . 136

8.4.1 Quantum graphs and quantum adjacency matrices . . . 136

8.4.2 Quantum homomorphisms . . . 138

8.4.3 Quantum isomorphisms . . . 139

8.4.4 The 2-category **QGraph** . . . 139

8.5 Quantum graphs and quantum relations . . . 141

9 Quantum non-local games and pseudo-telepathy **145**

9.1 Introduction . . . 145

9.2 Quantum graph homomorphisms . . . 146

9.3 Quantum graph isomorphisms . . . 147

9.4 Quantum non-local games for **QSet** . . . 150

9.4.1 Quantum function game . . . 150

9.4.2 Quantum bijection game . . . 152

9.5 Invariance results . . . 156

9.5.1 Existing results . . . 156

9.5.2 Composite quantum isomorphic graphs 156

Chapter 1

Preface

This thesis is the result of four years spent as a doctoral student within the Quantum Group of the department of computer science at the University of Oxford. My initial motivations concerned investigating the interaction of pure mathematics and mathematical physics. In particular the application of abstract algebra, combinatorics and algebraic topology to quantum information science. I began my doctoral career well versed in a set of high level techniques being used to phrase quantum mechanics in terms of category theory, called categorical quantum mechanics. These were the perfect tools to investigate the application of pure mathematics to quantum information.

The chapters of this thesis are based on five papers that I have authored and coauthored with a small amount of new material in addition. A summary of the papers on which most of this thesis is based is given below:

Title	Co-authors	Chapter(s)
Quantum Latin squares and unitary error bases **Quantum Inf. & Comput. 16:1318 1332, 2016.** arXiv:1504.02715	Jamie Vicary	Chapter 3
Constructing mutually unbiased bases from quantum Latin squares **Electron. Proc. Theor. Comput. Sci. 236, 108, 2017.** arXiv:1605.08919	Sole author	Chapter 4
Orthogonality for quantum Latin isometry squares **Electron. Proc. Theor. Comput. 287, 253, 2019.** arXiv:1804.04042	Jamie Vicary	Chapter 5
Characterizing maximal families of mutually unbiased bases **Not yet published** arXiv:1710.07046	Sole author	Chapter 6 & Chapter 7
A compositional approach to quantum functions **J. Math. Phys. 59, 081706, 42, 2018.** arXiv:1711.07945	Dominic Verdon & David Reutter	Chapter 8 & Chapter 9

I have an interest in the quantum analogues of objects in pure mathematics, the operational interpretation of such objects and the classification into essentially classical and truly quantum properties. Since the advent of quantum mechanics it has been clear that classical physics must sit inside quantum mechanics as a special case. Mathematically then, quantization has naturally manifested itself as generalization, a relaxation of axiomatic conditions. In particular various aspects of quantum mechanics imply a necessity to move from the commutativity of classical observables, always allowing for the joint measurement of sets of observables; to non-commutativity, where it is impossible to simultaneously measure certain observables. This manifests itself as Heisenberg's uncertainty principle and is a fundamental feature of quantum mechanics.

A central theme of this thesis is the hand-in-hand journey of generalization and quantization. In 2014, using the techniques of categorical quantum mechanics, Jamie Vicary and I discovered a quantum analogue to Latin squares which we named *quantum Latin squares*. Latin squares are objects from combinatorics which go back at least to around AD 1000 when Latin squares were inscribed upon amulets worn to ward off evil spirits by Arabic and Indian communities [Mac12]. In the 1960s and 70s Latin squares found use in producing error correcting codes in classical information theory. More recently Latin squares have found similar uses in quantum error correction [Wer01, KR03]. Latin squares can be used to construct unitary error bases, structures fundamental to various areas of quantum information, that encapsulate the properties necessary for protocols such as teleportation and superdense coding as well as giving rise to quantum codes for error correction. Using the graphical calculus of categorical quantum mechanics we were able to interpret Latin squares as linear algebraic tensors in Hilbert space, a generalization of complex group algebras. It was in investigating the properties of Latin squares that give rise to unitary error bases, expressed as graphical equations of linear maps, that we discovered quantum Latin squares. Not all of the axioms describing a Latin square were necessary to the construction of unitary error bases. In fact the only necessary axioms were that the following linear maps be unitary:



(1.1)

Here the white dot represents the Latin square and the black dot is the finite-dimensional commutative C^*-algebra associated via Gelfand duality, to the set of elements appearing in the Latin square. This elegantly simple condition also appears as the diagrammatic characterization of complementary observables in quantum mechanics [ZV14] and repeatedly arises in this thesis. We defined quantum Latin squares to be tensors of this type which interact with a finite-dimensional commutative C^*-algebra by the linear maps (1.1) being unitary. In retrospect, we have found that quantum Latin squares were waiting to be discovered as they are found underlying many structures in the mathematical underpinnings

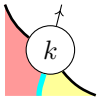
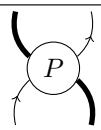
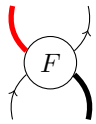
of quantum information theory, for example in quantum error correction (see Chapters 3 and 5) as well as quantum key distribution and quantum state determination (see Chapter 4) and quantum pseudo-telepathy (see Chapter 8 and 9).

In this thesis we introduce various mathematical structures including quantum Latin squares, quantum isometry Latin squares, quantum bijections and quantum functions. These objects existed and had even been implicitly used but had previously been overlooked, despite underpinning many quantum information theoretic protocols and fundamental concepts. As shown below many of these new structures can be seen as generalizations of Abelian groups.

The narrative of generalization in this thesis should rightly begin with Abelian complex group algebras viewed as certain pairs of interacting algebras in Hilbert space. Given a finite Abelian group, the set of elements can be seen via Gelfand duality, as a finite-dimensional commutative C^*-algebra giving rise to a Hilbert space. We refer to this algebra as the *indexing algebra*. The linear extension of the multiplication of the group, seen as an algebra on the Hilbert space is another finite-dimensional C^*-algebra whose elements are the complex characters of the group. We refer to this algebra as the *multiplication algebra*. In categorical quantum mechanics we can represent these algebras graphically using string diagrams. The axioms of an Abelian complex group can thus be formulated in terms of the interactions of these two algebras, for example they form a Frobenius Hopf bialgebra. One of the axioms that arises, is that the linear maps in diagram (1.1) are unitary. This actually comes from the Fourier transform of the Abelian group being a Hadamard, meaning that the two bases associated to the elements of the two C^*-algebras are mutually unbiased. This means that they model complementary observables.

So as a starting point we have an Abelian complex group algebra characterized by the interactions between an indexing algebra (a finite-dimensional commutative C^*-algebra) and a multiplication algebra (another finite-dimensional commutative C^*-algebra). If we allow the multiplication algebra to be non-commutative we obtain a general (ie not necessarily Abelian) Complex group algebra. If we further relax the conditions determining the multiplication algebra, we obtain the linear extension of a Latin square mentioned above. Now the multiplication algebra fails to be an algebra in the traditional sense, as it is in general non-associative, but we will keep the name for the sake of ease of reference. Next, by dropping the bialgebra condition and some others we obtain quantum Latin squares. At this point the multiplication algebra is more of a generalized quantum multiplication that allows outputs which are superpositions of elements. To continue this trend we obtain *quantum Latin isometry squares* which first appear in Chapter 5, by allowing the outputs to be linear maps rather than just states. Quantum Latin isometry squares still retain the condition that a pair of linear maps that generalize those in diagram (1.1) are unitary. We will see that quantum Latin isometry squares correspond to quantum channels preserving pointer states [BN17] and also characterize perfect strategies for certain quantum non-local games [AMR+19]. In the next generalization we remove the requirement for commutativity

from the indexing set algebra, this gives rise to quantum bijections of quantum sets and quantum automorphisms of quantum graphs, the quantum information theoretic implications of which are only beginning to be explored [DSW13, Sta16]. Finally we drop the requirement of unitarity for one of the linear maps in diagram (1.1) to obtain quantum functions between quantum sets or quantum graph homomosphisms. We give a table below to show the ladder of generalization and quantization, outlined above which is a central narrative thread in this thesis:

'Indexing set algebra'	'Multiplication algebra'	Resulting mathematical object
 Commutative C^*-algebra	 Commutative C^*-algebra	Abelian complex group algebra $\mathbb{C}[A]$
 Commutative C^*-algebra	 C^*-algebra	Complex group algebra $\mathbb{C}[G]$
 Commutative C^*-algebra	 Non-associative 'algebra'	Latin square L_n
 Commutative C^*-algebra	 QLS tensor	Quantum Latin square $\|\Psi_{ij}\rangle$
 Commutative C^*-algebra	 QILS tensor	Quantum Latin isometry square k_{ij}
 C^*-algebra	 Quantum bijection tensor	Quantum bijection P
 C^*-algebra	 Quantum function tensor	Quantum function F

We now give a summary of the main results of this thesis.

1.1 Summary of main results

Unitary error bases (UEBs) play an important role in this thesis. UEBs are bases of unitary operators which derive their name from the fact that they play a prominent role in quantum error correction, in which context they were first studied by Knill, Steane, and others [Kni96, Ste96]. Mathematically UEBs encode the data for teleportation and superdense coding protocols in quantum information as shown by Werner in 2001 [Wer01]. New constructions give new algorithms for the performance of teleportation and superdense coding as well as giving construction methods for new classes of quantum error correcting codes. UEBs have been studied since the 1990s but new constructions are rare despite being highly sought after. When we started working on UEBs there were only three known methods for construction, the algebraic, shift-and-multiply and Hadamard methods. In Chapter 3 of this thesis we give a new constructions of UEBs, based on quantum Latin squares and show that two of the existing methods are special cases of this new method. We also show that there exist UEBs obtainable from our method that are inequivalent to those obtainable by any previous methods.

In Chapter 6 we give a new characterization of UEBs as pairs of orthogonal quantum isometry Latin squares (QILS) which gives further possible avenues for construction. UEBs also arise as quantum bijections between a matrix algebra and a classical set as shown in Chapter 8. This connects quantum error correction to noncommutative topology and opens up new techniques to both fields. In Chapter 6 we prove the equivalence up to phase data of UEBs having certain extra properties, and maximal families of mutually unbiased bases, and give a new construction for these in Chapter 7.

Mutually unbiased bases (MUBs) are fundamental mathematical objects in quantum information that represent complementary observables. These are quantum observables that are as far apart as possible in the sense that, if one is measured then all possible outcomes for a measurement of the other become equally likely. MUBs have applications in many areas of quantum information such as, quantum key distribution, quantum state determination and reconstruction as well as quantum error correction. Maximal families of MUBs play a particularly important roll as they can perfectly distinguish density operators. MUBs have been studied since the early 1960s and yet, in non-prime dimension it is still an open question how many MUBs exist. In this thesis we give two new constructions of MUBs, the first in Chapter 4 is from quantum Latin squares and the second is a construction of maximal families of MUBs from a finite field in Chapter 7. Together with the result proving the correspondence between maximal families of MUBs and certain classes of UEBs, this thesis contributes to the study of MUBs. Further, the techniques developed show promise towards the ultimate goal of proving existence theorems for MUBs in arbitrary dimension.

In Chapter 5 we introduce a notion of orthogonality between quantum Latin isometry squares which allows quantum error codes to be built from these generalized structures. This gives the potential for new quantum error correcting schemes and also connects quantum error correction with the work on

quantum channels preserving pointer states, where we also show that quantum Latin isometry squares are the underlying mathematical structure.

Chapters 8 and 9 are based on joint work with David Reutter and Dominic Verdon which has thus far produced two published research papers [MRV18a, MRV18b] and enough other results for at least two more. Chapter 8 is based entirely on [MRV18a] and Chapter 9 is based partly on the same paper and partly on, as yet unpublished material from 2018. In Chapter 8 we introduce a 2-categorical framework for quantum sets, and quantum functions as well as for quantum graphs and quantum graph homomorphisms. We prove that this framework generalizes work in various areas including noncommutative topology, zero-error quantum channels and quantum nonlocal games.

Recently from the area of quantum non-local games many properties from classical graph theory have been given quantum analogues. These include quantum graph isomorphisms and quantum graph homomorphisms. These quantum analogues are framed as the existence of perfect strategies for bipartite non-local games where the participants are given access to quantum resources. A particular aim of that research is to find pairs of graphs which exhibit quantum advantage. Specifically, a pair of graphs are said to be *quantum pseudo telepathic* if they are quantum isomorphic but not isomorphic in the usual sense. In Chapter 9 we prove that the quantum graph homomorphisms and isomorphisms from quantum non-local games correspond precisely to our quantum functions and quantum bijections between classical sets. This allows the use of our categorical framework to prove results about quantum pseudo-telepathy. In Chapter 8 we also show that our framework captures and generalizes the noncommuative graphs and graph homomorphisms recently used in the study of zero-error quantum channels [DSW13, Sta16]. This is an active area of research and the categorical framework introduced is already being used to produce important results.

Below is a bullet point summary of the main results in this thesis:

- Introduction of QLS as a quantization of Latin squares (see Chapter 3, Section 3.1);
- A new construction method for UEBs inequivalent to existing methods (see Chapter 3, Section 3.4);
- a new construction of maximally entangled mutually unbiased bases from QLSs (see Chapter 4, Section 4.2);
- a new construction of quantum codes from orthogonal QILSs (see Chapter 5, Section 5.4.5);
- a new characterization of UEBs as pairs of orthogonal QILSs (see Chapter 5, Section 5.4.6);
- proof of the correspondence between maximal MUBs and partitioned UEBs (see Chapter 6, Section 6.5);
- a new construction of maximal MUBs from finite fields (see Chapter 7, Section 7.2.1);

- a new categorical framework for the study of quantum sets and quantum functions (see Chapter 8, Section 8.2.3);
- a new categorical framework for the study of quantum graphs and quantum graph homomorphisms (see Chapter 8, Section 8.4.4);
- proof that non-commutative graphs are captured and generalized by our categorical framework (see Chapter 8, Section 8.5);
- proof that quantum graph homomorphisms of classical graphs in the sense of Mančinska and Roberson [MR16] are captured by our framework (see Chapter 9, Section 9.2);
- proof that quantum graph isomorphisms of classical graphs in the sense of Atserias et al [AMR$^+$19] are captured by our framework (see Chapter 9, Section 9.3);
- proof that quantum pseudo telepathic pairs of graphs must have the same number of connected components (see Chapter 9, Section 9.5.2).

1.2 Related work

Before the paper on which Chapter 3 of this thesis is based came out in 2015 [MV15], there were two main constructions of unitary error bases. There was one method based on the representation theory of finite groups due to Knill in 1996 which gives rise to *nice error bases* [Kni96] and another due to Werner in 2001 giving rise to shift-and-multiply bases [Wer01] based on Latin squares and Hadamard matrices. A third method using only Hadamards was also known. In 2003 it was proven by Klappenecker and Rötteler that the first two methods above each produce bases inequivalent to the other. It was an open question as to whether other constructions existed for UEBs, and it was also unknown how the Hadamard UEBs were related to the other two. By introducing a new UEB construction method that generalizes Werner's method and the Hadamard method we answered these questions.

It has been known for some time that no more than $d+1$ MUBs can exist on a d dimensional Hilbert space and that for $d = p^n$ for some prime number p this upper bound is met [BBRV02]. In general dimension, and even for $d = 6$, the first non-prime power dimension, it is not known how many MUBs exist. There are various constructions of MUBs in prime power dimension, such as the Wootters and Field construction from a finite field [WF89], the construction from a commutative semifield due to Godsil and Roy [GR09] and a more general construction based on symplectic spreads by Abdukhalikov [Abd14]. In 2002 Bandyopadhyay et al made a key contribution to the field by showing that UEBs with a particular commuting structure which we refer to as *partitioned UEBs*, give rise to maximal families of MUBs. In Chapter 6 we prove the converse to this, and show that maximal families of MUBs in all dimensions are

characterized by partitioned UEBs. In Chapter 7 we give a new construction of maximal MUBs from finite fields that is easier to calculate than existing methods.

For general dimension, various attempts have been made to construct complete families of MUBs. Many links have been shown to exist between MUBs and mutually orthogonal Latin squares. Beth and Wocjan showed that in square dimension, families of MUBs can be constructed from mutually orthogonal Latin squares [BW04]. Taking a similar approach, we give a new construction for MUBs in square dimension from orthogonal quantum Latin squares in Chapter 4. This result has the potential to improve the known upper bounds for MUBs in some non-prime power dimensions, and opens up the possibility of a deeper understanding of MUBs through orthogonality of quantum Latin squares.

As mentioned above, there has been a lot of work recently in quantum non-local games on the quantum theory of graphs. Quantum graph homomorphisms were originally defined within the quantum non-local game framework by Mančinska and Roberson [MR16] and have been the focus of much research [SS12, AHKS06, CMN$^+$07, PT15, PSS$^+$16, Rob16]. Quantum graph isomorphisms were introduced in 2016 in a recently published paper by Atserias et al [AMR$^+$19]. As explained above pairs, of quantum pseudo telepathic graphs, are graphs which exhibit quantum advantage. As such they are highly sought after. The smallest pair of pseudo telepathic graphs known have 24 vertices; it is not known if any smaller pairs exist. Building on the framework introduced in Chapter 8 of this thesis and the results about connected components in Chapter 9, together with David Reutter and Dominic Verdon, we have proven that there are no pseudo telepathic pairs with 11 or fewer vertices. This is an important area as we try to ascertain where quantum advantage over classical computing can be gained as the advent of large scale quantum computing draws closer.

1.3 Outlook

Since we introduced quantum Latin squares and quantum shift-and-multiply bases in 2015 [MV15] (the basis for Chapter 3), various authors have built upon our work. In their 2017 paper Benoist and Nechita found that quantum Latin squares appear as bipartite unitaries that characterize quantum channels preserving certain matrix algebras [BN17]. They proposed an algorithm for sampling quantum Latin squares. Their work gives a physical interpretation to quantum Latin squares via the Stinespring dilation theorem [Sti55]. In later work we found that quantum Latin isometry squares are also algebra preserving quantum channels in the sense of Benoist and Nechita (see Chapter 5).

Reutter and Vicary introduced shaded diagrams for biunitaries in their 2016 paper [RV16]. They showed that quantum Latin squares, unitary error bases and Hadamards are all examples of different types of biunitary. They gave a high level description of the quantum shift-and-multiply method, and proposed new schemes for constructing UEBs and QLSs. For example, they showed that a QLS can be

constructed from a pair of Hadamard matrices.

Work by Verdon and Vicary makes use of quantum shift-and multiply bases to carry out teleportation protocols where the reference frames of the participants are misaligned [VV17, VV18]. This is an important development as we move toward the implementation of quantum communication systems which, in practice will need to be robust against reference frame error.

Quantum orthogonal arrays were introduced by Goyeneche et al in 2018, which generalize quantum Latin squares, producing quantum Latin cubes and quantum Latin hypercubes [GRDMŻ18]. They also proposed a notion of orthogonality between quantum Latin squares which we give a simplified characterization of in Chapter 5. They showed that orthogonal QLS give rise to perfect tensors, mathematical objects which are fundamental to quantum error correction.

In their 2018 paper Li and Wang showed that unlike in the bipartite case, masking of quantum information is possible for communication between three or more parties [LW18]. They showed a scheme for masking which used orthogonal quantum Latin squares in the sense of Chapter 4 of this thesis. This is an important result for quantum information security.

As mentioned above Chapters 8 and 9 are part of a body of work carried out in collaboration with Dominic Verdon and David Reutter. Since the publication of the paper on which Chapter 8 is based [MRV18a] was published there have been several papers making use of our framework and connecting quantum non-local games with noncommutative topology [Ban19b, BCF18, Ban19a, Soł19]. We have also made further progress ourselves. We have already published another paper utilizing the categorical structure to characterize in a high level way conditions for quantum pseudo telepathy [MRV18b]. We have further, as yet unpublished work, ruling out quantum pseudo telepathy between graphs with less than 11 vertices. We also have another paper in the pipeline concerning an explicit group theoretic construction for quantum pseudo telepathy, building on the results of [MRV18b].

Another paper which will be completed in the near future, based on joint work with Dominic Verdon, is a study of the complexity of completing quantum Latin squares. We show that this gives a new NP complete problem.

We finish this section with a list of open questions, research ideas and conjectures that arise out of the results in this thesis:

- We conjecture that there are nice error bases that are not quantum shift-and multiply and that both types of UEB are examples of a more general construction.
- What is the exact nature of the relationship between orthogonality of QLS and LS with mutually unbiased bases?
- Can mutually unbiased bases be constructed from orthogonal quantum Latin isometry squares?
- We would like to work out the conditions necessary for a quantum shift-and-multiply basis to be

partitioned into maximal families of operators. This would give rise to mutually unbiased bases as the eigenbases.

- We conjecture that many more links to quantum information will emerge from **QSet** and **QGraph** in the case of quantum morphisms between quantum sets.

1.4 Overview

The main chapters are designed to be mostly self contained but in Chapter 2 we give some preliminary background material, covering string diagrams, Frobenius algebras and the interacting algebras formulism mentioned in this chapter.

Part I concerns quantum Latin squares, their applications and generalizations. In Chapter 3 we introduce quantum Latin squares and use them to give a new construction method for UEBs. In Chapter 4 we introduce a first notion of orthogonality, called left orthogonality for QLS and give a construction for mutually unbiased bases using left orthogonal QLS. In Chapter 5 we give another definition of orthogonality for quantum Latin squares and their generalization, quantum Latin isometry squares. We give a construction for quantum codes using orthogonal quantum Latin isometry squares.

Part II concerns mutually unbiased bases and complex extensions of finite fields. In Chapter 6 we give a converse to the map taking a partitioned UEB to a maximal MUB and introduce graphical characterizations of UEBs, maximal MUBs and controlled Hadamards. In Chapter 7 we introduce a graphical representation of finite fields in Hilbert space and use it to give a new construction of maximal MUBs.

Part III concerns quantum sets, quantum functions and quantum graph theory. In Chapter 8 we give a 2-categorical framework for the study of quantum sets and quantum functions. We introduce another 2-category of quantum graphs and quantum homomorphisms and give a generalization of quantum graphs to define quantum relations. We show that structures arising in various different research areas are specific examples of structures in these two 2-categories. In Chapter 9 we prove that the quantum graph homomorphisms and isomorphisms of quantum non-local games are quantum homomorphisms and quantum isomorphisms between classical graphs. We illustrate how to move from the operational set up of non-local games to our abstract formulism by introducing the quantum function and bijection games. We also prove that pairs of graphs exhibiting quantum pseudo telepathy have the same multiset of sizes of connected components.

Chapter 2

Background

The Chapters 3 to 9 comprise the main body of this thesis and are designed to be largely self contained. Most of the necessary background will therefore be delayed until the main body. An exception to this is the diagrammatic language of categorical quantum mechanics which we find necessary to introduce below in Section 2.1 as it is utilized throughout this thesis and would detract from the narrative in the main body. We also introduce some background material in Section 2.2 concerning the central theme already discussed in the preface, namely interacting algebras and their generalizations. Finally in Section 2.3 we introduce the shaded graphical calculus which will be utilized in Chapters 5 and 8.

Before we begin, a well known result which is not difficult to prove and will be useful, is that isometric operators on finite-dimensional Hilbert spaces are always unitary [Mla91, page 130]. Since we will mainly be working with finite-dimensional Hilbert spaces we will make use of this to shorten proofs of unitarity.

2.1 An introduction to the graphical calculus

The graphical calculus of categorical quantum mechanics gives a diagrammatic notation through which certain kinds of problems are easier. The results of this thesis were all achieved using these high level techniques. The graphical calculus can be used to represent morphisms in any symmetric monoidal category. For much of this thesis we will be fixing the background symmetric monoidal category to be **FHilb** the category of finite-dimensional Hilbert spaces and linear maps. In the following we introduce the diagrammatic calculus with **FHilb** explicitly chosen as the background category. On the rare occasion when other background categories are required we will make this apparent to avoid confusion.

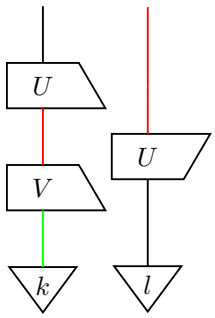
2.1.1 String diagrams

In order to read our diagrams the first thing to understand is that wires represent Hilbert spaces and boxes between wires are linear maps. We will use the convention that diagrams are read from bottom to

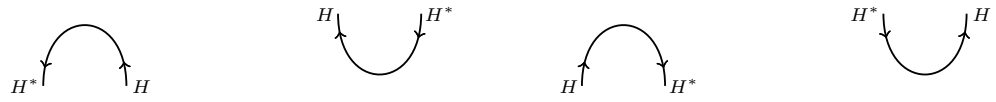
top. The composition of linear maps U and V is given by vertical composition and the tensor product is given by horizontal composition. We represent n-partite states by triangles with no wires in and n wires out. Scalars are represented by boxes with no wires in or out and can move freely around the diagram. Where the meaning is unambiguous we also represent scalars without boxes to the far left of diagrams. Adjoints are given by vertical mirror image, so asymmetry in the boxes representing linear maps is introduced to avoid ambiguity. With this in mind n-partite effects are inverted triangles with n wires in and none out. Different Hilbert spaces are denoted by different coloured wires or by labels.

Thus given Hilbert spaces $\mathcal{H}_1$(green), $\mathcal{H}_2$(red) and $\mathcal{H}_3$(black), linear maps $U : \mathcal{H}_2 \to \mathcal{H}_3$ and $V : \mathcal{H}_1 \to \mathcal{H}_2$ and states $|k\rangle \in \mathcal{H}_1$ and $|l\rangle \in \mathcal{H}_3$ we have the following diagrammatic rendering of $(i+1)UV|k\rangle \otimes U^\dagger|l\rangle$:

$(i+1)UV|k\rangle \otimes U^\dagger|l\rangle :=$ $(i+1)$



Given a Hilbert space H we denote the space of linear operators on H by $\mathcal{B}(H)$. Each Hilbert space H has a dual Hilbert space H^* defined to be the space of all linear maps $H \to \mathbb{C}$. In the graphical calculus we deal with duals by appending an orientation to our wires. We represent H^*as an oriented wire going in the opposite direction from H. The following linear maps characterize duality in **FHilb**:



$\langle\phi| \otimes |\psi\rangle \mapsto \langle\phi|\psi\rangle$ $\quad 1 \mapsto \mathbb{I}_H$ $\quad |\psi\rangle \otimes \langle\phi| \mapsto \langle\phi|\psi\rangle$ $\quad 1 \mapsto \mathbb{I}_H$ (2.1)

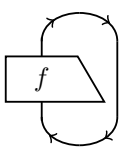
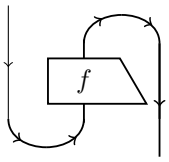
Note that in order to define the second and fourth linear maps we have used the fact that the space of linear operators on H, $\mathcal{B}(H) \cong H^* \otimes H \cong H \otimes H^*$. Also note that the first and fourth linear maps are mutual adjoints as are the second and third.

It can easily be checked that these linear maps, known as *cups* and *caps* fulfil the following equations known for obvious reasons as the *snake equations*:



(2.2)

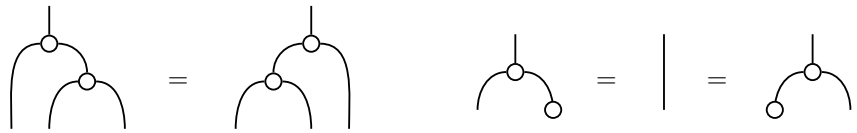
The trace and transpose of a linear operator f are given graphically by the following:

$\mathrm{tr}(f) :=$  $\qquad f^T :=$  (2.3)

2.1.2 Representing finite-dimensional C*-Algebras graphically

Finite-dimensional C^*-algebras can be seen as certain Frobenius algebras in **FHilb**. This categorical view of finite-dimensional C^*-algebras was introduced by Vicary [Vic10] and will play an important role throughout this thesis.

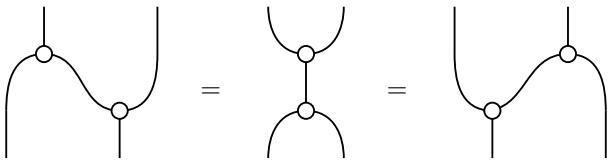
Definition 2.1.1 (Algebra)**.** Given a Hilbert space H and linear maps  $: H \otimes H \to H$ and  $: \mathbb{C} \to H$, $(H,$, $)$ is an *algebra* if the following equations are satisfied:

 (2.4)

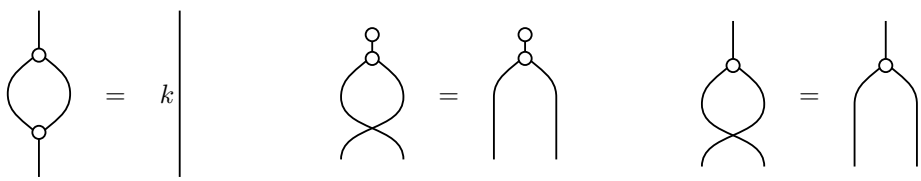
These equations represent *associativity* and *unitality* respectively.

A coalgebra $(H,$ , $)$ is defined similarly by taking the vertical reflection of equations (2.4). A coalgebra is *coassociative* and *counital*. The adjoint of an algebra is therefore a coalgebra and vice versa. Given an algebra and its adjoint coalgebra on H we define a *dagger Frobenius algebra* as follows:

Definition 2.1.2 (Dagger Frobenius algebra)**.** Given a Hilbert space H with algebra and coalgebra $:=$ †, $:=$ † we have that $(H,$, , , $)$ is a dagger Frobenius algebra if the following equations hold:

 (2.5)

Definition 2.1.3 (Special, symmetric, commutative)**.** A dagger Frobenius algebra is *quasi-special*, *symmetric* or *commutative* respectively if one of the following equations hold with $k \in \mathbb{C}$, $k \neq 0$:

 (2.6)

a) quasi-special $\qquad$ b) symmetric $\qquad$ c) commutative

A dagger quasi-special Frobenius algebra is *special* if $k = 1$ in the left hand side equation above.

We have chosen to represent the Hilbert space upon which a dagger Frobenius algebra is defined without orientation. This choice does not lead to ambiguity since any dagger Frobenius algebra on a Hilbert space H gives rise to a duality between H and itself in the following way. It can easily be checked that for any dagger Frobenius algebra $(H, \cup, \delta, \curlyvee, \varepsilon)$, the following linear maps satisfy the snake equations (2.2):



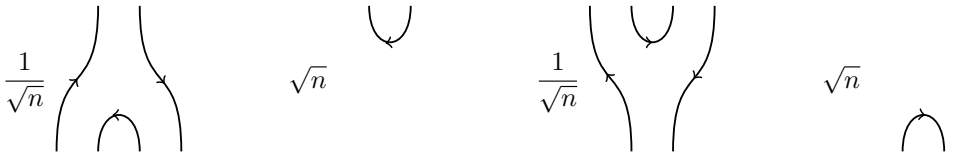
(2.7)

Dagger special symmetric Frobenius algebras (†-SSFAs) correspond precisely to finite-dimensional C^*-algebras:

Theorem 2.1.4 ([Vic10, Theorem 4.6])**.** *Every finite-dimensional C^*-algebra has a unique inner product making it a †-SSFA and every †-SSFA admits a unique norm making it a finite-dimensional C^*-algebra.*

We now give an important first example of a †-SSFA.

Example 2.1.5 (Endomorphism algebra)**.** The *endomorphism algebra* of an n-dimensional Hilbert space H is given by the following dagger special symmetric Frobenius algebra on $H \otimes H^* \cong \mathcal{B}(H)$:



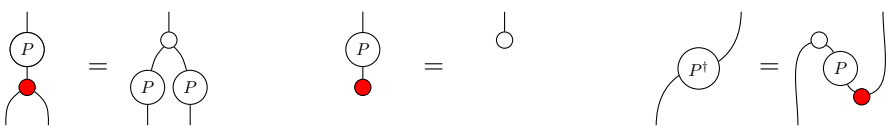
(2.8)

multiplication unit comultiplication counit (2.9)

This is $*$-isomorphic to the unique †-SSFA corresponding to the standard C^*-algebra defined on $\mathcal{B}(H)$ usually given without the normalization factors above.

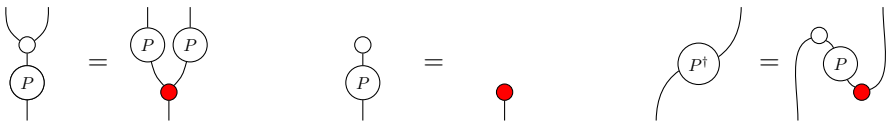
We now introduce homomorphisms and isomorphisms between Frobenius algebras which, in the case of †-SSFAs correspond precisely to $*$-homomorphisms and $*$-isomorphisms of finite-dimensional C^*-algebras. Given Frobenius algebras $(H, \cup, \delta, \curlyvee, \varepsilon)$ and $(G, \cup, \delta, \curlyvee, \varepsilon)$ we make the following definitions:

Definition 2.1.6 (Homomorphism of Frobenius algebras)**.** A linear map P obeying the following equations is a *homomorphism of Frobenius algebras*.



(2.10)

Definition 2.1.7 (Cohomomorphism of Frobenius algebras)**.** A linear map P obeying the following equations is a *cohomomorphism of Frobenius algebras*



(2.11)

An *isomorphism of Frobenius algebras* is both a homomorphism and a cohomomorphism.

Dagger special commutative Frobenius algebras play an important role in this thesis as they correspond to orthonormal bases of Hilbert spaces as we shall see in the next section.

2.1.3 Finite-dimensional Gelfand duality and dagger special commutative Frobenius algebras as orthonormal bases

Finite-dimensional commutative C^*-algebras correspond to dagger special commutative Frobenius algebras (†-SCFAs). We will see in this section that †-SCFAs correspond to orthonormal bases. This graphical treatment of Gelfand duality in the finite setting can be found in the work of Coecke, Pavlović and Vicary [CPV09].

First we show that given an orthonormal basis we have a †-SCFA. Given an orthonormal basis $|i\rangle, i \in [n]$ of an n-dimensional Hilbert space H we define a †-SCFA as follows:



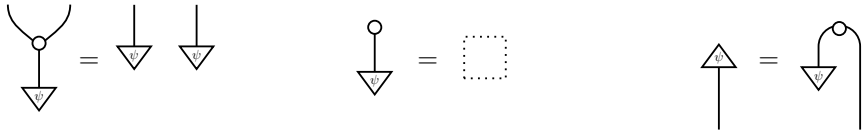
(2.12)



(2.13)

It can easily be checked that all the axioms are fulfilled. Conversely, given a †-SCFA we have an orthonormal basis. We first require the following definition.

Definition 2.1.8. Given a †-SCFA  on a Hilbert space H, a state $|\psi\rangle \in H$ is a *copyable element* of if the following equations hold:



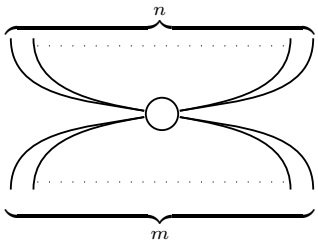
(2.14)

The copyable elements of a †-SCFA form an orthonormal basis.

Theorem 2.1.9 ([CPV09, Theorem 5.1.]). *Given a †-SCFA on a Hilbert space H, its copyable elements form an orthonormal basis of H and it is of the form of (2.12) and (2.13).*

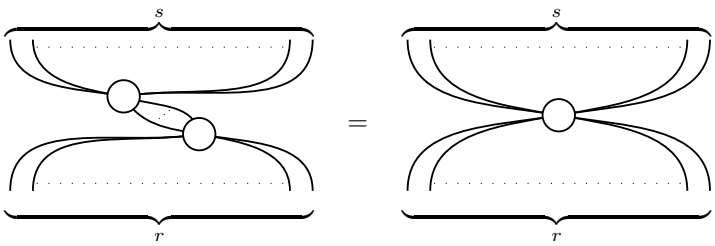
An immediate corollary of this is that any connected diagram made up of the four linear maps defined by (2.12) and (2.13) along with the identity on H and the swap map $\sigma : H \otimes H \to H \otimes H$ given by $\sigma(|i\rangle \otimes |j\rangle) = |j\rangle \otimes |i\rangle$ are uniquely determined by the overall number of input and output wires. We can therefore make the following definition without ambiguity.

Definition 2.1.10 (Spider). Any connected morphism from $H^{\otimes m}$ to $H^{\otimes n}$ built using the multiplication, comultiplication, unit and counit maps of a †-SCFA, as well as the identity and the swap map σ as above, is called a spider and is denoted as follows:



(2.15)

So any part of a diagram made up of connected spiders can be rewritten as any other as long as the total number of inputs and outputs are the same. We refer to this as the *spider merge* rule. For example we have the following:



(2.16)

Gelfand duality gives a way of interpreting commutative C^*-algebras as topological spaces. In the infinite setting this is as follows.

Theorem 2.1.11 (Gelfand duality). *The category with commutative C^*-algebras as objects and $*$-homomorphisms as morphisms is equivalent to the opposite of the category with compact Hausdorff spaces as objects and continuous functions as morphisms.*

Here we consider the restriction to the finite-dimensional setting where commutative C^*-algebras are equivalent to †-SCFAs. In this setting Gelfand duality reduces to the following.

Corollary 2.1.12 (Finite Gelfand duality). *The category with finite-dimensional commutative C^*-algebras as objects and $*$-homomorphisms as morphisms is equivalent to the opposite of the category* **Set** *with sets as objects and functions as morphisms.*

The correspondence between †-SCFAs and orthonormal bases above is a manifestation of this. A †-SCFA is equivalent to its set of copyable elements and a set X gives rise to a †-SCFA on $\mathbb{C}^{|X|}$ with orthonormal basis labelled by the elements of X. Cohomomorphisms of †-SCFA are the linear extensions of functions between sets. We will often use a Hilbert space equipped with a †-SCFA as an indexing leg for a set of linear maps.

We have seen that †-SCFAs correspond to orthonormal bases. Mutually unbiased bases have a special characterization in terms of †-SCFAs.

Definition 2.1.13 (Strong complementarity)**.** Given two †-SCFAs  and , they are *strongly complementary* if the following composite linear maps are both unitary:

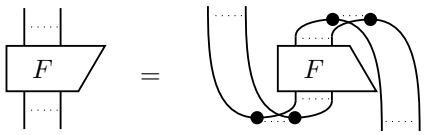


(2.17)

Theorem 2.1.14 ([ZV14], Theorem 9)**.** *A pair of †-SCFAs are strongly complementarity if and only if the corresponding bases are mutually unbiased.*

We end this section with a definition that captures the idea of a linear map being real valued with respect to a particular basis.

Definition 2.1.15 (●-real [DD16])**.** In a †-symmetric monoidal category, given an object A with a †-SCFA , a morphism $F : A^{\otimes n} \to A^{\otimes m}$ is *●-real* if:



(2.18)

2.2 Interacting algebras

As discussed in the Preface a central theme of this thesis is a series of generalization that starts with an Abelian group. The structure of an Abelian group can be characterized by the interactions of a pair of Frobenius algebras in Hilbert space. In this Section we present a diagrammatic characterization of Abelian groups which is due to Gogioso and Zeng [GZ15].

2.2.1 Abelian groups

First we define an Abelian group.

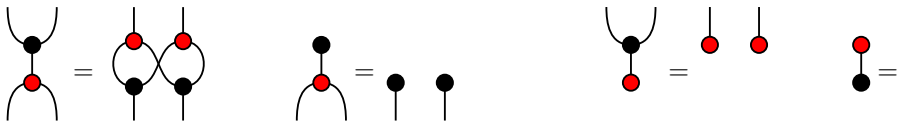
Definition 2.2.1 (Abelian group [LN97])**.** A set together with a binary operation is an *Abelian group* if it is closed, unital, associative, commutative and every element has an inverse.

We will now show how these axioms can be represented in Hilbert space. Let  be a †-SCFA. We can understand this, via Gelfand duality, to be a set indexing the elements of an Abelian group.

Unitality, associativity and commutativity. We introduce another Frobenius algebra which will represent the binary operator of the group. Let  be a †-quasi-special commutative Frobenius algebra (†-qSCFA). Since  is a commutative Frobenius algebra it is unital, associative and commutative by definition.

Closure. It is the interaction of red and black that gives us the structure of a group. We require that  is closed with respect to  this means that we need  to take pairs of black basis states to black basis states. This is equivalent to the following axiom:

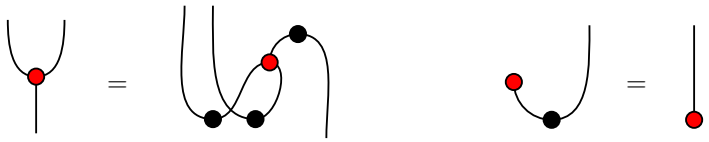
Definition 2.2.2 (Bialgebra)**.** A pair of unital associative algebras are a *bialgebra* if:



(2.19)

Note that the right hand side of the fourth equation is the empty diagram indicating the identity complex scalar 1.

Given Frobenius algebras  and , we call them Frobenius bialgebras if they obey the bialgebra rules. Note that the third bialgebra rule means that the red unit is copyable by, and thus a state of, the black basis. We will assume that the basis is ordered such that . Since we think of  as a binary operation taking black states to other black states, the morphism  should be real valued with respect to the black basis when considered as a linear map in Hilbert space. In other words it should be ●-real (see Definition 2.1.15). The following axiom gives this property:

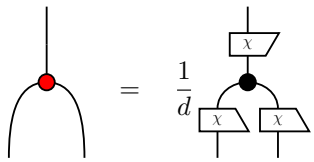


(2.20)

Inverses. Red and black being strongly complementary (see Definition 2.1.13) is equivalent to the binary operator having inverses, which gives us a Hopf algebra [DD16].

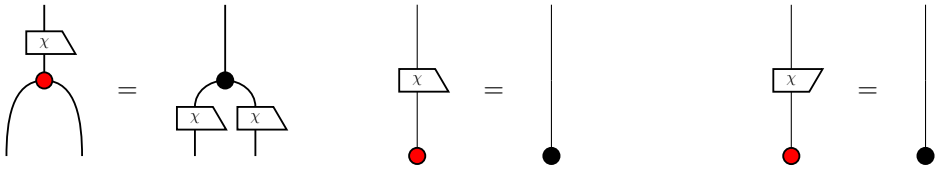
Character group. We shall now see that the basis states copyable by  form the character group, which has binary operator . Let χ be the change of basis linear map that maps the red basis to the

black basis up to a normalization factor, as follows:



(2.21)

By Theorem 2.1.14 we can see that the red and black bases are mutually unbiased. Another way of saying this is to say that χ is a Hadamard matrix [BBE+07]. This Hadamard is the Fourier transform of the group and its rows, which are the copyable states of the red basis, are the characters. Apart from the axioms for a Hadamard (see Definition 3.3.4 and Lemma 6.3.1), it can easily be shown that the following equations also hold which gives us the expected character theory.



(2.22)

Let $\chi_i(x) := \langle i|\chi|x\rangle$ so $\chi_i(x)$ is the ith character applied to an element of the group x. The left hand equation is then equivalent to; for all $i, x, y \in [n], \chi_i(x+y) = \chi_i(x)\chi_i(y)$ which is the expected property of a character. For a more detailed discussion of the above please refer to the 2015 paper by Gogioso and Zeng [GZ15]. We summarize the results of this subsection in the following theorem:

Theorem 2.2.3. *Given a d-dimensional Hilbert space with a †-qSCFA* *and a †-SCFA* *the following are equivalent [GZ15]:*

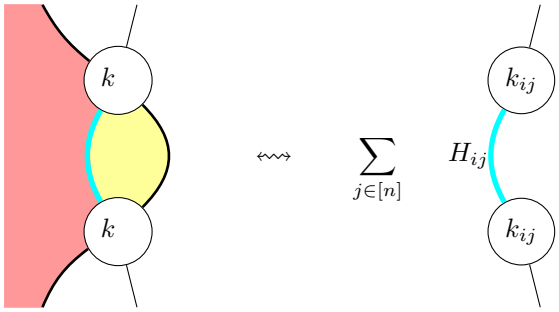
- *The copyable states of* *form an abelian complex group algebra under the linearly extended binary operator* *;*
- *The algebras*  *and*  *form a strongly complementary bialgebra and*  *is* ● *-real.*

2.2.2 Generalizations

More generally we can describe a (not necessarily Abelian) complex group algebra by the interaction between a pair of Frobenius algebras. The black algebra is still a †-SCFA but we now relax the condition that the red algebra needs to be commutative. All other axioms are the same as above for Abelian groups. In this thesis we continue this process of generalization obtaining the linear extension of a finite quasigroup and then stranger structures which go beyond the idea of red being the linear extension of a binary operator.

2.3 Shaded graphical calculus

In this thesis we make occasionally use of the shaded graphical calculus for monoidal 2-categories. For a rigorous higher categorical introduction please see one of [BMS12, Bar14, RV16]. For the purposes of this thesis it will suffice to view shaded string diagrams as indexed families of the string diagrams introduced above. With shaded diagrams we have the addition of the potential for regions in between wires and boxes to be coloured. The coloured regions represent sets which index every Hilbert space wire and linear map box that they touch. For example suppose we have indexing set $[m]$ represented by pink regions and $[n]$ represented by yellow. We have the following correspondence of string diagrams for $i \in [m]$ and $j \in [n]$:



The LHS shaded diagram represents the entire family of mn string diagrams and the RHS is a particular member of that family. Closed coloured regions represent a sum over the indexing set. The thick cyan wire represents, not a single Hilbert space but an indexed family of Hilbert spaces H_{ij} with $i \in [m]$ and $j \in [n]$. We have seen in Section 2.1.3 that we can use †-SCFAs in a similar way to represent indexed families of linear maps; the shaded graphical calculus becomes necessary to consider indexed families of linear maps on different Hilbert spaces.

Part I

Quantum Latin squares

Chapter 3

Quantum shift-and-multiply bases

In this chapter we introduce *quantum Latin squares*, combinatorial quantum objects which generalize classical Latin squares, and investigate their applications in quantum computer science. Our main results are on applications to *unitary error bases* (UEBs), basic structures in quantum information which lie at the heart of procedures such as teleportation, dense coding and error correction. We present a new method for constructing a UEB from a quantum Latin square equipped with extra data. Developing construction techniques for UEBs has been a major activity in quantum computation, with three primary methods proposed: *shift-and-multiply*, *Hadamard*, and *group-theoretic*. We show that our new approach simultaneously generalizes the shift-and-multiply and Hadamard methods. Furthermore, we explicitly construct a UEB using our technique which we prove cannot be obtained from any of these existing methods.

3.1 Introduction

We begin with the definition of a quantum Latin square.

Definition 3.1.1. A *quantum Latin square of order n* is an n-by-n array of elements of the Hilbert space $\mathbb{C}^n$, such that every row and every column is an orthonormal basis.

Example 3.1.2. Here is a quantum Latin square given in terms of the computational basis elements

$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\} \subset \mathbb{C}^4$:

$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$
$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$
$\|3\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$

It can readily be checked that along each row, and along each column, the elements form an orthonormal basis for $\mathbb{C}^4$. We can compare this to the classical notion of Latin square [FY34].

Definition 3.1.3. A *classical Latin square of order* n is an n-by-n array of integers in the range $\{0, \ldots, n-1\}$, such that every row and column contains each number exactly once.

Remark 1. *An alternative characterisation of a Latin square is as the Cayley table for a finite quasigroup [Hal45]. A quasigroup* Q *is a set together with a closed binary operator such that for each pair of elements* $a, b \in Q$ *there exist unique* x *and* y *in* Q *such that:*

$$a * x = b,$$
$$y * a = b.$$

By interpreting a number $k \in \{0, \ldots, n-1\}$ as a computational basis element $|k\rangle \in \mathbb{C}^n$, we can turn an array of numbers into an array of Hilbert space elements:

3	1	0	2
1	0	2	3
2	3	1	0
0	2	3	1

$\rightsquigarrow$

$\|3\rangle$	$\|1\rangle$	$\|0\rangle$	$\|2\rangle$
$\|1\rangle$	$\|0\rangle$	$\|2\rangle$	$\|3\rangle$
$\|2\rangle$	$\|3\rangle$	$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|2\rangle$	$\|3\rangle$	$\|1\rangle$

. (3.1)

It is easy to see that the original array of numbers being a classical Latin square implies that the corresponding grid of Hilbert space elements is a quantum Latin square made up of permutations of a single orthonormal basis. However, as Example 3.1.2 makes clear, not every quantum Latin square is of this form.

The main results of this chapter are on the construction of *unitary error bases* (UEBs) [KR03], also known as unitary operator bases. These are basic structures in quantum information which play a central role in quantum teleportation [BBC+93], dense coding [GCA+12] and error correction [Sho96]. Since

UEBs are hard to find, and given their wide applicability, construction techniques for UEBs have been widely studied [Kni96, KR03, Wer01, GS14]. In this chapter, we propose a new method for construction of UEBs:

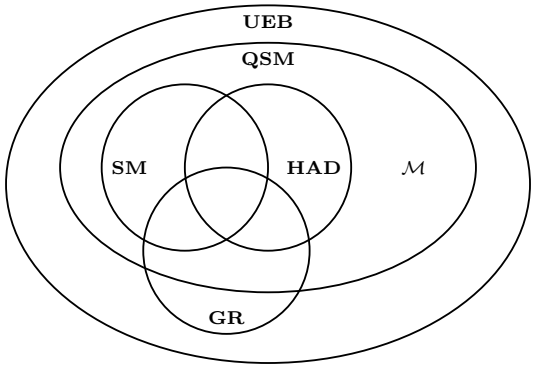
- Quantum shift-and-multiply method (**QSM**). Requires a quantum Latin square and a family of Hadamard matrices. (See Definition 3.4.4.)

We compare this to the other methods that have been proposed in the literature:

- Shift-and-multiply method (**SM**). Requires a classical Latin square and a family of Hadamard matrices. (See Definition 3.5.1.)
- Hadamard method (**HAD**). Requires a pair of mutually-unbiased bases. (See Definition 3.6.1.)
- Group-theoretic method (**GR**). Requires a finite group equipped with a projective representation, satisfying certain properties. (See Definition 3.7.2.)

Our theorems concern the relationships between these constructions. In Theorems 3.5.2 and 3.6.2, we prove that **QSM** contains **SM** and **HAD** as special cases. We also use **QSM** to construct a concrete unitary error basis $\mathcal{M}$ (Example 3.4.5), and prove that it is not equivalent to one arising from **SM**, **HAD** or **GR** (Corollaries 3.5.12, 3.6.7 and 3.7.5 respectively.)

The relationships between these constructions, up to a standard notion of equivalence of UEBs (see Definition 3.4.2), are indicated by the following Venn diagram:



(3.2)

Our work strongly extends previous results, in an area that has not seen progress since 2003. But there is much still to be settled: in particular, we do not know whether **GR** is a subset of **QSM**, or whether **QSM** equals **UEB**.

Before we get into the main results of this Chapter we will take a brief digression in Section 3.2 to discuss quantum Latin squares from the perspective of interacting algebraic structures (See Section 2.2) this is a theme which will recur throughout this thesis.

3.2 Interacting algebraic structures in Hilbert space

An n-by-n Latin square can be represented as a morphism in **Set** of the form $L : A \times A \to A$ for some n element set A as follows. Define $L(i, j)$ to be the the i, jth entry in the grid. So the mapping in equation 3.1 is an instance of Gelfand duality (see Section 2.1.3) and we have a morphism in **FHilb**, $L : A \otimes A \to A$ for some n dimensional Hilbert space with †-SCFA (or alternatively orthonormal basis) A. This is just the linear extension of the function L. The properties of a Latin square can now be stated in terms of the interaction between the algebra A and the algebraic structure L, in a similar way to the Abelian groups which we saw in Section 2.2. The main difference is that L is a quasigroup, having less structure than an Abelian group. In particular a quasigroup is not necessarily commutative or even associative. We now utilise the graphical calculus to discuss the interaction between L and A.

Graphically, let L be represented by  and A by . L is a real valued, closed binary operation with respect to A and has left and right inverses so equations (2.20) and (2.17) hold as well as the left hand two equations of (2.19) (but not the others since is not unital). We therefore have the following axiomatisation of Latin squares which first appeared in the present author's MSc Thesis [Mus14]:

Proposition 3.2.1 (See [Mus14],Proposition 3.2)**.** *Let A be an n dimensional Hilbert space with †-SCFA also denoted A and represented as* *. Let $L : A \otimes A \to A$ be a linear map represented by* *. L is a Latin square on the set of elements of A if the following hold:*

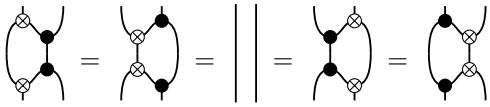
L is a binary operator on A

 (3.3)

L is real with respect to A

 (3.4)

Quasi-complementarity

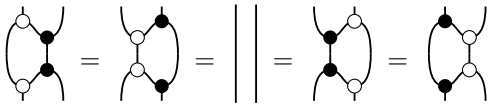
 (3.5)

The final condition which we refer to as *quasi-complementarity* ensures that each row and column of L is an orthonormal basis. This is the only axiom necessary for a QLS.

Proposition 3.2.2. *Let A be an n dimensional Hilbert space with †-SCFA also denoted A and represented*

as . *Let* $\psi : A \otimes A \to A$ *be a linear map represented by* . *ψ is a quantum Latin square on the set of elements of A if the following holds:*

Quasi-complementarity



(3.6)

Remark 2. *While states in a Latin square are restricted to being elements of the algebra A, QLS states can be a superposition of elements of A. In this sense a quantum Latin square is 'quantum'. In Part III we will explore two other approaches to 'quantization'.*

There are interesting connections between Hadamard matrices, unitary error bases and quantum Latin squares. In Section 3.3 we show that a quantum Latin square can be constructed from any Hadamard matrix. Hadamard matrices are mathematically equivalent to the data for a pair of *mutually unbiased bases* [BBE+07], the study and classification of which is a major activity in quantum computer science [MDG+13, DCK+13, BČL+16, SHB+12]. It has also been shown that in some cases a family of mutually unbiased bases can be extracted from a UEB [BBRV02]. So quantum Latin squares can be built from Hadamards, which can be built from UEBs. All of these objects are examples of Biunitaries as shown in a 2016 paper by Ruetter and Vicary. We will discuss biunitaries further in Chapter 5 Section 5.3.

3.3 Quantum Latin squares from Hadamard matrices

In this section we introduce some basic properties of quantum Latin squares, show how to construct a quantum Latin square from a Hadamard matrix, and prove that our quantum Latin square of Example 3.1.2 is not equivalent to one arising in this way.

We begin by developing a precise notation for working with quantum Latin squares. Throughout, we assume we are working with a quantum Latin square of order n, and that indices i, j, k, p, q range from 0 to $n-1$.

Definition 3.3.1. For a quantum Latin square Φ, we define the following:

- Φ_i is the matrix whose columns are the entries of the ith row of Φ;
- $|\Phi_{ij}\rangle \in \mathbb{C}^n$ is the Hilbert space element at the ith row and jth column of Φ;
- $\Phi_{ijk} := \langle k|\Phi_{ij}\rangle \in \mathbb{C}$ is the coefficient of the basis vector $|k\rangle$.

For a matrix M, it is a standard notation to write M_{ij} for the element at the ith row and jth column. Combining this with Definition 3.3.1, we have the following:

$$(\Phi_i)_{jk} = \Phi_{ikj}. \tag{3.7}$$

Note that the order of the final two indices changes.

Given a collection of numbers $\Phi_{ijk} \in \mathbb{C}$, we can easily identify when they arise from a quantum Latin square. For a matrix M, we write M^* for the conjugate matrix, M^{T} for the transpose matrix, and $M^\dagger = (M^*)^{\mathrm{T}} = (M^{\mathrm{T}})^*$ for the conjugate transpose matrix.

Lemma 3.3.2. *A family of numbers $\Phi_{ijk} \in \mathbb{C}$ arise from a quantum Latin square if and only if they satisfy the following properties for all i, p, q:*

$$\textstyle\sum_j \Phi^*_{ipj}\Phi_{iqj} = \delta_{pq}, \text{ or equivalently the matrices } \Phi_i \text{ are unitary and,} \tag{3.8}$$

$$\textstyle\sum_j \Phi^*_{pij}\Phi_{qij} = \delta_{pq}. \tag{3.9}$$

Proof. Equations (3.8) and (3.9) are exactly the condition that the rows and columns, respectively, of the quantum Latin square form orthonormal bases. Unitarity of Φ_i means precisely $(\Phi_i^\dagger \Phi_i)_{pq} = \delta_{pq}$, which expands to $\sum_j (\Phi_i^\dagger)_{pj}(\Phi_i)_{jq} = \sum_j \Phi^*_{ipj}\Phi_{iqj} = \delta_{pq}$. (Recall that for an operator O on a finite-dimensional Hilbert space, $OO^\dagger = \mathbb{I}_n$ if and only if $O^\dagger O = \mathbb{I}_n$.) □

The condition (3.9) equivalently says that the matrices formed by the *columns* of the Latin square are unitary, but this is not a fact that we will need directly.

There are certain trivial ways to transform a quantum Latin square into a different quantum Latin square, which we use to define a notion of equivalence.

Definition 3.3.3. Two quantum Latin squares are *equivalent* when one can be obtained from the other by permuting rows and columns, multiplying rows and columns by unit complex numbers, and applying a fixed unitary to every element. Algebraically, quantum Latin squares Φ and Ψ are equivalent when there exists some unitary U, diagonal unitary D, permutation matrix P, permutation σ, and a family of unit complex numbers c_j, such that the following holds:

$$\Psi_j = c_j U \Phi_{\sigma(j)} P D. \tag{3.10}$$

We now give the standard definition of a Hadamard matrix, as a square matrix with entries of absolute value 1 which is proportional to a unitary matrix.

Definition 3.3.4 (See [TŻ06], Definition 2.1)**.** A *Hadamard matrix of order* n is an n-by-n matrix H with the following properties for all i, j, which we write in both matrix and index form:

$$|H_{ij}| = 1, \qquad H_{ij}H^*_{ij} = 1, \tag{3.11}$$

$$HH^\dagger = n\,\mathbb{I}_n, \qquad \textstyle\sum_p H_{ip}H^*_{jp} = n\,\delta_{ij}, \tag{3.12}$$

$$H^\dagger H = n\,\mathbb{I}_n, \qquad \textstyle\sum_p H^*_{pi}H_{pj} = n\,\delta_{ij}. \tag{3.13}$$

Definition 3.3.5 (See [Wer01], Section 4)**.** Two Hadamard matrices are *equivalent* when one can be obtained from the other by permuting rows and columns, and multiplying rows and columns by unit complex numbers. Algebraically, Hadamard matrices H and G are equivalent if there exist P_1, P_2 permutation matrices and D_1, D_2 unitary diagonal matrices such that:

$$G = D_1P_1HP_2D_2. \tag{3.14}$$

We now give the construction of a quantum Latin square from a Hadamard matrix.

Definition 3.3.6. For a square matrix M, let $\mathrm{diag}(M, i)$ be the diagonal matrix whose diagonal entries are given by the ith row of M:

$$\mathrm{diag}(M, i)_{jk} := \delta_{jk}M_{ij}. \tag{3.15}$$

Definition 3.3.7. For a Hadamard matrix H of order n, its *associated quantum Latin square* $\Phi[H]$ of order n is defined as follows:

$$\Phi[H]_j := \tfrac{1}{n}H\mathrm{diag}(H, j)^\dagger H^\dagger. \tag{3.16}$$

We will refer to a quantum Latin square constructed in this way as a *Hadamard quantum Latin square*.

Theorem 3.3.8. *The associated quantum Latin square construction is correct.*

Proof. To establish property (3.8), we note that $\Phi[H]_j$ is the composite of three unitary matrices, and is therefore unitary. To verify (3.9), we write expression (3.16) in index form:

$$\begin{aligned}\Phi[H]_{qij} &\overset{(3.7)}{=} (\Phi[H]_q)_{ji} \overset{(3.16)}{=} \tfrac{1}{n}\textstyle\sum_{rs} H_{jr}\mathrm{diag}(H, q)^\dagger_{rs}H^\dagger_{si} \\ &\overset{(3.15)}{=} \tfrac{1}{n}\textstyle\sum_{rs} H_{jr}H^*_{qr}\delta_{rs}H^*_{is} = \tfrac{1}{n}\textstyle\sum_r H_{jr}H^*_{qr}H^*_{ir}.\end{aligned} \tag{3.17}$$

We then perform the following calculation:

$$\begin{aligned}&\textstyle\sum_j \Phi[H]^*_{pij}\Phi[H]_{qij} \overset{(3.17)}{=} \tfrac{1}{n^2}\textstyle\sum_j \big(\sum_r H^*_{jr}H_{pr}H_{ir}\big)\big(\sum_s H_{js}H^*_{qs}H^*_{is}\big) \\ &= \tfrac{1}{n^2}\textstyle\sum_{rs}\big(\sum_j H^*_{jr}H_{js}\big)H_{pr}H_{ir}H^*_{qs}H^*_{is} \overset{(3.13)}{=} \tfrac{1}{n}\textstyle\sum_{rs}\delta_{rs}H_{pr}H_{ir}H^*_{qs}H^*_{is}\end{aligned}$$

$$= \tfrac{1}{n}\sum_r H_{pr}H^*_{qr}H_{ir}H^*_{ir} \overset{(3.11)}{=} \tfrac{1}{n}\sum_r H_{pr}H^*_{qr} \overset{(3.12)}{=} \delta_{pq}. \tag{3.18}$$

In the second equality here, the sum is being reorganized. □

We now establish a lemma which we will use to prove Lemma 3.3.10 and later Proposition 3.6.4.

Lemma 3.3.9. *Let σ be the permutation associated with the permutation matrix P such that $P = \sum_k |\sigma(k)\rangle\langle k|$ and D be a diagonal unitary matrix. Then the following equations hold:*

$$\mathrm{diag}(PH, i) = \mathrm{diag}(H, \sigma(i)) = \mathrm{diag}(H_{\sigma(i),0}, ..., H_{\sigma(i),n-1}), \tag{3.19}$$

$$\mathrm{diag}(HP, i) = \mathrm{diag}(H_{i,\sigma(0)}, ..., H_{i,\sigma(n-1)}), \tag{3.20}$$

$$\mathrm{diag}(DH, i) = D_{ii}\,\mathrm{diag}(H, i), \tag{3.21}$$

$$\mathrm{diag}(HD, i) = D\,\mathrm{diag}(H, i) = \mathrm{diag}(H, i)D. \tag{3.22}$$

Proof. Straightforward calculation.

Lemma 3.3.10. *Equivalent Hadamard matrices give rise to equivalent quantum Latin squares.*

Proof. Let G and H be equivalent Hadamard matrices, P be a permutation matrix with associated permutation σ and D_1, D_2 be diagonal unitary matrices. We will prove equivalence on a case-by-case basis.

Suppose $G = PH$. Then we have the following, where we use the fact that $P^{-1} = P^\dagger = P^T$:

$$\begin{aligned}
\Phi[G]_j &\overset{(3.16)}{=} \tfrac{1}{n} PH\,\mathrm{diag}(PH, j)^\dagger H^\dagger P^{-1} \\
&\overset{(3.19)}{=} \tfrac{1}{n} PH\,\mathrm{diag}(H, \sigma(j))^\dagger H^\dagger P^{-1} \\
&\overset{(3.10)}{\sim} \tfrac{1}{n} H\,\mathrm{diag}(H, j)^\dagger H^\dagger \overset{(3.16)}{=} \Phi[H]_j.
\end{aligned}$$

Now consider $G = HP$:

$$\begin{aligned}
\Phi[G]_j &\overset{(3.16)}{=} \tfrac{1}{n} HP\,\mathrm{diag}(HP, j)^\dagger P^{-1} H^\dagger \\
&\overset{(3.20)}{=} \tfrac{1}{n} HP\,\mathrm{diag}(H_{j,\sigma(0)}, ..., H_{j,\sigma(n-1)})^\dagger P^{-1} H^\dagger \\
&\overset{(3.30)}{=} \tfrac{1}{n} HPP^{-1}\,\mathrm{diag}(H, j)^\dagger H^\dagger \\
&= \tfrac{1}{n} H\,\mathrm{diag}(H, j)^\dagger H^\dagger \overset{(3.16)}{=} \Phi[H]_j.
\end{aligned}$$

Finally, suppose $G = D_1 H D_2$, with $D_1 = \mathrm{diag}(c_1, \ldots, c_n)$, where $|c_i| = 1$. Then we calculate as follows:

$$\begin{aligned}
\Phi[G]_j &\overset{(3.16)}{=} \tfrac{1}{n} D_1 H D_2 \mathrm{diag}(D_1 H D_2, j)^\dagger D_2^\dagger H^\dagger D_1^\dagger \\
&\overset{(3.21)}{=} \tfrac{1}{n} D_1 H D_2 c_j \mathrm{diag}(H D_2, j)^\dagger D_2^\dagger H^\dagger D_1 \\
&\overset{(3.22)}{=} \tfrac{1}{n} D_1 H D_2 c_j \mathrm{diag}(H, j)^\dagger D_2 D_2^\dagger H^\dagger D_1 \\
&= \tfrac{1}{n} D_1 H D_2 c_j \mathrm{diag}(H, j)^\dagger H^\dagger D_1 \\
&\overset{(3.10)}{\sim} \tfrac{1}{\sqrt{n}} \mathrm{diag}(H, j)^\dagger H^\dagger \\
&\overset{(3.10)}{\sim} \tfrac{1}{n} H \mathrm{diag}(H, j)^\dagger H^\dagger \overset{(3.16)}{=} \Phi[H]_j.
\end{aligned}$$

This completes the proof. □

Not all quantum Latin squares are of this form and indeed the QLS from Example 3.1.2 does not arise in this way, even up to equivalence. We defer the proof of this until the end of Section 3.6 as it makes use of some results from later in this chapter.

Proposition 3.3.11. *The quantum Latin square given in Example 3.1.2 is not equivalent to a quantum Latin square constructed from a Hadamard matrix.*

3.4 Unitary error bases from quantum Latin squares

In this section we define unitary error bases, and present our new *quantum shift-and-multiply* construction, which produces a unitary error basis from a quantum Latin square equipped with a family of Hadamard matrices. We then introduce an example UEB $\mathcal{M}$, which will play an important role in later sections where we show that it cannot arise from the shift-and-multiply, Hadamard or group-theoretic methods, even up to equivalence.

We begin with the definition of unitary error basis. As remarked in the introduction, these structures play a central role in quantum computation.

Definition 3.4.1 (See [KR03], Section 1)**.** For a Hilbert space H of dimension n, a *unitary error basis* (or *unitary operator basis*) is a family of n^2 unitary matrices $U_{ij} : H \to H$ which form an orthogonal basis:

$$\mathrm{Tr}(U_{ij}^\dagger U_{i'j'}) = \delta_{ii'}\delta_{jj'} n. \tag{3.23}$$

There is a standard notion of equivalence of unitary error bases, which we recall here.

Definition 3.4.2 (See [KR03], Section 2)**.** Two families of unitary matrices $\mathcal{A}$, $\mathcal{B}$ are *equivalent* if there are unitary matrices U and V, such that for any element $A \in \mathcal{A}$, there is an element $B \in \mathcal{B}$ and a unit

complex number c such that the following holds:

$$B = cUAV. \tag{3.24}$$

The following simple lemma will be useful later.

Lemma 3.4.3. *Let D be a diagonal matrix, and A be a square matrix which is zero along the main diagonal, such that D and A are composable. Then DA is zero along the main diagonal.*

We now define the main construction of focus in this chapter. This construction is similar to Werner's shift-and-multiply method [Wer01], the difference being that ours is in terms of *quantum* Latin squares. As usual, we take all indices in the range 0 to $n-1$.

Definition 3.4.4 (Quantum shift-and-multiply method)**.** Let Φ be a quantum Latin square of order n, and H_j be a family of n Hadamard matrices of order n. Then the associated *quantum shift-and-multiply basis* has the following elements:

$$S_{ij} := \Phi_j \mathrm{diag}(H_j, i). \tag{3.25}$$

In words, the (i,j) entry of the quantum shift-and-multiply basis is the matrix given by the jth row of the quantum Latin square, composed with the diagonal matrix formed from the ith row of the jth Hadamard matrix.

We illustrate this with an example. This example will play a central role, as we will show in the remainder of the chapter that it cannot be obtained, even up to equivalence, by any of the existing methods of unitary error basis construction.

Example 3.4.5. The quantum shift-and-multiply basis $\mathcal{M}$ is constructed from the quantum Latin square of Example 3.1.2, and from the following family of Hadamard matrices:

$$H_0 = H_1 = H_2 = H_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{3.26}$$

The resulting family of 16 matrices is listed in Section 3.8.1.

We now show that quantum shift-and-multiply bases are unitary error bases. This has similarities with Werner's original proof [Wer01] for standard shift-and-multiply bases (see Section 3.5), but our use of quantum Latin squares requires nontrivial extra ideas.

Theorem 3.4.6. *Quantum shift-and-multiply bases are unitary error bases.*

Proof. First, we note that the elements $S_{ij} = \Phi_j \mathrm{diag}(H_j, i)$ are unitary, since they are composites of unitary matrices: the matrix Φ_j is the jth row of a quantum Latin square, and hence unitary by Lemma 3.3.2; and $\mathrm{diag}(H_j, i)$ is a diagonal matrix with unit complex numbers along the diagonal, and hence unitary.

We must establish the following trace property:

$$\mathrm{Tr}(S_{ij}^\dagger S_{i'j'}) = n\,\delta_{ii'}\delta_{jj'}. \tag{3.27}$$

We first consider the case that $j = j'$ and $i = i'$. By unitarity of S_{ij} we have $S_{ij}S_{i'j'}^\dagger = \mathbb{I}_n$, with $\mathrm{Tr}(\mathbb{I}_n) = n$, and so the condition follows.

Next we consider the case that $j = j'$ and $i \neq i'$. We perform the following calculation:

$$\begin{aligned}\mathrm{Tr}(S_{ij}^\dagger S_{i'j}) &\overset{(3.25)}{=} \mathrm{Tr}\left(\mathrm{diag}(H_j, i)^\dagger \Phi_j^\dagger \Phi_j \mathrm{diag}(H_j, i')\right) \\ &\overset{(3.8)}{=} \mathrm{Tr}\left(\mathrm{diag}(H_j, i)^\dagger \mathrm{diag}(H_j, i')\right).\end{aligned}$$

The final expression is equal to the inner product of rows i and i' of the Hadamard H_j. Since distinct rows of a Hadamard are orthogonal, the result is zero as required.

It remains to consider the case that $j \neq j'$. We use the cyclic property of the trace to rearrange our trace expression:

$$\begin{aligned}\mathrm{Tr}(S_{ij}^\dagger S_{i'j'}) &\overset{(3.25)}{=} \mathrm{Tr}\left(\mathrm{diag}(H_j, i)^\dagger \Phi_j^\dagger \Phi_{j'} \mathrm{diag}(H_{j'}, i')\right) \\ &= \mathrm{Tr}\left(\mathrm{diag}(H_{j'}, i')\mathrm{diag}(H_j, i)^\dagger \Phi_j^\dagger \Phi_{j'}\right).\end{aligned} \tag{3.28}$$

Inside the trace there is the composite $\mathrm{diag}(H_{j'}, i')\mathrm{diag}(H_j, i)^\dagger$, which is diagonal. There is also $\Phi_j^\dagger \Phi_{j'}$, which by the following argument is zero along the diagonal:

$$(\Phi_j^\dagger \Phi_{j'})_{kk} = \textstyle\sum_l (\Phi_j^\dagger)_{kl}(\Phi_{j'})_{lk} = \sum_l (\Phi_j^*)_{lk}(\Phi_{j'})_{lk} \overset{(3.7)}{=} \sum_l \Phi_{jkl}^* \Phi_{j'kl} \overset{(3.9)}{=} \delta_{jj'} = 0. \tag{3.29}$$

Hence by Lemma 3.4.3, expression (3.28) is zero as required. □

3.5 Shift-and-multiply method

The shift-and-multiply method of Werner [Wer01], which was a direct inspiration for our own results, can straightforwardly be seen as a special case of our quantum shift-and-multiply method. Our focus in this section is the proof that the unitary error basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a shift-and-multiply basis, and thus that the shift-and-multiply bases are *strictly* contained within the quantum

shift-and-multiply bases.

Definition 3.5.1. A *shift-and-multiply basis* is a quantum shift-and-multiply basis where the quantum Latin square is a classical Latin square.

Corollary 3.5.2. *Every shift-and-multiply basis is a quantum shift-and-multiply basis.*

Proof. Follows immediately from Definitions 3.1.3 and 3.5.1.

Monomial matrices will be crucial to our proof strategy.

Definition 3.5.3. A *monomial matrix* is a square matrix with exactly one nonzero entry in each row and each column. Equivalently, it is any matrix A which can be expressed as $A = D_A P_A$, where D_A is an invertible diagonal matrix and P_A is a permutation matrix.

Lemma 3.5.4. *Let σ be a permutation, $P = \sum_k |\sigma(k)\rangle\langle k|$ be the corresponding permutation matrix, and $D_1 = \sum_k d_k |k\rangle\langle k|$ and $D_2 = \sum_k d_{\sigma(k)} |k\rangle\langle k|$ be diagonal matrices. Then the following holds:*

$$D_1 P = P D_2. \tag{3.30}$$

Proof. We perform the following straightforward calculation:

$$\begin{aligned} D_1 P &= P P^\dagger D_1 P = P\big(\textstyle\sum_{ijk} |i\rangle\langle\sigma(i)|d_j|j\rangle\langle j|\sigma(k)\rangle\langle k|\big) \\ &= P\big(\textstyle\sum_{ik} d_{\sigma(k)} |i\rangle\langle\sigma(i)|\sigma(k)\rangle\langle k|\big) = P\big(\textstyle\sum_i d_{\sigma(i)} |i\rangle\langle i|\big) = P D_2. \end{aligned}$$

This completes the proof. □

Lemma 3.5.5. *The set of monomial matrices is closed under composition, taking inverses, taking adjoints, and multiplication by nonzero complex scalars.*

Proof. Straightforward.

Definition 3.5.6. A square matrix A is *monomializable* if there exists a unitary matrix U such that $UAU^\dagger$ is monomial.

Definition 3.5.7. A family of square matrices $A_1, ..., A_n$ are *simultaneously monomializable* if they are all monomializable by the same unitary matrix U.

We establish the following propositions, the first of which is adapted and generalized to suit our purposes from the literature.

Proposition 3.5.8 (See [KR03], final part of the proof of Theorem 3)**.** *If a family $\mathcal{S}$ of unitary matrices containing the identity is equivalent (in the sense of Definition 3.4.2) to a family of monomial matrices, then the members of $\mathcal{S}$ are simultaneously monomializable.*

Proof. Let $\mathcal{S} = \{S_i\}$ be a family of unitary matrices with $S_0 = \mathbb{I}_n$. Suppose S_i is equivalent to some monomial family $\mathcal{T} = \{T_i\}$ with $T_i = c_i U S_i V$, such that each c_i is a complex number of norm 1, and U, V are unitary matrices. We then perform the following calculation:

$$\frac{c_0}{c_j} T_j T_0^\dagger = \frac{c_0}{c_j}(c_j U S_j V)(c_0 U S_0 V)^\dagger = c_0 c_0^* U S_j V V^\dagger \mathbb{I}_n U^\dagger = U S_j U^\dagger. \tag{3.31}$$

The left hand side is monomial by Lemma 3.5.5, hence U simultaneously monomializes S_i. □

Proposition 3.5.9. *Let A, B be square matrices of size n, and let μ_n be the lowest common multiple of $\{1, 2, ..., n\}$. If A and B are simultaneously monomializable, then A^{μ_n} and B^{μ_n} commute.*

Proof. Suppose A, B are simultaneously monomializable, with μ_n defined as above. Then there exists a unitary matrix U such that $UAU^\dagger = D_A P_A$ and $UBU^\dagger = D_B P_B$ where D_A, D_B are diagonal matrices and P_A, P_B are permutation matrices. Note that $A = U^\dagger D_A P_A U$, so we have the following:

$$A^{\mu_n} = U^\dagger (D_A P_A)^{\mu_n} U = U^\dagger \widetilde{D}_A P_A^{\mu_n} U. \tag{3.32}$$

Here $\widetilde{D}_A$ is some diagonal matrix, and the last equality is obtained by repeated application of Lemma 3.5.4 and the fact that diagonal matrices are closed under composition. Since P_A is a permutation matrix of dimension n it has order k, where k is the lowest common multiple of the lengths of the permutation's cycles. Each cycle has length $\in \{1, 2, ..., n\}$. Thus k divides μ_n, and so $P_A^{\mu_n} = \mathbb{I}_n$. So $A^{\mu_n} = U^\dagger \widetilde{D}_A U$, and by the same argument, $B^{\mu_n} = U^\dagger \widetilde{D}_B U$ for some diagonal matrix $\widetilde{D}_B$. We then demonstrate that A^{μ_n} and B^{μ_n} commute:

$$A^{\mu_n} B^{\mu_n} = U^\dagger \widetilde{D}_A U U^\dagger \widetilde{D}_B U = U^\dagger \widetilde{D}_A \widetilde{D}_B U = U^\dagger \widetilde{D}_B \widetilde{D}_A U = U^\dagger \widetilde{D}_B U U^\dagger \widetilde{D}_A U = B^{\mu_n} A^{\mu_n}.$$

The central equality here holds because diagonal matrices commute. □

We are now ready to prove the necessary properties of our example basis.

Theorem 3.5.10. *The basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a monomial basis.*

Proof. For a contradiction, suppose that $\mathcal{M}$ is equivalent to a monomial basis. Note that $\mathcal{M}$ contains the identity matrix, so by Proposition 3.5.8 the elements of the UEB are simultaneously monomializable. The least common multiple of $\{1, 2, 3, 4\}$ is $\mu_4 = 12$; thus by Proposition 3.5.9 the 12th powers of the

elements of $\mathcal{M}$ will commute. To exhibit the contradiction, we compute the following commutator:

$$(\mathcal{M}_{01})^{12}(\mathcal{M}_{02})^{12} - (\mathcal{M}_{02})^{12}(\mathcal{M}_{01})^{12} = \frac{12168}{15625}\begin{pmatrix} -i & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & i \end{pmatrix} \neq 0. \tag{3.33}$$

This completes the proof. □

Proposition 3.5.11. *Shift-and-multiply bases are monomial bases.*

Proof. Recall from Definition 3.5.1 of a shift-and-multiply basis that each matrix is the product of a diagonal matrix with the permutation matrix given by a row of a classical Latin square. By definition, the result is a monomial matrix. □

Corollary 3.5.12. *The basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a shift-and-multiply basis.*

Proof. Immediate from Theorem 3.5.10 and Proposition 3.5.11.

3.6 Hadamard method

In this section we study the *Hadamard method*, a direct construction of a unitary error basis from a Hadamard matrix. While this is certainly known, we cannot find a clear description of it in full generality, although a special case is worked out in detail in [CD11]. The main results of this section are Theorem 3.6.2, where we show that the quantum shift-and-multiply method contains the Hadamard method as a special case, and Corollary 3.6.7, in which we show that this containment is proper.

Definition 3.6.1 (Hadamard method; folklore)**.** For a Hadamard matrix H of order n, its associated *Hadamard basis* $\{(U_H)_{ij}\}$ is defined as follows:

$$(U_H)_{ij} = \tfrac{1}{n} H \mathrm{diag}(H, j)^\dagger H^\dagger \mathrm{diag}(H^T, i). \tag{3.34}$$

Theorem 3.6.2. *A Hadamard basis is a quantum shift-and-multiply basis.*

Proof. By Definition 3.3.7 and Theorem 3.3.8 we have $(U_H)_{ij} = \Phi[H]_j \mathrm{diag}(H^T, i)$ where $\Psi[H]$ is the Hadamard QLS associated to H. Since the transpose of a Hadamard is also a Hadamard, the result follows. □

Corollary 3.6.3. *A Hadamard basis is a unitary error basis.*

Proof. Follows from Theorems 4.2.5 and 3.6.2.

Proposition 3.6.4. *If two Hadamard matrices are equivalent by Definition 3.3.5, then their associated unitary error bases are equivalent by Definition 3.4.2.*

Proof. We will once again prove equivalence on a case-by-case basis. Again suppose $G = PH$. Then we have the following:

$$(U_G)_{ij} \overset{(3.34)}{=} \frac{1}{n} PH\mathrm{diag}(PH, j)^\dagger H^\dagger P^{-1}\mathrm{diag}(H^T P^{-1}, i).$$

Again using the fact that P is real and unitary so, $P^{-1} = P^\dagger = P^T$. We continue:

$$\begin{aligned}
(U_G)_{ij} &\overset{(3.19)(3.20)}{=} \frac{1}{n} PH\mathrm{diag}(H, \sigma(j))^\dagger H^\dagger P^{-1}\mathrm{diag}(a_{\sigma(0),i}, ..., a_{\sigma(n-1),i}) \\
&\overset{(3.30)}{=} \frac{1}{n} PH\mathrm{diag}(H, \sigma(j))^\dagger H^\dagger \mathrm{diag}(a_{p^{-1}\sigma(0),i}, ..., a_{p^{-1}\sigma(n-1),i}) P^{-1} \\
&\overset{(3.15)}{=} \frac{1}{n} PH\mathrm{diag}(H, \sigma(j))^\dagger H^\dagger \mathrm{diag}(H^T, i) P^{-1} \\
&\overset{(3.24)}{\sim} \frac{1}{n} H\mathrm{diag}(H, \sigma(j))^\dagger H^\dagger \mathrm{diag}(H^T, i) \\
&\overset{(3.34)}{=} (U_H)_{i,\sigma(j)}.
\end{aligned}$$

The case that $G = HP$ is similar. Now suppose $G = DH$, with $D = \mathrm{diag}(c_1, \ldots, c_n)$, where $|c_i| = 1$. Then we calculate as follows:

$$\begin{aligned}
(U_G)_{ij} &\overset{(3.34)}{=} \frac{1}{n} DH\mathrm{diag}(DH, j)^\dagger H^\dagger D^\dagger \mathrm{diag}(H^T D^T, i) \\
&\overset{(3.21)}{=} \frac{1}{n} DHc_j\mathrm{diag}(H, j)^\dagger H^\dagger \mathrm{diag}(H^T D, i) D^\dagger \\
&\overset{(3.22)}{=} \frac{c_j}{n} DH\mathrm{diag}(H, j)^\dagger H^\dagger \mathrm{diag}(H^T, i) DD^\dagger \\
&\overset{(3.24)}{\sim} \frac{1}{n} H\mathrm{diag}(H, j)^\dagger H^\dagger \mathrm{diag}(H^T, i) \\
&\overset{(3.34)}{=} (U_H)_{ij}.
\end{aligned}$$

The case $G = HD$ is similar. □

Proposition 3.6.5 (See [Cra91], Theorem 1)**.** *All Hadamard matrices on $\mathbb{C}^4$ are equivalent to one of the following Fourier matrices, parameterised by $\alpha \in [0, \frac{\pi}{2}]$:*

$$H_\alpha := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{i\alpha} & -e^{i\alpha} \\ 1 & -1 & -e^{i\alpha} & e^{i\alpha} \end{pmatrix}. \tag{3.35}$$

Theorem 3.6.6. *Every unitary error basis for $\mathbb{C}^4$ arising from the Hadamard method is equivalent to a monomial basis.*

Proof. Write $\mathcal{F}_\alpha$ for the unitary error basis arising from H_α by the Hadamard method, for some fixed $\alpha \in [0, \frac{\pi}{2}]$. By Propositions 3.6.4 and 3.6.5 all unitary error bases arising from Hadamards in dimension 4 are equivalent to $\mathcal{F}_\alpha$, for some value of α. But the following unitary matrix simultaneously monomializes $\mathcal{F}_\alpha$, for all values of α:

$$Y := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}. \tag{3.36}$$

The basis $\mathcal{F}'_\alpha = \{YF_{ij}Y^\dagger | F_{ij} \in \mathcal{F}\}$ is listed in Section 3.8.2, and is monomial and equivalent to $\mathcal{F}_\alpha$. This completes the proof. □

Corollary 3.6.7. *The basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a Hadamard basis.*

Proof. Follows from Theorems 3.5.10 and 3.6.6. □

We are now ready to prove Proposition **??** which we restate below for ease of reference:

Proposition 3.3.11. *The quantum Latin square given in Example 3.1.2 is not equivalent to a quantum Latin square constructed from a Hadamard matrix.*

Proof. Let H_k be the family of Hadamard matrices as defined in equation (3.35) with associated QLSs $\Phi[H_k]$. We therefore have $\Phi[H_k]_j := \frac{1}{n} H_k \mathrm{diag}(H_k, j)^\dagger H_k^\dagger$. Let Ψ be the quantum Latin square of Example 3.1.2. By Lemma 3.3.10 and Proposition 3.6.5, any quantum Latin square arising from a Hadamard matrix in the manner of Definition 3.3.7 is equivalent to $\Phi[H_k]$ for some value of k.

For a contradiction, suppose that Ψ and $\Phi[H_k]$ are equivalent in the manner of Definition 3.3.3, for some fixed value of k. So there exists some unitary matrix U, diagonal unitary matrix D, permutation matrix P, permutation σ, and a family of unit complex numbers c_j, such that the following holds for all $j \in [n]$:

$$\Phi[H_k]_j = c_j U \Psi_{\sigma(j)} P D.$$

Note that the composite PD is unitary; so the families of matrices $\Phi[H_k]_j$ and Ψ_j, which are unitary by Lemma 3.3.2, are equivalent families in the sense of Definition 3.4.2.

The family $\Phi[H_k]_j$ are simultaneously monomializable, by the matrix Y defined in equation (3.36). (This follows from Theorem 3.6.6, in which we show that the members of $\mathcal{F}_k$, which include $\Phi[H_k]_j$ as a subset, are simultaneously monomializable.) So all together, the family of matrices Ψ_j contains the identity, and is equivalent in the sense of Definition 3.4.2 to a monomial family. So by Proposition 3.5.8, the family Ψ_j is simultaneously monomializable, and thus by Proposition 3.5.9, their 12th powers must all commute. But as established in the proof of Theorem 3.5.10, the 12th powers of $\Psi_1 = \mathcal{M}_{01}$ and $\Psi_2 = \mathcal{M}_{02}$ do not commute. This gives us our contradiction. □

3.7 Group-theoretic method

Another technique for constructing UEBs is the *group-theoretic method*, due to Knill [Kni96]. UEBs obtained using this technique are called *nice error bases*. The main result in this section is Corollary 3.7.5, that the basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a nice error basis. Throughout this section, we use '$\propto$' to denote equality up to multiplication by a unit complex number.

Recall that for a finite group G, an *n-dimensional unitary projective representation* is a function $\rho : G \to U(n)$, valued in the group of n-by-n unitary matrices, and for any $g, g' \in G$ a complex number $\omega_{g,g'} \in \mathbb{C}$ with unit norm, such that we have $\rho(gg') = \omega_{g,g'}\rho(g)\rho(g')$ and $\rho(1) = \mathbb{I}_n$ where 1 is the group identity. We therefore have the following:

$$\rho(g)\rho(g') \propto \rho(gg') \text{ for all } g, g' \in G. \tag{3.37}$$

The following basic result will also be useful.

Lemma 3.7.1. *Given a unitary projective representation ρ of a group G, the following holds:*

$$\rho(g)^\dagger \propto \rho(g^{-1}) \text{ for all } g \in G. \tag{3.38}$$

Proof. As follows: $\rho(g)^\dagger = \rho(g)^\dagger\rho(1) = \rho(g)^\dagger\rho(gg^{-1}) \overset{(3.37)}{\propto} \rho(g)^\dagger\rho(g)\rho(g^{-1}) = \rho(g^{-1})$. □

We now give the definition of a nice error basis, and show that a nice error basis is a unitary error basis.

Definition 3.7.2 (Nice error basis. See [Kni96], Section 2)**.** Let G be a finite group of order n^2, and let ρ be an n-dimensional unitary projective representation of G, such that for all $g \in G$ not equal to the identity, we have the following:

$$\mathrm{Tr}(\rho(g)) = 0. \tag{3.39}$$

Then a *nice error basis* $\mathcal{R}_{G,\rho} := \{\rho(g) \,|\, g \in G\}$ is the image of ρ.

Lemma 3.7.3 (See [KR03], Lemma 3)**.** *A nice error basis is a unitary error basis.*

We now prove a key proposition, which we will use to establish that our example basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a nice error basis.

Proposition 3.7.4. *Let $\mathcal{S}$ be a unitary error basis containing the identity matrix $\mathbb{I}_n$, such that $\mathcal{S}$ is equivalent to a nice error basis. Then up to multiplication by a unit complex number, $\mathcal{S}$ is closed under taking adjoints.*

Proof. Let $\mathcal{R}_{G,\rho}$ be a nice error basis, and let $\mathcal{S} = \{c_g U\rho(g)V \,|\, g \in G\}$ be an equivalent unitary error basis, with elements $\mathcal{S}_g := c_g U\rho(g)V$. Since by hypothesis $\mathbb{I}_n \in \mathcal{S}$, there is some $h \in G$ with $\mathcal{S}_h = c_h U\rho(h)V = \mathbb{I}_n$. In particular, writing '$\propto$' to indicate equality up to multiplication by a unit complex number, we have the following:

$$\mathbb{I}_n \propto U\rho(h)V, \tag{3.40}$$

$$\mathcal{S}_g \propto U\rho(g)V \text{ for all } g \in G. \tag{3.41}$$

We now perform the following calculation, for any $g \in G$:

$$\begin{aligned}(\mathcal{S}_g)^\dagger &\overset{(3.41)}{\propto} V^\dagger\rho(g)^\dagger U^\dagger = \mathbb{I}_n V^\dagger\rho(g)^\dagger U^\dagger \mathbb{I}_n \overset{(3.40)}{\propto} U\rho(h)VV^\dagger\rho(g)^\dagger U^\dagger U\rho(h)V \\ &= U\rho(h)\rho(g)^\dagger\rho(h)V \overset{(3.38)}{\propto} U\rho(h)\rho(g^{-1})\rho(h)V \overset{(3.37)}{\propto} U\rho(hg^{-1}h)V \overset{(3.41)}{\propto} \mathcal{S}_{hg^{-1}h}.\end{aligned}$$

So $\mathcal{S}$ is closed under adjoints, up to multiplication by a unit complex number. □

Corollary 3.7.5. *The basis $\mathcal{M}$ of Example 3.4.5 is not equivalent to a nice error basis.*

Proof. By inspection of the elements of $\mathcal{M}$, as listed in Section 3.8.1. For a contradiction, let us assume that $\mathcal{M}$ is equivalent to a nice error basis. Note that $\mathcal{M}$ contains the identity matrix; then by Proposition 3.7.4, it must be closed under taking adjoints, up to a unit complex number. But this is clearly false: for example, the second element of the first row of $\mathcal{M}_{01}$ has absolute value $\frac{1}{\sqrt{5}}$, but no member of $\mathcal{M}$ has an element with the same absolute value in the second element of the first column. □

3.8 Lists of unitary error bases

Here we list the unitary error bases that we make use of in the main text of this chapter.

3.8.1 The unitary error basis $\mathcal{M}$

Here we list the unitary error basis $\mathcal{M}$ defined in Example 3.4.5.

$$\mathcal{M}_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{M}_{01} = \begin{pmatrix} 0 & \frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{02} = \begin{pmatrix} 0 & \frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{03} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix} \quad \mathcal{M}_{11} = \begin{pmatrix} 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{12} = \begin{pmatrix} 0 & \frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{13} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -1 & 0 \\ 0 & i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{20} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \mathcal{M}_{21} = \begin{pmatrix} 0 & -\frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & -\frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{22} = \begin{pmatrix} 0 & -\frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{23} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{30} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \quad \mathcal{M}_{31} = \begin{pmatrix} 0 & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ 0 & -\frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{32} = \begin{pmatrix} 0 & -\frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{33} = \begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -1 & 0 \\ 0 & -i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

3.8.2 The unitary error basis $\mathcal{F}'$

Here we list the unitary error basis $\mathcal{F}'$ defined in the proof of Theorem 3.6.6.

$$\mathcal{F}'_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{01} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{02} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \mathcal{F}'_{03} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathcal{F}'_{10} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{12} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \mathcal{F}'_{13} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$$\mathcal{F}'_{20} = \begin{pmatrix} 0 & 0 & -e^{ia} & 0 \\ 0 & 0 & 0 & -1 \\ -e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{21} = \begin{pmatrix} 0 & 0 & e^{ia} & 0 \\ 0 & 0 & 0 & 1 \\ -e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{22} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ -e^{ia} & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{23} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ -e^{ia} & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{F}'_{30} = \begin{pmatrix} 0 & 0 & e^{ia} & 0 \\ 0 & 0 & 0 & -1 \\ e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{31} = \begin{pmatrix} 0 & 0 & -e^{ia} & 0 \\ 0 & 0 & 0 & 1 \\ e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{32} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ e^{ia} & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{33} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ e^{ia} & 0 & 0 & 0 \end{pmatrix}$$

Chapter 4

An application to mutually unbiased bases

In this chapter we introduce *left orthogonal quantum Latin squares*, which restrict to traditional orthogonal Latin squares, and investigate their application in quantum information science. We use quantum Latin squares to build maximally entangled bases, and show how mutually unbiased maximally entangled bases can be constructed in square dimension from left orthogonal quantum Latin squares. We also compare our construction to an existing construction due to Beth and Wocjan [BW04] and show that ours is strictly more general.

4.1 Introduction

In this chapter we introduce a notion of orthogonality between *quantum Latin squares* (QLSs) (see Chapter 3), mathematical objects which generalise *Latin squares*. We use this concept to give a new construction of *maximally entangled mutually unbiased bases* (MEMUBs), extending existing known techniques for Latin squares [BW04, WW10]. In addition we prove that our construction can produce bases that are unobtainable by existing methods [BW04, WW10]. We also introduce the concept of *mutually left orthogonal quantum Latin squares* (MLOQLS) which generalise *mutually orthogonal Latin squares* (MOLS), about which a significant body of research exists in connection with quantum information, and particularly pertaining to the connection between MOLS and MUBs [KR, PDB09, CC15]. Mutually unbiased bases are of fundamental importance to quantum information, as they capture the physical notion of complementary observables, quantities that cannot be simultaneously measured. Entanglement is one of the central phenomena of quantum theory that is at the foundation of quantum information and computation.

Everything that we present in this chapter is in the category **FHilb** of finite Hilbert spaces and linear

maps, but could be interpreted in any monoidal category such as **Rel** with *quantum-like* properties, which have been extensively researched as quantum toy theories.

Recall that a quantum Latin square of order n is an n-by-n array of elements of the Hilbert space $\mathbb{C}^n$, such that every row and every column is an orthonormal basis and a Latin square is a QLS with every element coming from a fixed computational basis.

We now give an example of a QLS that will prove useful later on.

Example 4.1.1. Here is an example of a quantum Latin square, Ψ given in terms of the computational basis states $|i\rangle$ for $i \in \{0, ..., 9\}$, and the following states:

$$|a\rangle := \frac{1}{\sqrt{3}}(i|3\rangle - |4\rangle + |5\rangle), \tag{4.1}$$

$$|b\rangle := \frac{1}{\sqrt{14}}(3|3\rangle - i|4\rangle + 2i|5\rangle), \tag{4.2}$$

$$|c\rangle := \frac{1}{\sqrt{42}}(|3\rangle - 5i|4\rangle - 4i|5\rangle), \tag{4.3}$$

$$|\alpha\rangle := \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \tag{4.4}$$

$$|\beta\rangle := \frac{1}{\sqrt{3}}(|0\rangle + e^{\frac{2\pi i}{3}}|1\rangle + e^{\frac{-2\pi i}{3}}|2\rangle), \tag{4.5}$$

$$|\gamma\rangle := \frac{1}{\sqrt{3}}(|0\rangle + e^{\frac{-2\pi i}{3}}|1\rangle + e^{\frac{2\pi i}{3}}|2\rangle). \tag{4.6}$$

$$\Psi := \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline |0\rangle & |2\rangle & |1\rangle & |3\rangle & |5\rangle & |4\rangle & |6\rangle & |8\rangle & |7\rangle \\ \hline |2\rangle & |1\rangle & |0\rangle & |5\rangle & |4\rangle & |3\rangle & |8\rangle & |7\rangle & |6\rangle \\ \hline |1\rangle & |0\rangle & |2\rangle & |4\rangle & |3\rangle & |5\rangle & |7\rangle & |6\rangle & |8\rangle \\ \hline |6\rangle & |8\rangle & |7\rangle & |0\rangle & |2\rangle & |1\rangle & |3\rangle & |5\rangle & |4\rangle \\ \hline |8\rangle & |7\rangle & |6\rangle & |2\rangle & |1\rangle & |0\rangle & |5\rangle & |4\rangle & |3\rangle \\ \hline |7\rangle & |6\rangle & |8\rangle & |1\rangle & |0\rangle & |2\rangle & |4\rangle & |3\rangle & |5\rangle \\ \hline |a\rangle & |c\rangle & |b\rangle & |6\rangle & |8\rangle & |7\rangle & |\alpha\rangle & |\gamma\rangle & |\beta\rangle \\ \hline |c\rangle & |b\rangle & |a\rangle & |8\rangle & |7\rangle & |6\rangle & |\gamma\rangle & |\beta\rangle & |\alpha\rangle \\ \hline |b\rangle & |a\rangle & |c\rangle & |7\rangle & |6\rangle & |8\rangle & |\beta\rangle & |\alpha\rangle & |\gamma\rangle \\ \hline \end{array}$$

It can be checked that every row and every column is an orthonormal basis. The quantum Latin square Ψ was constructed from a pair of 3×3 Latin squares and a pair of 3×3 unitary matrices as follows.

We define the Latin squares L and M as below:

$$L := \begin{array}{|c|c|c|} \hline |0\rangle & |1\rangle & |2\rangle \\ \hline |2\rangle & |0\rangle & |1\rangle \\ \hline |1\rangle & |2\rangle & |0\rangle \\ \hline \end{array} \qquad M := \begin{array}{|c|c|c|} \hline |0\rangle & |2\rangle & |1\rangle \\ \hline |2\rangle & |1\rangle & |0\rangle \\ \hline |1\rangle & |0\rangle & |2\rangle \\ \hline \end{array}. \tag{4.7}$$

Let V and W be defined as below:

$$V := \frac{1}{\sqrt{42}} \begin{pmatrix} \frac{i}{\sqrt{14}} & \frac{3}{\sqrt{3}} & 1 \\ \frac{-1}{\sqrt{14}} & \frac{-i}{\sqrt{3}} & -5i \\ \frac{1}{\sqrt{14}} & \frac{2i}{\sqrt{3}} & -4i \end{pmatrix} \qquad W := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{-2\pi i}{3}} \\ 1 & e^{\frac{-2\pi i}{3}} & e^{\frac{2\pi i}{3}} \end{pmatrix} \tag{4.8}$$

and let U_{ij} for $i, j \in [3]$ be the controlled family of unitary matrices such that $U_{20} = V$, $U_{22} = W$ and $U_{ij} = \mathbb{I}_3$ for all other values of i and j. The quantum Latin square Ψ is then given by the following where $|i\rangle := |p\rangle \otimes |n\rangle$ and $|j\rangle := |q\rangle \otimes |m\rangle$:

$$|\Psi_{ij}\rangle = |L_{pq}\rangle \otimes U_{pq} |M_{nm}\rangle. \tag{4.9}$$

The main result of this chapter is a construction of mutually unbiased maximally entangled bases from orthogonal QLSs. We now define the necessary concepts.

Definition 4.1.2 (Mutually unbiased bases)**.** Two orthonormal bases $|a_i\rangle$ and $|b_j\rangle$ for a Hilbert space $\mathcal{H}$ of dimension n are *mutually unbiased* when, for all $i, j \in \{0, ..., n-1\}$ [BBRV02]:

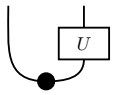
$$|\langle a_i | b_j \rangle|^2 = \frac{1}{n}. \tag{4.10}$$

Definition 4.1.3 (Maximally entangled state)**.** A *maximally entangled state* of a bipartite system is a state $|\psi\rangle$ of a product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim(\mathcal{H}_B) = n$, such that the partial trace over one of the systems of its density operator $\rho_{AB} = |\psi\rangle\langle\psi|$ is proportional to the identity. i.e:

$$\rho_A := \sum_{k=0} (\mathrm{id}_A \otimes \langle k|) \rho_{AB} (\mathrm{id}_A \otimes |k\rangle) = \frac{1}{n} \mathrm{id}_A. \tag{4.11}$$

Remark 3. *For the Hilbert space $\mathcal{H} \otimes \mathcal{H}$ with $dim(\mathcal{H}) = n$, all maximally entangled states are of the following form, where U is a unitary linear map and*  *is the classical structure (see Section 2.1) corresponding to the orthonormal basis $|k\rangle$:*

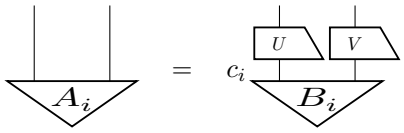
$$|U\rangle := \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle \otimes U|k\rangle \qquad \textit{or equivalently} \qquad |U\rangle := \frac{1}{\sqrt{n}} \tag{4.12}$$



Definition 4.1.4 (Maximally entangled basis)**.** A *maximally entangled basis* (MEB) for a bipartite system represented by a tensor product Hilbert space $\mathcal{H} \otimes \mathcal{H}$, is an orthonormal basis such that each basis state is maximally entangled.

Two MEBs $\mathcal{A} := |A_i\rangle$ and $\mathcal{B} := |B_i\rangle$ are equivalent when there exist unitaries U and V and complex

numbers of modulus 1, c_i such that:



(4.13)

In Section 4.2 we introduce our main result, the most general construction of mutually unbiased bases of the three presented in this chapter. We introduce left orthogonal quantum Latin squares and show how they can be used to construct MUBs, and we construct an explicit example. In Section 4.3 we start with traditional orthogonality of Latin squares and then show that the definition of orthogonality for QLSs in Section 4.2 generalises it. In Section 4.4 we present Beth and Wocjan's construction for MUBs in square dimension, and show that ours is strictly more general. In Section 4.5 we explain the correspondence between unitary error bases and maximally entangled bases and introduce mutually unbiased error bases. Finally in Section 4.6 we introduce mutually left orthogonal quantum Latin squares, which generalise mutually orthogonal Latin squares.

4.2 New construction for square dimension MUBs

In this section we introduce the main result of the chapter, a new construction for mutually unbiased maximally entangled bases. In order to formulate our construction we introduce *left orthogonal quantum Latin squares* which, as we will show in Section 4.3, reduce to traditional orthogonal Latin squares. As usual, given a QLS Φ we will denote the vector appearing in the i^{th} column of the j^{th} row as $|Q_{ij}\rangle$.

We now introduce a method for constructing MEBs given as input a family of Hadamard matrices and a quantum Latin square. This construction is in fact dual to the quantum shift-and-multiply method for constructing unitary error bases introduced in Chapter 3, as we will explain in Section 4.5.

Definition 4.2.1 (Quantum Latin square maximally entangled basis)**.** Given a quantum Latin square Φ and a family of Hadamard matrices H_j, a *quantum Latin square maximally entangled basis* $B(\Phi, H_j)$ is defined as follows:

$$\mathcal{A} := \left\{ |A_{ij}\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle \otimes |\Phi_{kj}\rangle\langle k|H_j|i\rangle \text{ such that } i,j \in \{0,..,n-1\} \right\}. \tag{4.14}$$

Lemma 4.2.2. *Quantum Latin square maximally entangled bases are maximally entangled bases.*

Proof. This MEB construction is the dual of the quantum shift-and-multiply basis construction, for a proof of the correctness of that construction see Chapter 3. □

Definition 4.2.3 (left orthogonal quantum Latin squares)**.** Given a pair of QLSs Ψ and Φ with vector entries $|\Psi_{ij}\rangle$ and $|\Phi_{ij}\rangle$ respectively, they are *left orthogonal* when for all $i,j \in \{0,..,n-1\}$, there exists

unique $t \in \{0, ..., n-1\}$ such that:

$$\sum_{k=0}^{n-1} |k\rangle\langle\Phi_{ki}|\Psi_{kj}\rangle = |t\rangle. \tag{4.15}$$

In words: if we take any column from Ψ and any column from Φ and compute the componentwise inner product of their vector entries, the resulting n numbers will always be $n-1$ zeros and a single 1. If the 1 appears in the t^{th} column then the output state of the linear map above will be $|t\rangle$.

Example 4.2.4. We present a pair of 9×9 left orthogonal quantum Latin squares, the first is the QLS from Example 4.1.1. Again let $|i\rangle$, $i \in \{0, ..., 9\}$ be the computational basis states and define the states $|a\rangle, |b\rangle, |c\rangle, |\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$ as in Equations (4.1) (4.2) (4.3) (4.4) (4.5) and (4.6). We define the following pair of QLSs:

$$\Psi := \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline |0\rangle & |2\rangle & |1\rangle & |3\rangle & |5\rangle & |4\rangle & |6\rangle & |8\rangle & |7\rangle \\ \hline |2\rangle & |1\rangle & |0\rangle & |5\rangle & |4\rangle & |3\rangle & |8\rangle & |7\rangle & |6\rangle \\ \hline |1\rangle & |0\rangle & |2\rangle & |4\rangle & |3\rangle & |5\rangle & |7\rangle & |6\rangle & |8\rangle \\ \hline |6\rangle & |8\rangle & |7\rangle & |0\rangle & |2\rangle & |1\rangle & |3\rangle & |5\rangle & |4\rangle \\ \hline |8\rangle & |7\rangle & |6\rangle & |2\rangle & |1\rangle & |0\rangle & |5\rangle & |4\rangle & |3\rangle \\ \hline |7\rangle & |6\rangle & |8\rangle & |1\rangle & |0\rangle & |2\rangle & |4\rangle & |3\rangle & |5\rangle \\ \hline |a\rangle & |c\rangle & |b\rangle & |6\rangle & |8\rangle & |7\rangle & |\alpha\rangle & |\gamma\rangle & |\beta\rangle \\ \hline |c\rangle & |b\rangle & |a\rangle & |8\rangle & |7\rangle & |6\rangle & |\gamma\rangle & |\beta\rangle & |\alpha\rangle \\ \hline |b\rangle & |a\rangle & |c\rangle & |7\rangle & |6\rangle & |8\rangle & |\beta\rangle & |\alpha\rangle & |\gamma\rangle \\ \hline \end{array} \qquad \Phi := \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline |0\rangle & |1\rangle & |2\rangle & |6\rangle & |7\rangle & |8\rangle & |3\rangle & |4\rangle & |5\rangle \\ \hline |1\rangle & |2\rangle & |0\rangle & |7\rangle & |8\rangle & |6\rangle & |4\rangle & |5\rangle & |3\rangle \\ \hline |2\rangle & |0\rangle & |1\rangle & |8\rangle & |6\rangle & |7\rangle & |5\rangle & |3\rangle & |4\rangle \\ \hline |3\rangle & |4\rangle & |5\rangle & |0\rangle & |1\rangle & |2\rangle & |6\rangle & |7\rangle & |8\rangle \\ \hline |4\rangle & |5\rangle & |3\rangle & |1\rangle & |2\rangle & |0\rangle & |7\rangle & |8\rangle & |6\rangle \\ \hline |5\rangle & |3\rangle & |4\rangle & |2\rangle & |0\rangle & |1\rangle & |8\rangle & |6\rangle & |7\rangle \\ \hline |6\rangle & |7\rangle & |8\rangle & |a\rangle & |b\rangle & |c\rangle & |\alpha\rangle & |\beta\rangle & |\gamma\rangle \\ \hline |7\rangle & |8\rangle & |6\rangle & |b\rangle & |c\rangle & |a\rangle & |\beta\rangle & |\gamma\rangle & |\alpha\rangle \\ \hline |8\rangle & |6\rangle & |7\rangle & |c\rangle & |a\rangle & |b\rangle & |\gamma\rangle & |\alpha\rangle & |\beta\rangle \\ \hline \end{array}. \tag{4.16}$$

It can be checked that if we take any column from Ψ and any column from Φ and compute the componentwise inner product of their vector entries, the resulting n numbers will always be $n-1$ zeros and a single 1.

Recall that Ψ is constructed from Latin squares L and M and controlled unitary U_{ij} as defined in Example 4.1.1. We now show how Φ was constructed similarly. Let V and W be unitary matrices as in equations (4.8), and let X_{ij} with $i, j \in [2]$ be a controlled unitary such that $X_{21} = V$, $X_{22} = W$ and $X_{ij} = \mathbb{I}_3$ for all other values of i and j. Also define the following Latin squares J and K:

$$J := \begin{array}{|c|c|c|}\hline |0\rangle & |1\rangle & |2\rangle \\ \hline |1\rangle & |2\rangle & |0\rangle \\ \hline |2\rangle & |0\rangle & |1\rangle \\ \hline \end{array} \qquad K := \begin{array}{|c|c|c|}\hline |0\rangle & |2\rangle & |1\rangle \\ \hline |1\rangle & |0\rangle & |2\rangle \\ \hline |2\rangle & |1\rangle & |0\rangle \\ \hline \end{array}. \tag{4.17}$$

Then Φ is constructed as follows where $|i\rangle := |p\rangle \otimes |n\rangle$ and $|j\rangle := |q\rangle \otimes |m\rangle$:

$$|\Phi_{ij}\rangle = |K_{pq}\rangle \otimes X_{pq}|J_{nm}\rangle.$$

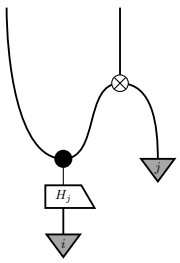
It can easily be checked that L and K form a left orthogonal pair (in the sense of Definition 4.2.3) as do M and J. Recalling that $|\Psi_{ij}\rangle = |L_{pq}\rangle \otimes U_{pq}|M_{nm}\rangle$ and given the careful choice of U_{ij} and X_{ij} (ensuring that the same unitary rotations are applied on the same columns of each QLS) we can see that the property of left orthogonality for Ψ and Φ is ensured by the left orthogonality of the constituent Latin squares. Since 2×2 Latin squares cannot be left orthogonal, 9×9 is the smallest possible size for a pair of left orthogonal quantum Latin squares constructed in this way. There may however be other constructions by which smaller pairs can be obtained.

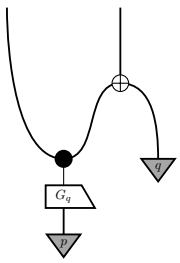
Theorem 4.2.5. *Given two indexed families of n Hadamard matrices H_k and G_j both of size n-by-n, and a pair of n-by-n left orthogonal quantum Latin squares Ψ and Φ, the bases $B(\Phi, H_k)$ and $B(\Psi, G_j)$ are mutually unbiased.*

Proof. Let $\Psi :=$ , $\Phi :=$  and  be the computational basis. By Definition 4.2.1 the $(i,j)^{th}$ state of the basis $\mathcal{A}$ and the $(p,q)^{th}$ state of the basis $\mathcal{B}$ are as follows:

$$|A_{ij}\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle \otimes |\Psi_{kj}\rangle\langle k|H_j|i\rangle,$$
$$|B_{pq}\rangle = \frac{1}{\sqrt{n}} \sum_{s=0}^{n-1} |s\rangle \otimes |\Phi_{sq}\rangle\langle s|G_q|p\rangle.$$

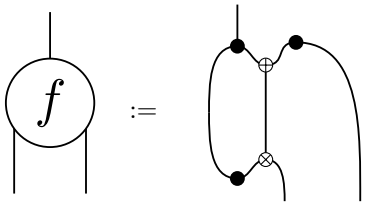
Graphically they are as follows:

$|A_{ij}\rangle :=$ 

$|B_{pq}\rangle :=$ 

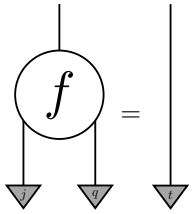
(4.18)

Ψ and Φ are left orthogonal so by Equation (4.27), f defined as follows is a function on computational basis states:



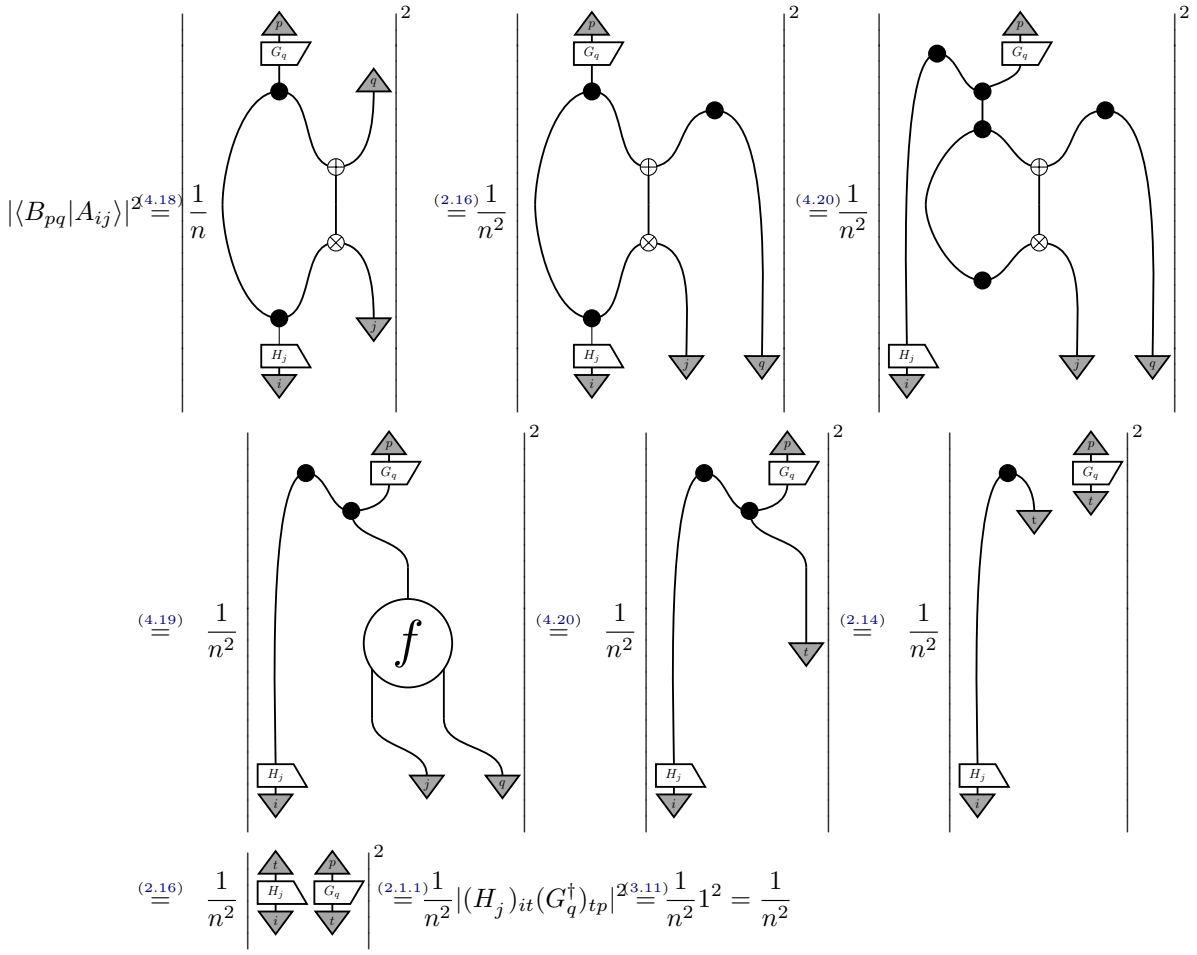
(4.19)

Since f is a function on basis states, $f(|j\rangle \otimes |q\rangle)$ is a computational basis state, say $|t\rangle$ i.e.



(4.20)

We are now ready to show that $\mathcal{A}$ and $\mathcal{B}$ are mutually unbiased.



□

Example 4.2.6. Given as input Ψ and Φ from Example 4.2.4 and the Hadamard matrix $H = H_0 = H_1 = ... = H_{n-1} = G_0 = ... = G_{n-1}$ defined below with $\omega := e^{2\pi i/3}$ we have constructed

a pair of maximally entangled mutually unbiased bases $\mathcal{A}$ and $\mathcal{B}$ for the Hilbert space $\mathbb{C}^9 \otimes \mathbb{C}^9$:

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{pmatrix}. \tag{4.21}$$

A sample of the 162 basis states of $\mathcal{A}$ and $\mathcal{B}$ with some calculations showing mutual unbiasedness (see Definition 6.1.1) can be found in Section 4.7. We have performed inner product calculations using Mathematica for all 6561 combinations of states from $\mathcal{A}$ and $\mathcal{B}$ and can confirm that they are mutually unbiased.

4.3 Left orthogonality and Latin square conjugates

In this section we explain how left orthogonality for QLSs restricts to orthogonality for Latin squares, and why this is a natural generalisation of Latin square orthogonality for QLSs. We start with the traditional definition of orthogonality.

Definition 4.3.1 (Orthogonal Latin squares)**.** Given a pair of Latin squares A and B of equal size, we take each computational basis state from A and form the ordered pair with the state from B corresponding to the same position in the grid. A and B are *orthogonal* when this procedure gives us all possible pairs of computational basis states [Man42].

This definition does not immediately lend itself to generalisation to QLSs since we may now have more than n^2 possible ordered pairs, but we can take an alternative approach. We characterise orthogonality in the following way:

Lemma 4.3.2. *Latin squares A and B are orthogonal if and only if the following linear map P is a permutation of basis states:*

$$P := \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} |i\rangle|j\rangle\langle A_{ij}|\langle k|B_{ij}\rangle\langle k|. \tag{4.22}$$

Proof. We now rearrange the equation defining the linear map P:

$$\begin{aligned}
P &:= \sum_i \sum_j \sum_k |i\rangle|j\rangle\langle A_{ij}|\langle k|B_{ij}\rangle\langle k| \\
&= \sum_i \sum_j \sum_k |i\rangle|j\rangle\langle A_{ij}|\langle B_{ij}|k\rangle\langle k| \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} |i\rangle|j\rangle\langle A_{ij}|\langle B_{ij}| \sum_k |k\rangle\langle k| \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} |i\rangle|j\rangle\langle A_{ij}|\langle B_{ij}|.
\end{aligned}$$

The second equality above holds because all $|B_{ij}\rangle$ and $|k\rangle$ are real valued vectors, and so $\langle k|B_{ij}\rangle = \overline{\langle k|B_{ij}\rangle} = \langle B_{ij}|k\rangle$. The third equality is just a rearranging of terms. The last equality holds by virtue of $\sum_k |k\rangle\langle k|$ being the resolution of the identity. The linear map P takes in the state $|p\rangle|q\rangle$ and outputs a superposition of all the states $|i\rangle|j\rangle$ such that $|A_{ij}\rangle = |p\rangle$ *and* $|B_{ij}\rangle = |q\rangle$, or outputs 0 if no such i, j exist. P is a permutation if and only if for all inputs p, q there exists unique i, j such that $|A_{ij}\rangle = |p\rangle$ *and* $|B_{ij}\rangle = |q\rangle$, i.e. A and B are orthogonal Latin squares. □

We now have a condition that we can apply to quantum Latin squares. However, for QLSs A and B this turns out to preclude superpositions, thus making A and B Latin squares.

Lemma 4.3.3. *Given a pair of quantum Latin squares, if they obey equation* (4.22)*, then they are Latin squares.*

Proof. Let A and B be QLSs such that the linear map P as defined above is a permutation of basis states. Then the adjoint of P, $P^\dagger = \sum_i \sum_j \sum_k |A_{ij}\rangle|k\rangle\langle i|\langle B_{ij}|k\rangle\langle j|$ must also be a permutation of basis states. We input computational basis states p and q into $P^\dagger$:

$$\begin{aligned}
P^\dagger(|p\rangle|q\rangle) &= \sum_k |A_{pq}\rangle|k\rangle\langle B_{pq}|k\rangle \\
&= \sum_k |A_{pq}\rangle|k\rangle\overline{\langle k|B_{pq}\rangle} \\
&= \sum_k |A_{pq}\rangle|k\rangle\langle k|\overline{B_{pq}\rangle} \\
&= |A_{pq}\rangle \left[\sum_k |k\rangle\langle k|\right] \overline{|B_{pq}\rangle} \\
&= |A_{pq}\rangle\overline{|B_{pq}\rangle}.
\end{aligned}$$

The second equality is due to the fact that the inner product is Hermitian, the third equality is due to $|k\rangle$ being real valued for all k, the fourth equality is an algebraic rearrangement and the final equality is

a resolution of the identity. If $P^\dagger$ above is a permutation of basis states, then for all $p, q \in [n]$, $|A_{pq}\rangle$ and $\overline{|B_{pq}\rangle}$ must be computational basis states. Thus A and B are Latin squares. □

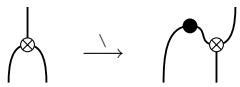
In order to define orthogonality for QLSs we will now make a (very) brief detour into quasigroup theory. Latin squares can be thought of as the multiplication (Cayley) table for finite order quasigroups [Smi06] on the computational basis states. Let $*$ be the binary operation given by a Latin square. The fact that each state appears exactly once in each row and each column means that knowledge of any two of a, b and c in the equation $a * b = c$ uniquely determines the third. This means we can canonically define the binary operation $\backslash$, read as *left divide*, such that $a * b = c \Rightarrow a \backslash c = b$. This new binary operation defines a new quasigroup and therefore a new Latin square called the *left conjugate Latin square* (it can easily be checked that this does indeed give a Latin square) [Smi06]. The map that takes a Latin square and gives the left conjugate $L \xrightarrow{\backslash} L'$, is in fact involutive so we can recover L from L' by applying the map again. We will see a nice graphical characterisation of this fact below. The map $L \xrightarrow{\backslash} L'$ is a bijection on the set of all Latin squares.

Definition 4.3.4 (Left orthogonality for Latin squares)**.** Given a pair of Latin squares they are *left orthogonal* when their left conjugates are orthogonal.

Remark 4. *We could equally well talk about the right conjugate given by right divide and define right orthogonality. In this thesis we only discuss left orthogonality.*

Since $L \xrightarrow{\backslash} L'$ is a bijection as mentioned above, the set of orthogonal Latin squares and left orthogonal Latin squares are isomorphic. Left orthogonality is in fact the property that we have generalised to QLSs in Definition 4.2.3.

To proceed further it will be useful to introduce some diagrams. Let  be a Latin square and  be the classical structure corresponding to the computational basis. Then the left divide map has the following form:



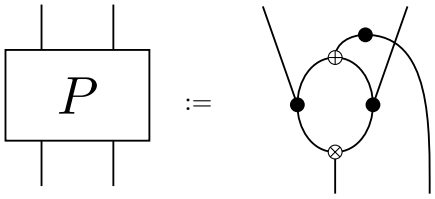
(4.23)

The fact that $\backslash$ is an involution can be verified using the snake equation:

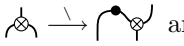


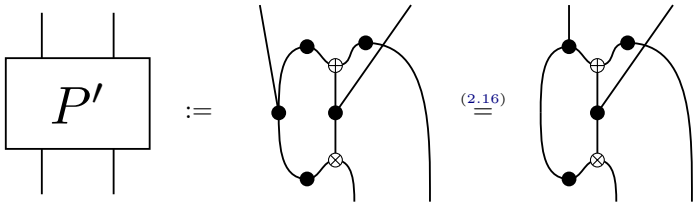
(4.24)

For Latin squares $A =$  and $B =$ , equation (4.22) can be expressed diagramatically as follows:



is a permutation. (4.25)

We now substitute in the left conjugates of Latin squares A and B,  and to obtain a linear map P' which must be a permutation of basis states for A and B to be left orthogonal. The condition that A and B are left orthogonal is thus equivalent to the following statement:



is a permutation. (4.26)

In words: first we input two states i and j and then compute the component-wise inner products of the i^{th} row of A and the j^{th} row of B. There must be one unique column, say s, such that $\langle B_{sj}|A_{si}\rangle = 1$ with $\langle B_{rj}|A_{ri}\rangle = 0$ for all r not equal to s. We then output s on the left and $|A_{si}\rangle$ on the right. The set of output states $s \otimes |A_{si}\rangle$ must be every possible combination of computational basis states.

We can interpret this for QLSs but again we encounter the same difficulty.

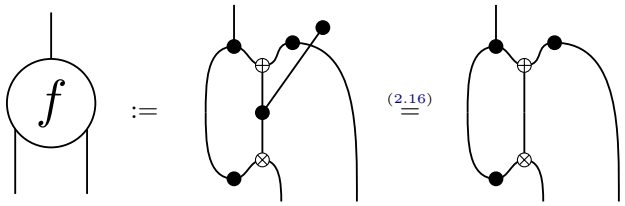
Lemma 4.3.5. *Every pair of left orthogonal QLSs are Latin squares.*

Proof. For a contradiction assume that A and B are left orthogonal QLSs that are not Latin squares. There is some vector entry in A that is not a computational basis state say $|A_{pq}\rangle$. For P' as defined in Equation (4.26) to be a permutation, $|A_{pq}\rangle$ cannot be the output on the right for any input q, j. This means that no row of B has the complex conjugate of $|A_{pq}\rangle$ as its p^{th} column entry. But each row of B must have one column entry that is the complex conjugate of the corresponding column entry of the q^{th} row of A. Thus at least two of the rows of B have the same vector in the same column. This violates the rule that B is a QLS and thus gives a contradiction. Therefore A must be a Latin square. Reversing the roles, we find that B must be a Latin square too (left orthogonality, like orthogonality is a symmetric relation). □

The condition must therefore be weakened if we want to define a property that non-Latin square QLSs can satisfy. One approach is to delete the output from the right hand wire and require that the linear map thus obtained be a function on the computational basis states. This is in fact the *left orthogonality* property of Definition 4.2.3. This condition turns out to be strong enough to give rise to interesting and

useful properties, enabling LOQLSs to be build mutually unbiased MEBs (see Theorem 4.2.5), yet weak enough so that pairs of Latin squares are left orthogonal if and only if they are orthogonal.

Graphically Definition 4.2.3 becomes the following:



is a function. (4.27)

Lemma 4.3.6. *Given a pair of Latin squares (which are of course quantum Latin squares), A and B the following are equivalent:*

- *A and B are left orthogonal Latin squares (see Definition 4.2.3).*
- *A and B are left orthogonal quantum Latin squares(see Definition 4.3.4).*

Proof. If A and B are left orthogonal then P', as defined in Equation (4.26), is a permutation of basis states, which clearly implies the weaker condition that f as defined in Equation (4.27) is a function. For the other implication let A and B be left orthogonal Latin squares. Consider the p^{th} columns of A and B. They both contain all n computational basis states and there must therefore exist values of i and j for all $q \in [n]$ such that $|A_{pi}\rangle = |B_{pj}\rangle = |q\rangle$. So for column p there exist i, j such that $P'(|i\rangle \otimes |j\rangle) = |p\rangle \otimes |q\rangle$ for all q. This is true for all rows q, so P' is a permutation. □

4.4 Beth and Wocjan's MUB construction

In their 2004 paper [BW04] Beth and Wocjan gave a construction for a pair of mutually unbiased bases of a Hilbert space $\mathcal{H}$ of square dimension $s = n^2$, given as input a pair of n-by-n orthogonal Latin squares and an n-by-n Hadamard matrix which was later put in explicit Latin square form by Wehner and Winter [BW04, WW10].

The construction takes each Latin square together with the Hadamard matrix and produces an MEB of dimension n^2. The fact that the Latin squares are orthogonal is then shown to entail that these two bases are mutually unbiased. I will refer to this MEB construction as the Left Beth-Wocjan maximally entangled basis (LBW MEB) construction*.

Definition 4.4.1 (Left Beth-Wocjan maximally entangled basis)**.** Given an n-by-n Latin square L and an n-by-n Hadamard matrix H, then $\mathcal{B}$ as defined below is a *Left Beth-Wocjan maximally entangled*

*The construction presented here is technically the construction given by taking the left conjugate of the Latin square L first and then applying the construction defined by Beth and Wocjan. Since taking the left conjugate gives us a bijection (see Equation (4.3)) on the set of Latin squares the MEBs obtainable are not affected by this.

basis (LBW MEB). [†]

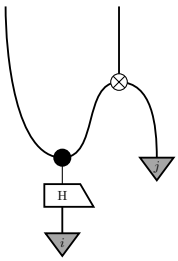
$$\mathcal{B} := \left\{ B_{ij} = \frac{1}{\sqrt{n}} \sum_{k,p=0}^{n-1} |k,p\rangle H_{ik} \langle L_{kp}|j\rangle \text{ such that } i,j \in \{0,..,n-1\} \right\}. \tag{4.28}$$

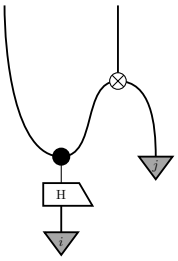
The graphical calculus gives a good notation with which to compare LBW MEBs to QLS MEBs (see Definition 4.2.1).

Lemma 4.4.2. *Under the restriction to Latin squares and to having a single fixed Hadamard matrix the QLS MEBs are the same as LBW MEBs.*

Proof. We construct an LBW MEB $\mathcal{B}$ and a QLS MEB $\mathcal{C}$ from the latin square $A =$  and Hadamard matrix H.

Left Beth-Wocjan MEB ***Quantum Latin square MEB***

$|B_{ij}\rangle := \frac{1}{\sqrt{n}}$ 

$|C_{ij}\rangle := \frac{1}{\sqrt{n}}$ 

We see that the diagrams are the same. □

Theorem 4.4.3. *Given a pair of n-by-n left*[‡] *orthogonal Latin squares and an n-by-n Hadamard matrix, construct two LBW MEBs using each Latin square with the Hadamard matrix. The bases are mutually unbiased.*

Lemma 4.4.4. *The construction of MUBs in Theorem 4.2.5 restricts to the construction of Theorem 4.4.3, under the restriction of the QLS to a Latin square and the two families of Hadamard matrices to a single fixed Hadamard matrix.*

Proof. Follows directly from Lemma 4.4.2. □

The following corollary gives a construction for MUBs in square dimension that is more general than the LBW MUB construction but not as general as our main construction.

[†] The definition below is slightly different to the one given by Beth and Wocjan even taking into account the use of the left conjugate Latin square. However, when the input is a Latin square the two constructions agree precisely.

[‡] In their paper Beth and Wocjan use orthogonal Latin squares, but since we defined their MEB construction on the left conjugate the *left* becomes necessary here.

Corollary 4.4.5. *Given two indexed families of n-by-n Hadamard matrices H_k and G_j both of size n, and a pair of n-by-n left orthogonal Latin squares Ψ and Φ, the bases $B(\Psi, H_k)$ and $B(\Phi, G_j)$ are mutually unbiased.*

So our new construction generalises Beth and Wocjan's in two directions, having two arbitrary families of Hadamard matrices rather than a single fixed Hadamard matrix and quantum Latin squares rather than Latin squares. The next theorem shows, by explicit example, that the generalisation is strict.

Theorem 4.4.6. *The pair of mutually unbiased MEBs from Example 4.2.6 are inequivalent to any MEBs obtainable by the LBW MEB construction.*

Proof. It will be sufficient to prove that one of our MEBs is inequivalent to any obtainable by the LBW MEB construction. Since equivalence of MEBs is the same as equivalence of UEBs we will take the dual approach here (see Section 4.5 below) and prove that the UEB arising from QLS Ψ and Hadamard matrix H in Example 4.2.6, which we will refer to as X, is inequivalent to any LBW UEB.

We will proceed along the same lines as Corollary 3.5.12. Note that LBW UEBs are a restriction to a single fixed Hadamard matrix of shift-and-multiply UEBs. Thus by Proposition 3.5.11, LBW UEBs are *monomial* (meaning each unitary matrix of the basis is the product of a diagonal matrix and a permutation matrix).

Suppose for a contradiction that X is equivalent to a monomial basis. The first matrix of X is as follows:

$$X_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

X_{00} is self adjoint. We obtain the equivalent UEB X' by composing all the matrices of X on the right by X_{00}. Thus $X'_{00} = \mathrm{id}_9$. Now X' contains the identity and is equivalent to a monomial basis so by Proposition 3.5.8 X' is *simultaneously monomializable.* (See Definition 3.5.7) . The least common multiple of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is $\mu_9 = 2520$; thus by Proposition 3.5.9 the 2520^{th} powers of the elements of X will commute. Now let $\omega = e^{2\pi i/3}$and consider X'_{06} and X'_{07} below:

$$X'_{06} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{\omega}{\sqrt{3}} & \frac{\omega^2}{\sqrt{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{\omega^2}{\sqrt{3}} & \frac{\omega}{\sqrt{3}} \\ \frac{i}{\sqrt{3}} & \frac{3}{\sqrt{14}} & \frac{1}{\sqrt{42}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-1}{\sqrt{3}} & \frac{-i}{\sqrt{14}} & \frac{-5i}{\sqrt{42}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{3}} & i\sqrt{\frac{2}{7}} & -2i\sqrt{\frac{2}{21}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad X'_{07} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{\omega^2}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{\omega}{\sqrt{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{\omega}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{\omega^2}{\sqrt{3}} \\ \frac{1}{\sqrt{42}} & \frac{i}{\sqrt{3}} & \frac{3}{\sqrt{14}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-5i}{\sqrt{42}} & \frac{-1}{\sqrt{3}} & \frac{-i}{\sqrt{14}} & 0 & 0 & 0 & 0 & 0 & 0 \\ -2i\sqrt{\frac{2}{21}} & \frac{1}{\sqrt{3}} & i\sqrt{\frac{2}{7}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

For a contradiction we now compute the first column sixth row entry of the commutator:

$$K := (X_{06})^{2520}(X_{07})^{2520} - (X_{07})^{2520}(X_{06})^{2520}$$
$$\langle 5|K|0\rangle \approx 0.5425 - 1.0829i \neq 0.$$

Thus X' and therefore X is not equivalent to any monomial basis, and in particular any LBW MEB. □

4.5 Mutually unbiased error bases

Unitary error bases (UEBs) are the mathematical data necessary for protocols such as dense coding and teleportation as well as having important applications to quantum error correction. In this section we explain how the results of this chapter can also be described in terms of UEBs via the correspondence between maximally entangled bases in square dimension and UEBs by introducing the natural concept of mutually unbiased UEBs.

Definition 4.5.1 (Unitary error basis)**.** A *unitary error basis* on an n-dimensional Hilbert space is a family of n^2 unitary matrices U_i, each of size n-by-n, such that [KR03]:

$$\mathrm{tr}(U_i^\dagger U_j) = \delta_{ij} n. \tag{4.29}$$

Via state-process duality a bijection exists between UEBs and MEBs (See Definition 4.1.4) [GS14]. The correspondence is particularly clear graphically.

Given a UEB, $\mathcal{A} := \{U_i | 0 < i \leq n^2\}$ and the computational basis , we have the corresponding

MEB, $\mathcal{B} := \{|U_i\rangle | 0 < i \leq n^2\}$ defined as follows (see [VW00] Lemma 2):

$$U_i := \quad \boxed{U_i} \quad \rightsquigarrow \quad \frac{1}{\sqrt{n}} \quad \boxed{U_i} \quad =: |U_i\rangle. \tag{4.30}$$

By Equation (4.12) the condition that the matrices U_i are unitary means that the states $|U_i\rangle$ are maximally entangled. Under this duality equivalence of MEBs as described by Equation 4.13, becomes the usual notion of equivalence for UEBs. The fact that the states on the right hand side of Equation (4.30) are orthonormal follows directly from Equation (4.29) as follows:

$$\langle U_i|U_j\rangle \overset{(4.30)}{=} \frac{1}{n} \quad \boxed{U_j^\dagger} \quad \boxed{U_i} \quad = \frac{1}{n}\mathrm{tr}(U_i^\dagger U_j) \overset{(4.29)}{=} \delta_{ij}. \tag{4.31}$$

In this chapter the dual MEB constructions of two of the main constructions for UEBs were used. As mentioned above Lemma 4.2.2 the QLS MEB of that lemma is the dual of the quantum shift-and-multiply error bases of Chapter 3. The MEB used in Corollary 4.4.5 is the shift-and-multiply basis introduced by Werner [Wer01]. Thus the LBW MEB construction described in Definition 4.4.3 gives us a family of UEBs strictly contained within Werners construction.

The duality of MEBs and UEBs makes it natural to talk about mutually unbiased unitary error bases.

Definition 4.5.2 (Mutually unbiased error bases)**.** A pair of unitary error bases over a Hilbert space $\mathcal{H}$ of dimension n, $\mathcal{A} = \{U_i | i \in \{0, ..., n-1\}\}$ and $\mathcal{B} = \{V_j | j \in \{0, ..., n-1\}\}$ are *mutually unbiased* when the following equation holds for all i, j:

$$|\mathrm{tr}(U_i^\dagger V_j)|^2 = \frac{1}{n}. \tag{4.32}$$

We had two choices in defining mutually unbiased UEBs above, we used the inner product of Equation (4.29) to interpret Equation (6.1.1) of Definition 6.1.1 directly but we could have defined mutually unbiased UEBs to be UEBs with corresponding MEBs that are mutually unbiased. Fortunately it does not matter as they are equivalent by a similar argument to Equation (4.31).

This definition brings up the question of what it may mean for two teleportation protocols to be mutually unbiased, or what kind of error correction could be performed by a pair of mutually unbiased error bases.

The main result of this chapter can now be interpreted as a construction for a pair of mutually unbiased unitary error bases from a pair of left orthogonal quantum Latin squares.

4.6 Mutually left orthogonal quantum Latin squares

In this section we introduce the concept of families of orthogonal quantum Latin squares. In their 2004 paper Beth and Wocjan [BW04] introduced the construction of square dimensional MUBs from orthogonal Latin squares as described in Section 4.4. They used this construction to improve the known lower bounds for maximal sets of pairwise mutually unbiased bases. A set of *mutually orthogonal Latin squares* (MOLs) is a set of two or more Latin squares that are pairwise orthogonal. Beth and Wocjan use their construction on a set of w MOLs of size n-by-n and give $w+2$ MUBs for dimension n^2. The extra two MUBs come from the two squares of vectors (which do not satisfy the axioms to be Latin squares, or even quantum Latin squares) described below: [§]

- The first is the n-by-n grid with the i^{th} row consisting of the repeated entry $|i\rangle$ for every column.
- The second is the n-by-n grid with $\sum_k^{n-1} |k\rangle$ as every diagonal entry and 0s elsewhere.

Some thought reveals that although they are not Latin squares, these two squares are left orthogonal to every n-by-n Latin square and to each other. Note that the bases obtained from these extra two however are not maximally entangled. The following definition is a natural extension of the concept of sets of MOLs.

Definition 4.6.1 (Mutually left orthogonal quantum Latin squares)**.** A set of w quantum Latin squares are *Mutually left orthogonal quantum Latin squares* (MLOQLs) when they are pairwise left orthogonal.

There are no generalisations of the two squares of vectors described above that would be left orthogonal to every QLS. However, with a particular set of MOQLs, an analogue of the first vector square above can be found by considering the subspaces spanned by the non-computational basis states. As an example we present a square of vectors that is left orthogonal to both of the pair of left orthogonal QLSs from Example 4.2.4. Again let $|i\rangle$, $i \in \{0, ..., 9\}$ be the computational basis states and define the states $|a\rangle, |b\rangle, |c\rangle, |\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$ as in Equations (4.1) (4.2) (4.3) (4.4) (4.5) and (4.6). We define the

[§]Note that due to the presentation of Beth and Wocjan's construction in Section 4.4, in which we start by taking the left-conjugate, the left conjugate map must also be applied to these squares of vectors to recover the ones used by Beth and Wocjan. In addition the second square here only gives a basis using the original Beth-Wocjan method and not the altered version given by definition 4.4.1 (See footnote †).

following square of vectors:

$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|\alpha\rangle$	$\|\alpha\rangle$	$\|\alpha\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|\beta\rangle$	$\|\beta\rangle$	$\|\beta\rangle$
$\|2\rangle$	$\|2\rangle$	$\|2\rangle$	$\|2\rangle$	$\|2\rangle$	$\|2\rangle$	$\|\gamma\rangle$	$\|\gamma\rangle$	$\|\gamma\rangle$
$\|a\rangle$	$\|a\rangle$	$\|a\rangle$	$\|3\rangle$	$\|3\rangle$	$\|3\rangle$	$\|3\rangle$	$\|3\rangle$	$\|3\rangle$
$\|b\rangle$	$\|b\rangle$	$\|b\rangle$	$\|4\rangle$	$\|4\rangle$	$\|4\rangle$	$\|4\rangle$	$\|4\rangle$	$\|4\rangle$
$\|c\rangle$	$\|c\rangle$	$\|c\rangle$	$\|5\rangle$	$\|5\rangle$	$\|5\rangle$	$\|5\rangle$	$\|5\rangle$	$\|5\rangle$
$\|6\rangle$	$\|6\rangle$	$\|6\rangle$	$\|6\rangle$	$\|6\rangle$	$\|6\rangle$	$\|6\rangle$	$\|6\rangle$	$\|6\rangle$
$\|7\rangle$	$\|7\rangle$	$\|7\rangle$	$\|7\rangle$	$\|7\rangle$	$\|7\rangle$	$\|7\rangle$	$\|7\rangle$	$\|7\rangle$
$\|8\rangle$	$\|8\rangle$	$\|8\rangle$	$\|8\rangle$	$\|8\rangle$	$\|8\rangle$	$\|8\rangle$	$\|8\rangle$	$\|8\rangle$

.

It can be checked that this square is left orthogonal to Ψ and Φ in Example 4.2.4. It is also left orthogonal to any QLS left orthogonal to Ψ or Φ. To see this consider that any two left orthogonal QLSs must have columns that are permutations of each other.

This example relies on the *block-like* structure of the QLSs in question. Any family of MLOQLS having a similar structure will admit a similar square of vectors. It is unknown whether all QLSs are of this form, but to the authors knowledge none have been found yet that do not have this structure up to equivalence.

The lower bound for the number of MLOQLS in dimension n must be at least the lower bound for the number of MOLS, more research is required to say any more than that at this stage.

In Chapter 3 we introduced the quantum combinatorial objects of quantum Latin squares and gave a construction of UEBs using them. In this chapter we have built upon that work by introducing mutually orthogonal quantum Latin squares which generalise mutually orthogonal Latin squares, which have been used extensively to derive results in quantum information. As an application we have given a construction for mutually unbiased bases in square dimension which gives MUBs that are inequivalent to those that can be constructed by any known method. There is the potential for improved bounds on maximal families of MUBs in composite dimensions using the main result of this chapter.

4.7 Quantum Latin square 9×9 example MUB

We now give a sample of the 81 states of basis $\mathcal{A}$ and the 81 states of basis $\mathcal{B}$ from Example 4.2.6, with some calculations of their inner products showing mutual unbiasedness. We give everything in terms of the computational basis states $|i, j\rangle$ such that $i, j \in [n]$. And we define the scalar $\omega := e^{2\pi i/3}$. Here are

some states from $\mathcal{A}$ and $\mathcal{B}$:

$$\begin{aligned}
\mathcal{A}_{74} &= \frac{1}{3}|0,5\rangle + \omega|1,4\rangle + \omega^2|2,3\rangle + \omega^2|3,2\rangle + \omega^2|4,1\rangle + \omega|5,0\rangle + \omega|6,8\rangle + \omega^2|7,7\rangle + |8,6\rangle),\\
\mathcal{A}_{46} &= \frac{1}{3}(|0,6\rangle + \omega|1,8\rangle + \omega^2|2,7\rangle + \omega|3,3\rangle + \omega|4,5\rangle + |5,4\rangle + \frac{\omega^2}{\sqrt{3}}|6,0\rangle + \frac{\omega^2}{\sqrt{3}}|6,1\rangle + \frac{\omega^2}{\sqrt{3}}|6,2\rangle\\
&\quad + \frac{1}{\sqrt{3}}|7,0\rangle + \frac{\omega^2}{\sqrt{3}}|7,1\rangle + \frac{\omega}{\sqrt{3}}|7,2\rangle + \frac{\omega}{\sqrt{3}}|8,0\rangle + \frac{1}{\sqrt{3}}|8,1\rangle + \frac{\omega^2}{\sqrt{3}}|8,2\rangle),\\
\mathcal{B}_{38} &= \frac{1}{3}(|0,5\rangle + |1,3\rangle + |2,4\rangle + \omega|3,8\rangle + \omega|4,6\rangle + \omega|5,8\rangle + \frac{\omega^2}{\sqrt{3}}|6,0\rangle + \frac{\omega}{\sqrt{3}}|6,1\rangle + \frac{1}{\sqrt{3}}|6,2\rangle\\
&\quad + \frac{\omega^2}{\sqrt{3}}|7,0\rangle + \frac{\omega^2}{\sqrt{3}}|7,1\rangle + \frac{\omega^2}{\sqrt{3}}|7,2\rangle + \frac{\omega^2}{\sqrt{3}}|8,0\rangle + \frac{1}{\sqrt{3}}|8,1\rangle + \frac{\omega}{\sqrt{3}}|8,2\rangle),\\
\mathcal{B}_{03} &= \frac{1}{3}(|0,6\rangle + |1,7\rangle + |2,8\rangle + |3,0\rangle + |4,1\rangle + |5,2\rangle + \frac{i}{\sqrt{3}}|6,3\rangle + \frac{-1}{\sqrt{3}}|6,4\rangle\\
&\quad + \frac{1}{\sqrt{3}}|6,5\rangle + \frac{3}{\sqrt{14}}|7,3\rangle + \frac{-i}{\sqrt{14}}|7,4\rangle + \frac{2i}{\sqrt{14}}|7,5\rangle + \frac{1}{\sqrt{42}}|8,3\rangle + \frac{-5i}{\sqrt{42}}|8,4\rangle + \frac{-4i}{\sqrt{42}}|8,5\rangle).
\end{aligned}$$

Here are some calculations for mutual unbiasedness. Note that they all equal $\frac{1}{81}$ as required:

$$\begin{aligned}
|\langle\mathcal{A}_{74}|B_{38}\rangle|^2 &= |\frac{1}{9}|^2 = \frac{1}{81},\\
|\langle\mathcal{A}_{74}|\mathcal{B}_{03}\rangle|^2 &= |\frac{1}{9}\omega^2|^2 = \frac{1}{81},\\
|\langle\mathcal{A}_{46}|\mathcal{B}_{38}\rangle|^2 &= |\frac{1}{9}\left[\frac{1}{3}(\omega^2+\omega+1) + \frac{1}{3}(\omega^2+\omega+1) + \frac{1}{3}(1+1+1)\right]|^2 = \frac{1}{81},\\
|\langle\mathcal{A}_{46}|\mathcal{B}_{03}\rangle|^2 &= |\frac{1}{9}|^2 = \frac{1}{81}.
\end{aligned}$$

Chapter 5

Orthogonality and generalizations

In the previous chapter we gave a notion of orthogonality for QLSs which was useful to enable us to construct MUBs. This we refer to as left orthogonality for QLSs. In 2018 Goyeneche et al proposed an alternative notion of orthogonality for quantum Latin squares, and showed that orthogonal quantum Latin squares yield quantum codes [GRDMŻ18]. In this chapter we give a simplified characterization of orthogonality for quantum Latin squares, which we show is equivalent to that of Goyeneche et al. We refer to this simply as orthogonality for QLSs. We use this simplified characterization to give an upper bound for the number of mutually orthogonal quantum Latin squares of a given size, and to give the first examples of orthogonal quantum Latin squares that do not arise from ordinary Latin squares.

We then discuss quantum Latin isometry squares, generalizations of quantum Latin squares recently introduced by Benoist and Nechita, and define a new orthogonality property for these objects, showing that it also allows the construction of quantum codes. We give a new characterization of unitary error bases using these structures.

5.1 Introduction

5.1.1 Summary

The results of Chapter 3 were originally published in 2016. Since then the work has been built on separately by a number of researchers: in particular, by Goyeneche, Raissi, Di Martino and Życzkowski [GRDMŻ18], who propose a notion of *orthogonality* for quantum Latin squares which allows the construction of quantum codes; and also by Benoist and Nechita [BN17], who introduce *matrices of partial isometries of type (C1,C2,C3,C4)*, generalizations of quantum Latin squares which characterize system-environment observables preserving a certain set of pointer states.

In this chapter we give a new formulation of orthogonality for quantum Latin squares, and use it to relate and generalize the works just cited, and extend them in certain ways. In particular, we highlight

the following key contributions.

- We give a new, simplified definition of orthogonality for quantum Latin squares, and show that it is equivalent to the existing definition of Goyeneche et al [GRDMŻ18, Definition 3]. (Definition 5.2.1, Theorem 5.2.8.)
- We give the first example of a pair of orthogonal quantum Latin squares which are not equivalent to a pair of classical Latin squares. (Example 5.2.2 and Proposition 5.2.11.)
- We show that there can be at most $n-1$ mutually orthogonal quantum Latin squares of dimension n (Theorem 5.2.16.)
- We introduce *quantum Latin isometry squares* based on the *matrices of partial isometries of type (C1,C2,C3,C4)* defined by Benoist and Nechita [BN17, Definition 3.2], and define a new notion of orthogonality for these objects. (Definitions 5.4.1 and 5.4.9.)
- We show how orthogonal quantum Latin isometry squares can be used to build quantum codes. (Theorem 5.4.14.)
- We show that unitary error bases give rise to orthogonal pairs of quantum Latin isometry squares, and in fact can be characterized in terms of them. (Theorem 5.4.18.)

5.1.2 The two other notions of orthogonal quantum Latin squares

Left orthogonality, introduced in the previous chapter is not comparable to the notion of orthogonality discussed in this chapter.

More recently, Goyeneche et al [GRDMŻ18] introduced another notion of orthogonality for quantum Latin squares, which also extends the traditional definition for classical Latin squares, and the definition which we study here is equivalent. They extended their notion to quantum orthogonal arrays, more general objects which we do not consider here.

Remark 5. *Note that the definition of orthogonal quantum Latin squares introduced by Goyeneche et al includes not only pairs of quantum Latin squares satisfying an orthogonality condition but also entangled bipartite states known as 'essentially quantum' pairs. This more general definition is exactly equivalent to that of perfect tensors which are already well studied. We only consider orthogonality between two or more quantum Latin squares in this chapter, and only use the terms orthogonal quantum Latin squares and mutually orthogonal quantum Latin squares to refer to such objects.*

5.1.3 Outline

This chapter has the following structure. In Section 5.2, we give background on quantum Latin squares, introduce our new definition of orthogonality, and explore its consequences, especially in relation to

the work of Goyeneche et al [GRDMŻ18]. In Section 5.3 we explore the connection of orthogonality to biunitaries and perfect tensors. This gives an elegant graphical interpretation of orthogonal QLSs. In Section 5.4, we define quantum Latin isometry squares based on the work of Benoist and Nechita [BN17], and investigate a new notion of orthogonality for these objects as well as a connection to unitary error bases.

5.2 Quantum Latin squares and orthogonality

In this section we prove our main results concerning orthogonal quantum Latin squares. In Section 5.2.1 we recall the definition of quantum Latin squares, give our new definition of orthogonality, and give a nontrivial example. In Section 5.2.2 we show that our notion of orthogonality is equivalent to a previous, more complicated definition due to Goyeneche et al [GRDMŻ18]. In Section 5.2.3 we explore the connection between equivalence and orthogonality of quantum Latin squares, and show that our example of orthogonal quantum Latin squares is not equivalent to a pair of orthogonal classical Latin squares. In Section 5.2.4, we give a simpler definition of orthogonality for families of quantum Latin squares, and show it agrees with that due to Goyeneche et al. In Section 5.2.5, we prove an upper bound on the number of mutually orthogonal quantum Latin squares that can exist in any dimension.

5.2.1 First definitions

We begin with the definition of a quantum Latin square, recently proposed by the present authors [MV15].

Recall that a *quantum Latin square (QLS)* Ψ of dimension n is an n-by-n array of elements $|\Psi_{ij}\rangle \in \mathbb{C}^n$, such that every row and every column gives an orthonormal basis for $\mathbb{C}^n$ and that by convention we write $|\Psi_{ij}\rangle$, the indices i and j refer to the row and columns of the array respectively, and take values in the set $[n] = \{0, 1, \ldots, n-1\}$.

We now introduce our new notion of orthogonality for QLSs.

Definition 5.2.1. Two quantum Latin squares Φ, Ψ of dimension n are *orthogonal* just when the set of vectors $\{|\Phi_{ij}\rangle \otimes |\Psi_{ij}\rangle | i, j \in [n]\}$ form an orthonormal basis of the space $\mathbb{C}^n \otimes \mathbb{C}^n$.

We show in Theorem 5.2.8 that this agrees with a more complicated definition recently proposed by Goyeneche et al [GRDMŻ18], in terms of partial traces of a tensor expression.

In that paper, it was shown that for classical Latin squares, this agrees with the classical notion of orthogonality. However, no non-classical examples were given of pairs of quantum Latin squares that are orthogonal . We now rectify this.

Example 5.2.2 (Non-classical orthogonal quantum Latin squares)**.** Define the unitary matrix U as follows:

$$U := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{-2\pi i}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & e^{\frac{-2\pi i}{3}} & e^{\frac{2\pi i}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1+i & (1-i)/\sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i/\sqrt{2} & 1 & 1/\sqrt{2}+i & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/\sqrt{2} & i & 1-i/\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{3/2} & \sqrt{3/2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{3/2} & -\sqrt{3/2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{3} \end{pmatrix}.$$

Then the following arrays are a pair of orthogonal quantum Latin squares of dimension 9:

$\|0\rangle$	$\|2\rangle$	$\|1\rangle$	$\|3\rangle$	$\|5\rangle$	$\|4\rangle$	$\|6\rangle$	$\|8\rangle$	$\|7\rangle$
$\|2\rangle$	$\|1\rangle$	$\|0\rangle$	$\|5\rangle$	$\|4\rangle$	$\|3\rangle$	$\|8\rangle$	$\|7\rangle$	$\|6\rangle$
$\|1\rangle$	$\|0\rangle$	$\|2\rangle$	$\|4\rangle$	$\|3\rangle$	$\|5\rangle$	$\|7\rangle$	$\|6\rangle$	$\|8\rangle$
$\|6\rangle$	$\|8\rangle$	$\|7\rangle$	$\|0\rangle$	$\|2\rangle$	$\|1\rangle$	$\|3\rangle$	$\|5\rangle$	$\|4\rangle$
$\|8\rangle$	$\|7\rangle$	$\|6\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$	$\|5\rangle$	$\|4\rangle$	$\|3\rangle$
$\|7\rangle$	$\|6\rangle$	$\|8\rangle$	$\|1\rangle$	$\|0\rangle$	$\|2\rangle$	$\|4\rangle$	$\|3\rangle$	$\|5\rangle$
$U\|3\rangle$	$U\|5\rangle$	$U\|4\rangle$	$\|6\rangle$	$\|8\rangle$	$\|7\rangle$	$U\|0\rangle$	$U\|2\rangle$	$U\|1\rangle$
$U\|5\rangle$	$U\|4\rangle$	$U\|3\rangle$	$\|8\rangle$	$\|7\rangle$	$\|6\rangle$	$U\|2\rangle$	$U\|1\rangle$	$U\|0\rangle$
$U\|4\rangle$	$U\|3\rangle$	$U\|5\rangle$	$\|7\rangle$	$\|6\rangle$	$\|8\rangle$	$U\|1\rangle$	$U\|0\rangle$	$U\|2\rangle$

$\|0\rangle$	$\|2\rangle$	$\|1\rangle$	$\|3\rangle$	$\|5\rangle$	$\|4\rangle$	$\|6\rangle$	$\|8\rangle$	$\|7\rangle$
$\|1\rangle$	$\|0\rangle$	$\|2\rangle$	$\|4\rangle$	$\|3\rangle$	$\|5\rangle$	$\|7\rangle$	$\|6\rangle$	$\|8\rangle$
$\|2\rangle$	$\|1\rangle$	$\|0\rangle$	$\|5\rangle$	$\|4\rangle$	$\|3\rangle$	$\|8\rangle$	$\|7\rangle$	$\|6\rangle$
$\|3\rangle$	$\|5\rangle$	$\|4\rangle$	$\|6\rangle$	$\|8\rangle$	$\|7\rangle$	$U\|0\rangle$	$U\|2\rangle$	$U\|1\rangle$
$\|4\rangle$	$\|3\rangle$	$\|5\rangle$	$\|7\rangle$	$\|6\rangle$	$\|8\rangle$	$U\|1\rangle$	$U\|0\rangle$	$U\|2\rangle$
$\|5\rangle$	$\|4\rangle$	$\|3\rangle$	$\|8\rangle$	$\|7\rangle$	$\|6\rangle$	$U\|2\rangle$	$U\|1\rangle$	$U\|0\rangle$
$U\|6\rangle$	$U\|8\rangle$	$U\|7\rangle$	$\|0\rangle$	$\|2\rangle$	$\|1\rangle$	$\|3\rangle$	$\|5\rangle$	$\|4\rangle$
$U\|7\rangle$	$U\|6\rangle$	$U\|8\rangle$	$\|1\rangle$	$\|0\rangle$	$\|2\rangle$	$\|4\rangle$	$\|3\rangle$	$\|5\rangle$
$U\|8\rangle$	$U\|7\rangle$	$U\|6\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$	$\|5\rangle$	$\|4\rangle$	$\|3\rangle$

(5.1)

We now consider some equivalent characterizations of Definition 5.2.1, which will be useful later.

Lemma 5.2.3. *Two quantum Latin squares Φ, Ψ are orthogonal if and only if one, and hence both, of the following equivalent conditions hold:*

$$\sum_{i,j=0}^{n-1} |\Phi_{ij}\rangle\langle\Phi_{ij}| \otimes |\Psi_{ij}\rangle\langle\Psi_{ij}| = \mathbb{I}_n \otimes \mathbb{I}_n, \tag{5.2}$$

$$\sum_{i,j,p,q=0}^{n-1} \langle\Phi_{ij}|\Phi_{pq}\rangle\langle\Psi_{ij}|\Psi_{pq}\rangle |ij\rangle\langle pq| = \mathbb{I}_n \otimes \mathbb{I}_n. \tag{5.3}$$

Proof. For the first condition, equation (5.2) says that if we sum up outer products of each element of the family $\{|\Phi_{ij}\rangle \otimes |\Psi_{ij}\rangle | i, j \in [n]\}$, we get the identity; clearly this is equivalent to the statement that the family yields an orthonormal basis. For the second condition, consider the linear map

$S = \sum_{i,j} |ij\rangle\langle\Phi_{ij}|\langle\Psi_{ij}|$, an operator on $\mathbb{C}^n \otimes \mathbb{C}^n$. The quantum Latin squares Φ, Ψ are orthogonal if and only if this map is unitary, since it transports the orthonormal basis $\{|\Phi_{ij}\rangle \otimes |\Psi_{ij}\rangle | i, j \in [n]\}$ to the computational basis. Since it is an operator on a finite-dimensional Hilbert space, S is unitary if and only if it is an isometry, and equation (5.3) is the isometry condition. □

Orthogonality of quantum Latin squares is unaffected by conjugation of one of the squares.

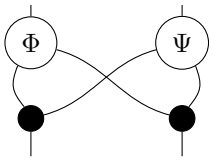
Definition 5.2.4. Given a quantum Latin square Ψ, its *conjugate* Ψ^* is the quantum Latin square with entries $(\Psi^*)_{ij} = (\Psi_{ij})^*$.

Lemma 5.2.5. *Two quantum Latin squares Φ, Ψ are orthogonal just when Φ^*, Ψ are orthogonal.*

Proof. Suppose Φ, Ψ are orthogonal quantum Latin squares. Then by equation (5.3), it follows that $\sum_{i,j,p,q=0}^{n-1} \langle\Phi_{ij}|\Phi_{pq}\rangle\langle\Psi_{ij}|\Psi_{pq}\rangle = \delta_{ip}\delta_{jq}$. So for all $(i,j) \neq (p,q)$ either $\langle\Phi_{ij}|\Phi_{pq}\rangle = 0$ or $\langle\Psi_{ij}|\Psi_{pq}\rangle = 0$, and we know that $\langle\Phi_{ij}|\Phi_{ij}\rangle = \langle\Psi_{ij}|\Psi_{ij}\rangle = 1$. Since $0, 1 \in \mathbb{R}$, we conclude that $\sum_{i,j,p,q=0}^{n-1} \langle\Phi^*_{ij}|\Phi^*_{pq}\rangle\langle\Psi_{ij}|\Psi_{pq}\rangle = \delta_{ip}\delta_{jq}$, and hence by equation (5.2) it follows that Φ^*, Ψ are orthogonal. The converse then follows since $(\Phi^*)^* = \Phi$. □

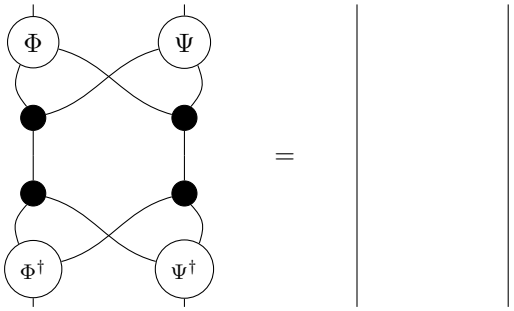
We have the following diagrammatic characterization of orthogonal quantum Latin squares.

Lemma 5.2.6. *A pair of QLSs Ψ and Φ are orthogonal if and only if the following linear map is unitary:*

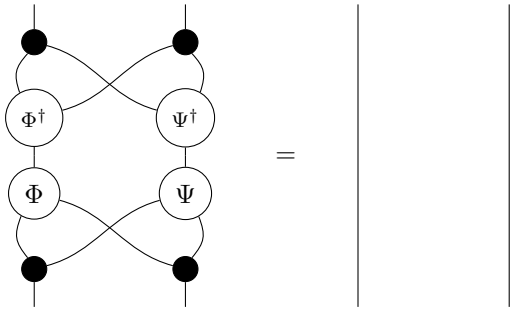


(5.4)

Proof. This follows directly from Lemma 5.2.3. Equation (5.2) translates into the graphical calculus as follows:



Equation (5.3) is equivalent to the following graphical equation:



□

5.2.2 Relationship to previous notion of orthogonality

The following equivalent definition of orthogonality for quantum Latin squares has recently been proposed.

Definition 5.2.7 ([GRDMŻ18], Definition 3)**.** Two quantum Latin squares Φ, Ψ are *GRMZ-orthogonal* when for each tensor factor $X \in \{A, B, C\}$, the following holds:

$$\mathrm{Tr}_X \left(\sum_{i,p,j=0}^{n-1} |\Phi_{ij}\rangle\langle\Phi_{ij}|_A \otimes |\Psi_{pj}\rangle\langle\Psi_{pj}|_B \otimes |i\rangle\langle p|_C \right) = \mathbb{I}_{n^2}. \tag{5.5}$$

Note that in the presentation of this definition we have restricted the original definition to orthogonality between pairs of quantum Latin squares (please refer to Remark 5). We now show that Definition 5.2.7 is equivalent to our Definition 5.2.1.

Theorem 5.2.8. *Two quantum Latin squares Φ, Ψ are orthogonal if and only if they are GRMZ-orthogonal.*

Proof. We first consider equation (5.5) for the case $X = C$, which yields the following equation:

$$\sum_{i,j,p=0}^{n-1} |\Phi_{ij}\rangle\langle\Phi_{pj}| \otimes |\Psi_{ij}\rangle\langle\Psi_{pj}|\langle p|i\rangle = \sum_{i,j=0}^{n-1} |\Phi_{ij}\rangle\langle\Phi_{ij}| \otimes |\Psi_{ij}\rangle\langle\Psi_{ij}|\langle ij|ij\rangle = \mathbb{I}_{n^2}. \tag{5.6}$$

This corresponds to our equation (5.2). By Lemma 5.2.3, it will hold if and only if Φ, Ψ are orthogonal.

We now show that the trace conditions over $X = A$ and $X = B$ in the GRMZ-orthogonality definition are redundant, in the sense that they hold automatically for all pairs of quantum Latin squares Φ, Ψ, regardless of orthogonality. We analyze the case that $X = B$; the case $X = A$ is similar. The trace

condition yields the following equation:

$$\sum_{i,j,p=0}^{n-1} \langle\Phi_{ij}|\Phi_{pj}\rangle|\Psi_{ij}\rangle\langle\Psi_{pj}| \otimes |i\rangle\langle p| = \mathbb{I}_{n^2}.$$

But this equation holds for any pair of quantum Latin squares Φ, Ψ, as follows:

$$\sum_{i,j,p=0}^{n-1} \langle\Phi_{ij}|\Phi_{pj}\rangle|\Psi_{ij}\rangle\langle\Psi_{pj}| \otimes |i\rangle\langle p| = \sum_{i,j,p=0}^{n-1} \delta_{ip}|\Psi_{ij}\rangle\langle\Psi_{pj}| \otimes |i\rangle\langle p| = \sum_{i,j=0}^{n-1} |\Psi_{ij}\rangle\langle\Psi_{ij}| \otimes |i\rangle\langle i|$$
$$= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} |\Psi_{ij}\rangle\langle\Psi_{ij}| \right) \otimes |i\rangle\langle i| = \sum_{i=0}^{n-1} \mathbb{I}_n \otimes |i\rangle\langle i| = \mathbb{I}_n \otimes \left(\sum_{i=0}^{n-1} |i\rangle\langle i| \right) = \mathbb{I}_n \otimes \mathbb{I}_n.$$

Here the first equality uses the fact that Φ is a QLS, the second equality uses the definition of the Kronecker delta function, the third equality rearranges the sum, the fourth equality uses the fact that Ψ is a QLS, and the final equalities are trivial algebraic manipulations. This completes the proof. □

5.2.3 Equivalence and orthogonality

Two classical Latin squares are said to be equivalent if one can be transformed into the other by permutations of the rows, columns or computational basis state labels. Similarly, there is a notion of equivalence between quantum Latin squares [MV15], which we now recall.

Definition 5.2.9. Two quantum Latin squares Φ, Ψ of dimension n are *equivalent* if there exists some unitary operator U on $\mathbb{C}^n$, family of modulus-1 complex numbers c_{ij}, and permutations $\sigma, \tau \in S_n$, such that the following holds for all $i, j \in [n]$:

$$c_{ij} U|\Phi_{\sigma(i),\tau(j)}\rangle = |\Psi_{ij}\rangle. \tag{5.7}$$

Orthogonality is preserved by taking potentially different equivalences of each QLS, as long as the same pair of permutations are used.

Lemma 5.2.10. *Given quantum Latin squares Φ, Ψ, Φ', Ψ' of dimension n, unitary operators U, V on $\mathbb{C}^n$, families of modulus-1 complex numbers c_{ij}, d_{ij}, and permutations $\sigma, \tau \in S_n$ such that*

$$|\Phi'_{ij}\rangle := c_{ij} U|\Phi_{\sigma(i),\tau(j)}\rangle \qquad \text{and} \qquad |\Psi'_{ij}\rangle := d_{ij} V|\Psi_{\sigma(i),\tau(j)}\rangle, \tag{5.8}$$

then Φ, Ψ are orthogonal if and only if Φ', Ψ' are orthogonal.

Proof. By Lemma 5.2.3 we have the following for all i, j, m, n:

$$\langle \Phi_{mn}|\Phi_{ij}\rangle\langle \Psi_{mn}|\Psi_{ij}\rangle = \delta_{im}\delta_{jn}$$
$$\Leftrightarrow \langle \Phi_{m'n'}|U^\dagger \circ U|\Phi_{i'j'}\rangle\langle \Psi_{m'n'}|V^\dagger \circ V|\Psi_{i'j'}\rangle = \delta_{i'm'}\delta_{j'n'}c_{i'j'}c^*_{i'j'}d_{i'j'}d^*_{i'j'} = \delta_{i'm'}\delta_{j'n'}c_{m'n'}c^*_{i'j'}d_{m'n'}d^*_{i'j'}$$
$$\Leftrightarrow \langle \Phi_{m'n'}|U^\dagger c^*_{m'n'}c_{i'j'}U|\Phi_{i'j'}\rangle\langle \Psi_{m'n'}|V^\dagger d^*_{m'n'}d_{i'j'}V|\Psi_{i'j'}\rangle = \delta_{i'm'}\delta_{j'n'}$$
$$\Leftrightarrow \langle \Phi'_{mn}|\Phi'_{ij}\rangle\langle \Psi'_{mn}|\Psi'_{ij}\rangle = \delta_{im}\delta_{jn}.$$

Where $\sigma(i) = i', \tau(j) = j', \sigma(m) = m'$ and $\tau(n) = n'$. □

We now show that the pair of orthogonal quantum Latin squares illustrated in Example 5.2.2 are not equivalent to any pair of orthogonal Latin squares.

Proposition 5.2.11. *The orthogonal quantum Latin squares of Example 5.2.2 are not equivalent to a pair of orthogonal classical Latin squares.*

Proof. It is enough to show that the left-hand quantum Latin square of Example 5.2.2, which we call Φ, is not equivalent to a classical Latin square. Clearly no permutation of the rows or columns could transform Φ into a classical Latin square. Suppose for a contradiction that there exists a unitary operator V and a set of phases c_{ij} such that $|\eta_{ij}\rangle := c_{ij}V|\Phi_{ij}\rangle$ are all computational basis elements, and therefore yield a classical Latin square. Then for all i, j, m, n, we must have $\langle \eta_{mn}|\eta_{ij}\rangle = 0$ or 1. We choose $m = 0$, $n = 3$, $i = 6$ and $j = 2$ to obtain $\langle \eta_{03}|\eta_{62}\rangle = c^*_{03}c_{62}\langle \Phi_{03}|V^\dagger V|\Phi_{62}\rangle = c^*_{03}c_{62}\langle \Phi_{03}|\Phi_{62}\rangle = c^*_{03}c_{62}\langle 3|U|4\rangle = c^*_{03}c_{62}(1+i)/\sqrt{3}$. But since the c_{ij} have modulus 1, this can never equal 0 or 1, and the contradiction is established. □

5.2.4 Generalization to multiple systems

We now extend this definition to families of quantum Latin squares, generalizing mutually orthogonal Latin squares. In particular, we show that no essentially new concept is introduced, with the existing pairwise orthogonality property being sufficient.

Definition 5.2.12 (MOQLS)**.** A family of m quantum Latin squares $\{\Phi^k | k \in [m]\}$ are *mutually orthogonal* if they are pairwise orthogonal.

We now present the definition of mutually orthogonal quantum Latin squares due to Goyeneche et al. As usual we only consider the definition with respect to families of quantum Latin squares (see Remark 5).

Definition 5.2.13 (GRMZ-MOQLS)**.** A family of m quantum Latin squares $\{\Phi^k | k \in [m]\}$ are *GRMZ–mutually orthogonal* when the following equations hold, where X indicates a partial trace over any of

the $m+1$ subsystems:

$$\mathrm{Tr}_X\left(\sum_{i,j,p,q=0}^{n-1}|\Phi^0_{ij}\rangle\langle\Phi^0_{pq}|\otimes|\Phi^1_{ij}\rangle\langle\Phi^1_{pq}|\otimes...\otimes|\Phi^{m-1}_{ij}\rangle\langle\Phi^{m-1}_{pq}|\otimes|ij\rangle\langle pq|\right)=\mathbb{I}_{n^2}. \tag{5.9}$$

This definition is equivalent to Definition 5.2.12.

Proposition 5.2.14 (MOQLS = GRMZ-MOQLS)**.** *A family of m quantum Latin squares $\{\Phi^k|k\in[m]\}$ are mutually orthogonal just when they are GRMZ–mutually orthogonal.*

Proof. We label the kth QLS system by A_k and the two other systems in equation (5.9) as α and β. So X can range over m element subsets of $\{A_0,A_1,...,A_{m-1},\alpha,\beta\}$. We will label such sets by the two elements that are NOT included so for example $(A_g,A_h)=\{A_0,...,A_{g-1},A_{g+1},...,A_{h-1},A_{h+1},...A_{m-1},\alpha,\beta\}$.

First we show that for all g and h, substituting $X=(A_g,A_h)$ into equation (5.9) reduces to equation (5.2) and so by varying g and h we obtain Definition 5.2.12. Let $X=(A_g,A_h)$ then we have:

$$\sum_{i,j,p,q=0}^{n-1}\langle\Phi^0_{pq}|\Phi^0_{ij}\rangle\cdots\langle\Phi^{g-1}_{pq}|\Phi^{g-1}_{ij}\rangle|\Phi^g_{pq}\rangle\langle\Phi^g_{ij}|\langle\Phi^{g+1}_{pq}|\Phi^{g+1}_{ij}\rangle\cdots\langle\Phi^{g-1}_{pq}|\Phi^{h-1}_{ij}\rangle|\Phi^h_{pq}\rangle\langle\Phi^h_{ij}|\langle\Phi^{h+1}_{pq}|\Phi^{h+1}_{ij}\rangle$$
$$\cdots\langle\Phi^{m-1}_{pq}|\Phi^{m-1}_{ij}\rangle\langle pq|ij\rangle=\mathbb{I}_{n^2}\qquad\Leftrightarrow\qquad\sum_{i,j=0}^{n-1}|\Phi^g_{ij}\rangle\langle\Phi^g_{ij}|\otimes|\Phi^h_{ij}\rangle\langle\Phi^h_{ij}|=\mathbb{I}_{n^2}.$$

Thus by Lemma 5.2.3, equation (5.9) with $X=(A_g,A_h)$ holds if and only if Φ^g and Φ^h are orthogonal. We now show that Definition 5.2.12 implies equation (5.9) for all other possible values of X.

Since $\sum_{j=0}^{n-1}\langle\Phi_{ij}|\Phi_{pj}\rangle=\delta_{ip}$ by the quantum Latin square property, we have that for all k, substituting $X=(A_k,\alpha)$ into equation (5.9) reduces to $\sum_{i,j=0}^{n-1}|\Phi^k_{ij}\rangle\langle\Phi^k_{ij}|\otimes|j\rangle\langle j|=\mathbb{I}_{n^2}$, which holds for all QLSs. Similarly by setting $X=(A_k,\beta)$ we obtain $\sum_{i,j=0}^{n-1}|\Phi^k_{ij}\rangle\langle\Phi^k_{ij}|\otimes|j\rangle\langle j|=\mathbb{I}_{n^2}$ which again holds for all QLSs. Finally we are left with $X=(\alpha,\beta)$, which gives the following:

$$\sum_{i,j,p,q=0}^{n-1}\langle\Phi^0_{ij}|\Phi^0_{pq}\rangle...\langle\Phi^{m-1}_{ij}|\Phi^{m-1}_{pq}\rangle|ij\rangle\langle pq|=\mathbb{I}_{n^2}. \tag{5.10}$$

Split the m QLSs into pairs. Equation (5.3) is equivalent to $\sum_{i,j,p,q=0}^{n-1}\langle\Phi_{ij}|\Phi_{pq}\rangle\langle\Psi_{ij}|\Psi_{pq}\rangle=\delta_{ip}\delta_{qj}$. If m is even then the LHS of equation (5.10) becomes $\sum_{i,j,p,q=0}^{n-1}\delta_{ip}\delta_{pq}|ij\rangle\langle pq|$ which is a resolution of the identity. For m odd we have $\sum_{i,j}^{n-1}\langle\Phi^{m-1}_{ij}|\Phi^{m-1}_{ij}\rangle|ij\rangle\langle ij|$ which again is a resolution of the identity since all entries of a QLS are unit vectors. □

It follows as a corollary of Lemma 5.2.10 that MOQLS are preserved by equivalences in the same way as pairs of orthogonal QLSs.

Corollary 5.2.15. *Given a set of MOQLS Φ^k, the set of quantum Latin squares with entries $c_{ij}U_k|\Phi^k_{\sigma(i),\tau(j)}\rangle$ are also mutually orthogonal, for any set of unitary operators U_k, complex phases c_{ij} and permutations σ, τ.*

5.2.5 Upper bounds on the number of mutually orthogonal quantum Latin squares

We now show that the upper bound for the number of MOQLS of a given size is equal to the upper bound for MOLS.

Theorem 5.2.16. *Any family of MOQLS of dimension n has size at most $n-1$.*

Proof. Suppose that we have a set of m-MOQLS $|\Phi^0_{ij}\rangle, ..., |\Phi^{m-1}_{ij}\rangle$ of size n-by-n. By Corollary 5.2.15 we can apply unitaries to each QLS such that the first row of every QLS is the ordered computational basis $|i\rangle, i \in [n]$ so $|\Phi^k_{0i}\rangle = |i\rangle$ for all $k \in [m], i \in [n]$. Consider $\langle\Phi^k_{10}|\Phi^l_{10}\rangle$ for some $k, l \in [m]$ such that $k \neq l$. We have that:

$$\langle\Phi^k_{10}|\Phi^l_{10}\rangle = \sum_{i=0}^{n-1}\langle\Phi^k_{10}|i\rangle\langle i|\Phi^l_{10}\rangle = \sum_{i=0}^{n-1}\langle\Phi^k_{10}|\Phi^k_{0i}\rangle\langle\Phi^l_{0i}|\Phi^l_{10}\rangle = \sum_{i=0}^{n-1}\langle\Phi^k_{10}|\Phi^k_{0i}\rangle\langle\Phi^{l*}_{10}|\Phi^{l*}_{0i}\rangle$$
$$= \sum_{i,m,n,p,q=0}^{n-1}\langle\Phi^k_{10}|\Phi^k_{0i}\rangle\langle\Phi^{l*}_{10}|\Phi^{l*}_{0i}\rangle\langle 10|mn\rangle\langle pq|0i\rangle = \sum_{i}^{n-1}\langle 10|0i\rangle = \langle 1|0\rangle = 0.$$

The first equality is a resolution of the identity, the second holds since $|\Phi^k_{0i}\rangle = |\Phi^l_{0i}\rangle = |i\rangle$, the third is a straightforward property of inner products, the fourth equality is simple algebraic rearrangement and the fifth equality is due to Lemma 5.2.5 and equation 5.3. So the m unit vectors $|\Phi^i_{10}\rangle$ together with $|0\rangle$ are $m+1$ linearly independent vectors. Thus m can be at most $n-1$. □

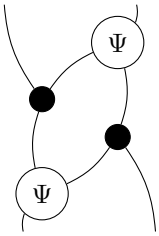
5.3 Biunitaries and perfect tensors

In this section we take a broader perspective on orthogonal QLSs and see that the definition naturally leads to *perfect tensors*, highly symmetric tensors whose properties are very useful in quantum error correction. This connection was discovered by Goyeneche et al [GRDMŻ18].

We begin by defining a *projective quantum Latin square* which is derived from a QLS and associated orthonormal bases (or †-SCFA by Gelfand duality).

Definition 5.3.1. Given a quantum Latin square Ψ with associated †-SCFA , we define the following

linear map to be a *projective quantum Latin square*:



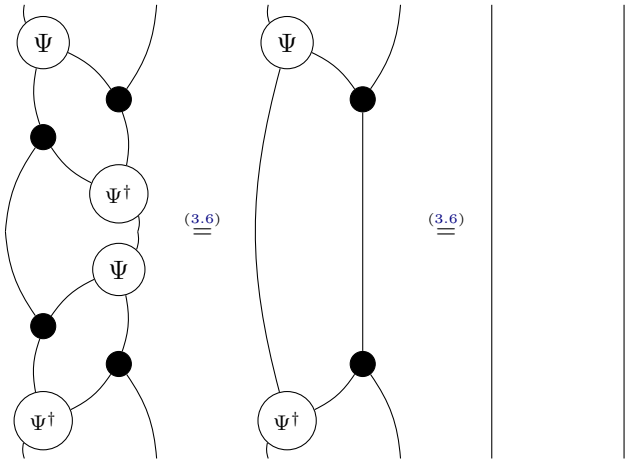
(5.11)

In words: if we consider the bottom left and top right wires to be the indexing systems then a projective QLS is a grid of one dimensional projectors which form orthogonal projective measurements on each row and each column. If we ignore phase data there is a one-to-one correspondence between QLSs and projective QLSs.

In 2016 Ruetter and Vicary gave a graphical description of *biunitaries* and showed that many of the objects of interest in this thesis, QLSs as well as UEBs, Hadamards and controlled Hadamards are examples of biunitaries. To be specific it is projective QLSs that are biunitary, as we shall now see. A 4-valent tensor B is a biunitary if the following linear maps are unitary:



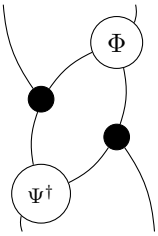
It is easily verifiable that equations (3.6) ensure that projective QLSs are biunitary. We show the first part below:



The composite linear map (5.11) is made up of Ψ and $\Psi^\dagger$. However no relationship between the two are necessary for biunitarity. A composite linear map of the same form as (5.11) but made up of two different QLSs will also be biunitary.

Proposition 5.3.2. *Given a pair of QLSs Ψ and Φ sharing the same associated †-SCFS the following*

linear map is biunitary:



(5.12)

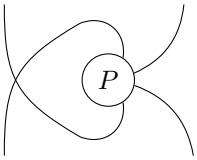
Proof. Straightforward. □

We will see later that this is an example of a *matrix of partial isometries*. We now define a *perfect tensor* and show that one can be constructed from a pair of orthogonal QLSs.

Definition 5.3.3. Given a 4-valent tensor P it is a (4-valent) perfect tensor if the following linear maps are unitary [PYHP15]:



(5.13)



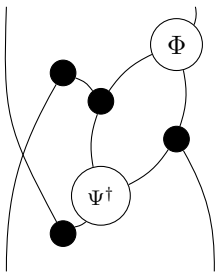
(5.14)

In other words a perfect tensor is a biunitary for which the linear map (5.14) is also unitary.

We now show that given a pair of orthogonal QLSs Ψ and Φ, the linear map (5.12) is a perfect tensor if and only if Ψ and Φ are orthogonal. This result was also proven by Goyeneche et al [GRDMŻ18].

Lemma 5.3.4. *Given a pair of QLSs Ψ and Φ the following are equivalent:*

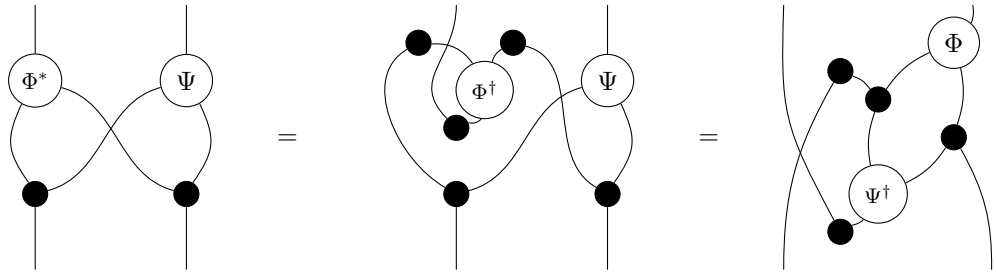
- *Ψ and Φ are orthogonal.*
- *The following linear map is unitary:*



(5.15)

Proof. Combining Lemmas 5.2.5 and 5.2.6 we have that Ψ and Φ are orthogonal if and only if the linear

map on the LHS below is unitary:



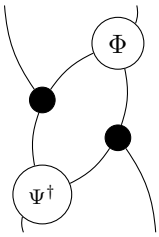
(5.16)

The first equality is replacing Φ^* by $(\Phi^\dagger)^T$ and the second is basic rearranging and black spider merge. □

Now if we combine Lemma 5.3.4 with Proposition 5.3.2 we obtain the following result.

Corollary 5.3.5 (See [GRDMŻ18], Section IV)**.** *Given a pair of QLSs* Ψ *and* Φ *the following are equivalent:*

- Ψ *and* Φ *are orthogonal.*
- *The following linear map is a perfect tensor:*



(5.17)

5.4 Quantum Latin isometry squares and quantum error detecting codes

In this section we introduce quantum Latin isometry squares a generalization of quantum Latin squares and use them to construct quantum error detecting codes. In Section 5.4.1 we give the definition of quantum isometry Latin squares and give a simple example. In Section 5.4.2 we compose pairs of compatible quantum isometry Latin squares and thereby recover both *matrices of partial isometries* and *projective permutation matrices*. In Section 5.4.4 we give orthogonality criteria for pairs and families of quantum isometry Latin squares. In Section 5.4.5 we show how quantum error detecting codes can be constructed from orthogonal pairs of quantum isometry Latin squares. Finally in Section 5.4.6 we show that *unitary error bases* can be characterized as quantum isometry Latin squares that are orthogonal to the *identity square*.

5.4.1 Quantum isometry Latin squares

A normalized vector $|\Psi\rangle$ of dimension n is a trivial example of an isometry $|\Psi\rangle : \mathbb{C} \to \mathbb{C}^n$. We can thus consider n-dimensional QLSs as arrays of isometries of this type. This perspective leads to the following definition which generalizes QLSs.

Definition 5.4.1 (Quantum isometry Latin square)**.** An n-by-n array of isometries $k_{ij} : \mathbb{C}^{a_{ij}} \to \mathbb{C}^d$ is a *quantum isometry Latin square (QILS)*, denoted (k_{ij}, a_{ij}, d) if the following hold for all $i, j, p, q \in [n]$:

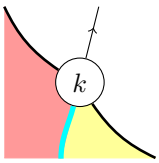
$$k_{ip}^\dagger \circ k_{iq} = \delta_{pq} \mathbb{I}_{a_{ip}}, \tag{5.18}$$

$$k_{pj}^\dagger \circ k_{qj} = \delta_{pq} \mathbb{I}_{a_{mj}}, \tag{5.19}$$

$$\sum_{i=0}^{n-1} k_{ij} \circ k_{ij}^\dagger = \sum_{j=0}^{n-1} k_{ij} \circ k_{ij}^\dagger = \mathbb{I}_d. \tag{5.20}$$

Remark 6. *A quantum Latin square Φ of size n-by-n is a quantum isometry Latin squares such that $a_{ij} = 1$ for all i and j, and is therefore of the form $(|\Phi_{ij}\rangle, 1, n)$.*

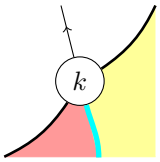
In order to discuss quantum isometry Latin squares graphically we will require the shaded graphical calculus introduced in Section 2.3. Given an n-by-n QILS (k_{ij}, a_{ij}, d) we can represent it as the following type of node using the shaded graphical calculus:



(5.21)

The set of Hilbert spaces $\mathbb{C}^{a_{ij}}$ for $i, j \in [n]$ is represented here by the thick cyan coloured wire. The yellow and pink shaded regions index both the cyan wire and the node k, hence the need for shading.

We will now translate equations (5.18), (5.19) and (5.20) into the shaded graphical calculus. Note that the way the yellow and pink regions are slanted in diagram (5.21) is not canonical and is part of the topology of the diagrams under which the meaning is invariant. The following diagram, which we will also utilize, also represents K diagrammatically:



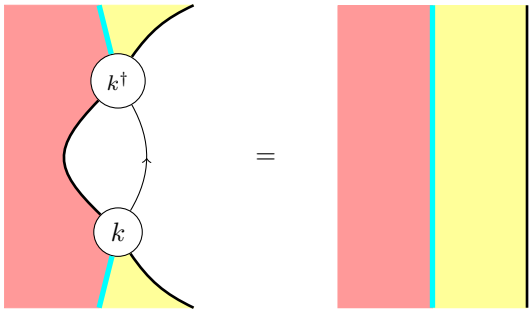
Lemma 5.4.2. *[Diagrammatic QILS] Given a node k as in diagram (5.21), then K is an n-by-n QILS*

(k_{ij}, a_{ij}, d) *if and only if the following linear maps are unitary:*

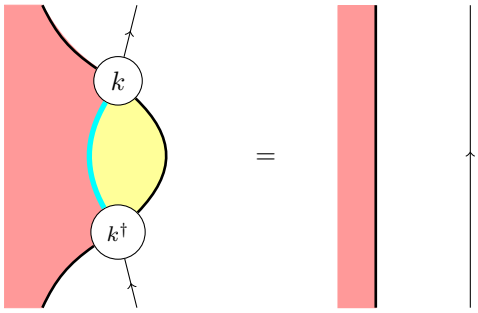


(5.22)

Proof. Equation (5.18) translates diagrammatically as follows:



The RHS of equation (5.20) translates as follows:



We have now shown that the LHS linear map of diagram (5.22) is unitary. Unitarity of the RHS diagram follows similarly from equation (5.19) and the LHS of equations (5.20). □

As a first example, we show how to construct quantum Latin isometry squares from arbitrary families of unitaries.

Example 5.4.3. For a Hilbert space $\mathbb{C}^n$ equipped with a family of m unitaries $\mathcal{U} := \{U_i : \mathbb{C}^n \to \mathbb{C}^n | i \in [m]\}$, we can build a quantum Latin isometry square, denoted $L(\mathcal{U})$, of size m:

$$L(\mathcal{U}) := (U_i \delta_{ij}, n\delta_{ij}, n).$$

Such a quantum Latin isometry square $L(\mathcal{U})$ is diagonal, with nonzero isometries only on the leading diagonal. It is straightforward to see that equations (5.18),(5.19) and (5.20) are satisfied.

5.4.2 Skew projective permutation matrices

Pairs of quantum isometry Latin squares that share the same multiset of values a_{ij} can be composed to form a new structure.

Definition 5.4.4 (Skew projective permutation matrix)**.** Given a pair of n-by-n quantum isometry Latin squares (k_{ij}, a_{ij}, b) and (q_{ij}, a_{ij}, b), let $T_{ij} := q_{ij} \circ k_{ij}^\dagger$. We define the n-by-n array of linear operators $T_{ij} : \mathbb{C}^b \to \mathbb{C}^b$ to be a *skew projective permutation matrix* (skew PPM).

Remark 7. *Let (k_{ij}, a_{ij}, b) and (q_{ij}, a_{ij}, b) be a pair of quantum isometry Latin squares as in Definition 5.4.4 such that $a_{ij} = 1$ for all $i, j \in [n]$ (ie a pair of QLSs). The skew projective permutation matrix $T := \{T_{ij} = q_{ij} \circ k_{ij}^\dagger | i, j \in [n]\}$ is precisely of the form of equation (5.12).*

We now show that skew projective permutation matrices are precisely the *matrices of partial isometries of type (C1,C2,C3,C4)* introduced in a recent paper by Benoist and Nechita [BN17]. These structures were shown to characterize quantum channels preserving pointer states. We first require the following definition.

Definition 5.4.5 (Partial isometry [HM63])**.** A *partial isometry* is a linear map such that the restriction to the orthogonal complement of its kernel is an isometry. Alternatively, a partial isometry A is a linear map such that $A \circ A^\dagger \circ A = A$. The *initial space* of a partial isometry is the orthogonal complement of its kernel. The *final space* is its range.

Two simple examples of partial isometries are orthogonal projectors and unitaries. We now give Benoist and Nechita's definition.

Definition 5.4.6 ([BN17], Definition 3.2 conditions (C1) to (C4))**.** An n-by-n *matrix of partial isometries of type (C1,C2,C3,C4)* and dimension b is an n-by-n array of partial isometries $T_{ij} : \mathbb{C}^b \to \mathbb{C}^b$ such that along each row and column the initial and final spaces of the T_{ij} partition $\mathbb{C}^b$.

Skew PPMs are matrices of partial isometries of type (C1,C2,C3,C4).

Lemma 5.4.7. *Given a pair n-by-n quantum isometry Latin squares (k_{ij}, a_{ij}, b) and (q_{ij}, a_{ij}, b), the corresponding skew PPM is a b dimensional n-by-n matrix of partial isometries of type (C1,C2,C3,C4).*

Proof. Given the pair of isometries $k_{ij}, q_{ij} : \mathbb{C}^{a_{ij}} \to \mathbb{C}^b$ for some $i, j \in [n]$, we form the following composite linear maps:

$$K_{ij} := k_{ij} \circ k_{ij}^\dagger, \qquad Q_{ij} := q_{ij} \circ q_{ij}^\dagger, \qquad T_{ij} := q_{ij} \circ k_{ij}^\dagger.$$

It is easy to see that K_{ij} and Q_{ij} are orthogonal projectors. The linear map T_{ij} is a partial isometry since $T_{ij} \circ T_{ij}^\dagger \circ T_{ij} = q_{ij} \circ k_{ij}^\dagger \circ k_{ij} \circ q_{ij}^\dagger \circ q_{ij} \circ k_{ij}^\dagger = q_{ij} \circ k_{ij}^\dagger = T_{ij}$ with each equality holding either

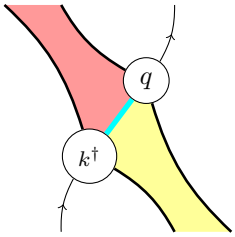
by definition or using the properties of an isometry. It can easily be checked that the initial and final spaces of each T_{ij} are the spaces projected onto by K_{ij} and Q_{ij} respectively. By equations (5.18),(5.19) and (5.20) the initial and final spaces of the T_{ij} partition $\mathbb{C}^b$ along the rows and columns as required. □

Skew PPMs also appear in another, currently very active area of research. Skew PPMs are a generalization of *projective permutation matrices* (PPMs). PPMs are square arrays of orthogonal projectors that form a projective measurement on every row and column. PPMs are skew PPMs coming from pairs of identical quantum isometry Latin squares. In this case the partial isometries T_{ij} are all orthogonal projectors, having the same initial and final spaces. Clearly these projectors form projective measurements on every row and column since the spaces they project onto partition the whole Hilbert space along every row and column by Lemma 5.4.7.

PPMs, also known as magic unitaries and quantum bijections between classical sets have recently appeared in the context of quantum non-local games [ABdSZ17, AMR+19, Mus17, MRV18a] and the study of compact quantum groups [Ban05, Bic03, Wan98].

5.4.3 Skew PPMs are biunitary

Let (k_{ij}, a_{ij}, d) and (q_{ij}, a_{ij}, d) be QILS with associated skew PPM $T_{ij} = q_{ij} \circ k_{ij}^\dagger$. We can diagrammatically capture T as follows:



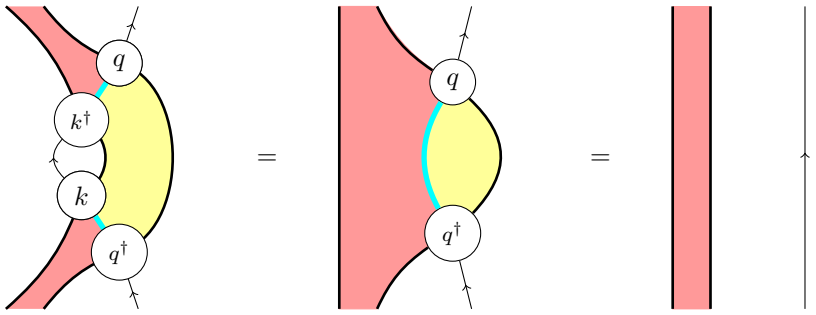
(5.23)

Here the cyan wire represents the Hilbert spaces $\mathbb{C}^{a_{ij}}$ controlled by the pink and yellow shaded regions as usual.

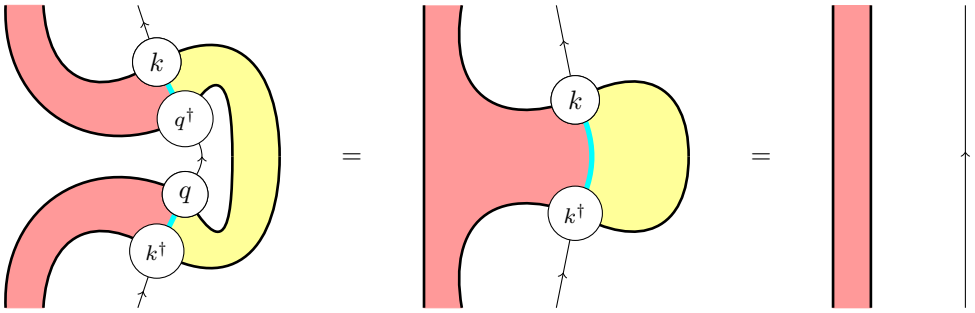
Proposition 5.4.8. *Given T a skew PPM as above, the linear map represented in diagram (5.23) is biunitary.*

Proof. Biunitarity is preserved under the taking of adjoints. As the diagrams work out more easily we

will prove biunitarity of the adjoint of diagram (5.23). We first prove unitarity.



Both equalities hold directly due to Lemma 5.4.2. The other direction is similar. We now show that the other biunitarity condition holds.



Again both equalities hold directly due to Lemma 5.4.2 (note that the different slant of the shaded regions through the k and q nodes is not significant as explained above). The other direction is similar. This completes the proof. □

5.4.4 Orthogonal quantum isometry Latin squares

We now extend the definition of orthogonal quantum Latin squares to quantum isometry Latin squares.

Definition 5.4.9 (Orthogonal quantum isometry Latin squares)**.** A pair of quantum isometry Latin squares (k_{ij}, a_{ij}, d) and (q_{ij}, a_{ij}, d) are *orthogonal* if the operators $T_{ij} = q_{ij} \circ k_{ij}^\dagger$ span the space of operators and for all non-zero T_{ij} we have that $\mathrm{Tr}(T_{ij}^\dagger \circ T_{ij}) = a$ for some $a \in \mathbb{C}$. We say that the T_{ij} form an orthogonal skew PPM.

We now give a more algebraic characterization of orthogonal quantum isometry Latin squares.

Lemma 5.4.10. *Given a pair of n-by-n quantum isometry Latin squares, $K = (k_{ij}, a_{ij}, d)$ and $Q = (q_{ij}, a_{ij}, d)$ define the following linear map $S : \mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^d \otimes \mathbb{C}^d$:*

$$S := \sum_{i,j,p,q=0}^{n-1} \sum_{x=0}^{d-1} |ij\rangle\langle x| q_{ij} \circ k_{ij}^\dagger \otimes \langle x|. \tag{5.24}$$

K and Q are orthogonal just when S is an isometry.

Proof. Assuming K and Q are orthogonal, the partial isometries $q_{ij} \circ k_{ij}^\dagger$ span the operator space. We therefore have:

$$\mathbb{I}_{d^2} = \sum_{i,j=0}^{n-1} \sum_{x,y=0}^{d-1} |y\rangle \otimes k_{ij} \circ q_{ij}^\dagger |y\rangle\langle x| q_{ij} \circ k_{ij}^\dagger \otimes \langle x| \tag{5.25}$$

$$= \sum_{i,j,p,q=0}^{n-1} \sum_{x,y=0}^{d-1} |y\rangle \otimes k_{pq} \circ q_{pq}^\dagger |y\rangle\langle pq|ij\rangle\langle x| q_{ij} \circ k_{ij}^\dagger \otimes \langle x| \tag{5.26}$$

$$= S^\dagger \circ S. \tag{5.27}$$

The other direction follows straightforwardly. □

Remark 8. *Note that $Tr(T_{ij}^\dagger \circ T_{pq}) = \delta_{ip}\delta_{jq} Tr(T_{ij}^\dagger \circ T_{ij})$.*

Remark 9. *A PPM can never be orthogonal since the projectors T_{ij} of a PPM span the operator space for every row and column.*

Orthogonal quantum isometry Latin squares generalize orthogonal QLSs (and therefore orthogonal Latin squares).

Lemma 5.4.11. *Pairs of QLSs are orthogonal quantum isometry Latin squares if and only if they are orthogonal quantum Latin squares.*

Proof. Consider a pair of n-by-n QLSs $(|k_{ij}\rangle, 1, n)$ and $(|q_{ij}\rangle, 1, n)$ such that they are orthogonal quantum isometry Latin squares by Definition 5.4.9. By Lemma 5.4.10, S is an isometry. Since S is a linear operator on a finite-dimensional Hilbert space, S is unitary. This yields the following equation:

$$\sum_{i,j,x,y=0}^{n-1} |k_{ij}\rangle\langle q_{ij}|x\rangle\langle y|q_{ij}\rangle\langle k_{ij}| \otimes |x\rangle\langle y| = \sum_{i,j=0}^{n-1} |k_{ij}\rangle\langle k_{ij}| \otimes |q_{ij}^*\rangle\langle q_{ij}^*| = \mathbb{I}_{n^2}.$$

By Lemmas 5.2.3 and 5.2.5 this holds if and only if $|q_{ij}\rangle$ and $|k_{ij}\rangle$ are orthogonal QLSs. □

We define *mutually orthogonal quantum isometry Latin squares,* to be sets of pairwise orthogonal quantum isometry Latin squares thus generalizing MOLS and MOQLS (see Definition 5.2.12).

We now present an example pair of orhogonal quantum isometry Latin squares which are not QLSs.

Example 5.4.12. We present a pair of orthogonal quantum Latin isometry squares Q and K and associated orthogonal skew PPM, T. We have $n = 8$, $d = 4$ and $a_{ij} = 2$ or 0 for all $i, j \in \{0, ..., 7\}$. There are $d^2 = 16$ non-zero T_{ij} as required to span the operator space.

We fix the computational basis $|a\rangle, |b\rangle$ for $\mathbb{C}^2$ and $|0\rangle, |1\rangle, |2\rangle$ $|3\rangle$ for $\mathbb{C}^4$.

We present the first quantum Latin isometry square Q:

$\|0\rangle\langle a\| + \|1\rangle\langle b\|$	$\|2\rangle\langle a\| + \|3\rangle\langle b\|$	0	0	0	0	0	0
$\|2\rangle\langle a\| + \|3\rangle\langle b\|$	$\|1\rangle\langle a\| + \|0\rangle\langle b\|$	0	0	0	0	0	0
0	0	$\|0\rangle\langle a\| - \|1\rangle\langle b\|$	$\|3\rangle\langle b\| - \|2\rangle\langle a\|$	0	0	0	0
0	0	$\|2\rangle\langle a\| - \|3\rangle\langle b\|$	$\|0\rangle\langle a\| - \|1\rangle\langle b\|$	0	0	0	0
0	0	0	0	$\|1\rangle\langle a\| + \|2\rangle\langle b\|$	$\|0\rangle\langle a\| + \|3\rangle\langle b\|$	0	0
0	0	0	0	$\|3\rangle\langle b\| - \|0\rangle\langle a\|$	$\|2\rangle\langle b\| - \|1\rangle\langle a\|$	0	0
0	0	0	0	0	0	$\|0\rangle\langle a\| + \|2\rangle\langle b\|$	$\|3\rangle\langle b\| - \|1\rangle\langle a\|$
0	0	0	0	0	0	$\|1\rangle\langle a\| + \|3\rangle\langle b\|$	$\|2\rangle\langle b\| - \|0\rangle\langle a\|$

.

Now we present the quantum Latin isometry square K:

$\|0\rangle\langle a\| + \|1\rangle\langle b\|$	$\|2\rangle\langle a\| + \|3\rangle\langle b\|$	0	0	0	0	0	0
$\|2\rangle\langle a\| + \|3\rangle\langle b\|$	$\|0\rangle\langle a\| + \|1\rangle\langle b\|$	0	0	0	0	0	0
0	0	$\|0\rangle\langle a\| + \|1\rangle\langle b\|$	$\|3\rangle\langle a\| + \|2\rangle\langle b\|$	0	0	0	0
0	0	$\|2\rangle\langle a\| + \|3\rangle\langle b\|$	$\|1\rangle\langle a\| + \|0\rangle\langle b\|$	0	0	0	0
0	0	0	0	$\|2\rangle\langle a\| + \|1\rangle\langle b\|$	$\|3\rangle\langle a\| + \|0\rangle\langle b\|$	0	0
0	0	0	0	$\|3\rangle\langle a\| + \|0\rangle\langle b\|$	$\|2\rangle\langle a\| + \|1\rangle\langle b\|$	0	0
0	0	0	0	0	0	$\|2\rangle\langle a\| + \|0\rangle\langle b\|$	$\|3\rangle\langle a\| + \|1\rangle\langle b\|$
0	0	0	0	0	0	$\|3\rangle\langle a\| + \|1\rangle\langle b\|$	$\|2\rangle\langle a\| + \|0\rangle\langle b\|$

.

Finally we present the associated skew projective permutation matrix T with entries T_{ij}:

$\|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|3\rangle\langle 2\| + \|2\rangle\langle 3\|$	0	0	0	0	0	0
$\|2\rangle\langle 2\| + \|3\rangle\langle 3\|$	$\|1\rangle\langle 0\| + \|0\rangle\langle 1\|$	0	0	0	0	0	0
0	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|3\rangle\langle 2\| - \|2\rangle\langle 3\|$	0	0	0	0
0	0	$\|2\rangle\langle 2\| - \|3\rangle\langle 3\|$	$\|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	0	0	0	0
0	0	0	0	$\|2\rangle\langle 1\| + \|1\rangle\langle 2\|$	$\|3\rangle\langle 0\| + \|0\rangle\langle 3\|$	0	0
0	0	0	0	$\|3\rangle\langle 0\| - \|0\rangle\langle 3\|$	$\|2\rangle\langle 1\| - \|1\rangle\langle 2\|$	0	0
0	0	0	0	0	0	$\|2\rangle\langle 0\| + \|0\rangle\langle 2\|$	$\|3\rangle\langle 1\| - \|1\rangle\langle 3\|$
0	0	0	0	0	0	$\|3\rangle\langle 1\| + \|1\rangle\langle 3\|$	$\|2\rangle\langle 0\| - \|0\rangle\langle 2\|$

.

5.4.5 Quantum error detecting codes

We now prove the main result of this section, a construction of quantum error detecting codes from orthogonal skew PPMs. In their famous 1997 paper Knill and Laflamme proved that certain one-to-three 4-valent tensors can be used as encoding maps for quantum codes that can detect any single local error.

Theorem 5.4.13. *[Kni96] Given a three-to-one tensor $\langle E_{ijk}| : \mathbb{C}^a \to \mathbb{C}^b \otimes \mathbb{C}^c \otimes \mathbb{C}^d$, it is an encoding map that detects an arbitrary single q-dit error if the following hold:*

$$\sum_{i=0}^{b-1}\sum_{j=0}^{c-1}\sum_{l,k=0}^{d-1} |E_{ijl}\rangle\langle E_{ijk}| \otimes |l\rangle\langle k| = \mathbb{I}_a \otimes \mathbb{I}_d, \tag{5.28}$$

$$\sum_{i=0}^{b-1}\sum_{l,j=0}^{c-1}\sum_{k=0}^{d-1} |E_{ilk}\rangle\langle E_{ijk}| \otimes |l\rangle\langle j| = \mathbb{I}_a \otimes \mathbb{I}_c, \tag{5.29}$$

$$\sum_{l,i=0}^{b-1}\sum_{j=0}^{c-1}\sum_{k=0}^{d-1} |E_{ljk}\rangle\langle E_{ijk}| \otimes |l\rangle\langle i| = \mathbb{I}_a \otimes \mathbb{I}_b. \tag{5.30}$$

Theorem 5.4.14. *Given an n-by-n pair of orthogonal quantum isometry Latin squares (k_{ij}, a_{ij}, d) and (q_{ij}, a_{ij}, d); the following one-to-three tensor is an encoding map that detects a single error:*

$$\langle T| := \sum_{i,j=0}^{n-1} |i\rangle \otimes q_{ij} \circ k_{ij}^\dagger \otimes |j\rangle. \tag{5.31}$$

Proof. First we show equation (5.28), we have:

$$\sum_{x=0}^{d-1}\sum_{l,i,j=0}^{n-1} |T\rangle\langle T| \otimes |l\rangle\langle i| = \sum_{x=0}^{d-1}\sum_{l,i,j=0}^{n-1} |l\rangle \otimes k_{lj} \circ q_{lj}^\dagger |x\rangle\langle x| q_{ij} \circ k_{ij}^\dagger \otimes \langle i|$$
$$\overset{(5.19)}{=} \sum_{i,j=0}^{n-1} |i\rangle \otimes k_{ij} \circ k_{ij}^\dagger \otimes \langle i| \overset{(5.20)}{=} \mathbb{I}_d \otimes \mathbb{I}_n.$$

Equation (5.30) can be derived from equations (5.18) and (5.20) similarly.

We now show equation (5.29).

$$\sum_{x,y=0}^{d-1}\sum_{i,j=0}^{n-1} |T\rangle\langle T| \otimes |y\rangle\langle x| = \sum_{x,y=0}^{d-1}\sum_{i,j=0}^{n-1} |y\rangle \otimes k_{ij} \circ q_{ij}^\dagger |y\rangle\langle x| q_{ij} \circ k_{ij}^\dagger \otimes \langle x|.$$
$$\overset{(5.26)}{=} \mathbb{I}_{d^2}$$

□

Example 5.4.15. Given the orthogonal skew PPM $T = \{T_{ij} | i, j \in \{0, ..., 7\}\}$ as in Example 5.4.12, by Theorem 5.4.14 the following three-to-one 4-valent tensor is an encoding map that detects a single qubit

local error:

$$\langle T| := \sum_{i,j=0}^{n-1} |i\rangle \otimes T_{ij} \otimes |j\rangle.$$

5.4.6 Orthogonal quantum Latin isometry squares from unitary error bases

Here we recall the standard notion of unitary error basis, and show that they can be characterized as orthogonal pairs of quantum Latin isometry squares, which are not quantum Latin squares. Unitary error bases were introduced by Werner [Wer01], and provide the basic data for quantum teleportation, dense coding and error correction procedures [Wer01, Kni96, Sho96].

Definition 5.4.16. For a Hilbert space $\mathbb{C}^n$, a *unitary error basis* is a family of unitary operators $U_i : \mathbb{C}^n \to \mathbb{C}^n$ which span the space of operators, and which are orthogonal under the trace inner product:

$$\mathrm{Tr}(U_i \circ U_j^\dagger) = n\delta_{ij}. \tag{5.32}$$

We have already seen in Example 5.4.3 that any family of unitaries is a quantum Latin isometry square. We now show that unitary error bases can be characterized in terms of an orthogonal pair of quantum Latin isometry squares. We first define the *identity square*.

Definition 5.4.17 (Identity square)**.** The d-dimensional *identity square* is the quantum Latin isometry square given by $(\mathbb{I}_d\delta_{ij}, d\delta_{ij}, d)$. Note that the identity square is also a skew PPM and a PPM.

We now present the main result of this section.

Theorem 5.4.18. *The following are equivalent:*

- *the set of all n^2-by-n^2 quantum Latin isometry squares that are orthogonal to the n^2-dimensional identity square;*
- *the set of all unitary error basis for $\mathbb{C}^n$.*

Proof. First note that any quantum Latin isometry square that is orthogonal to the identity square must be of the form $(X_{ij}, d\delta_{ij}, d)$ in order to be composed. The isometries X_{ij} are linear operators and must therefore be unitary. The orthogonality condition for the quantum Latin isometry squares unpacks to the requirement that the unitary operators X_i are orthogonal and span the space of operators; this is exactly the unitary error basis condition. □

Part II

Mutually unbiased bases and finite fields

Chapter 6

The correspondence between mutually unbiased bases and unitary error bases

In this chapter we show that maximal families of mutually unbiased bases are characterized in all dimensions by partitioned unitary error bases, up to a choice of a family of Hadamards. We introduce new diagrammatic characterizations of maximal families of mutually unbiased bases, partitioned unitary error bases, Hadamards and controlled Hadamards. We utilize these techniques in the following chapter to construct a maximal family of MUBs from a finite field.

6.1 Introduction

In this chapter we present the following results:

- an equivalence between *partitioned unitary error bases* (partitioned UEBs) and maximal families of MUBs equipped with families of *Hadamards*;
- a new diagrammatic axiomatisation of maximal families of MUBs.

It has been shown that the largest family of d-dimensional mutually unbiased bases that can exist is $d+1$ [BBRV02]. In light of this result we will refer to a family of $d+1$ MUBs as a *maximal family of MUBs*. Maximal families of MUBs represent $d+1$ measurements that are, in some sense 'as far apart as possible', and can perfectly distinguish any density operator on a d-dimensional Hilbert space [WF89]. Maximal families of MUBs are fundamental to areas such as quantum tomography [Ivo81] and quantum key distribution [CBKG02] and are as such of great importance to quantum information. In spite of

this much is still to be discovered about maximal families of MUBs. In general dimension it is not even known whether maximal families of MUBs exist although the existence of maximal families of MUBs in prime power dimension has long been established [BBRV02, GR09, BSTW05].

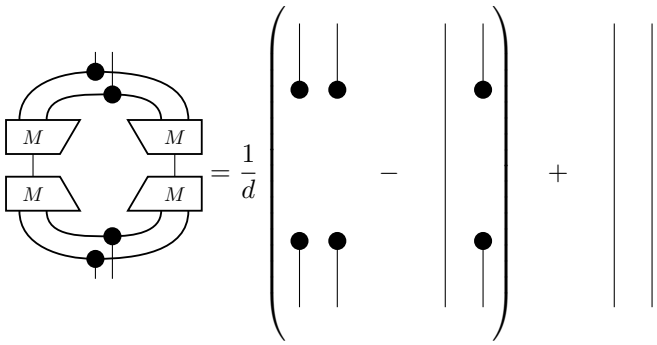
Definition 6.1.1 (Mutually unbiased bases [WF89])**.** A pair of orthonormal bases $|a_i\rangle$ and $|b_i\rangle$ with $i \in \{0, ..., d-1\}$ are *mutually unbiased* if $|\langle a_i|b_j\rangle|^2 = 1/d$ for all $i, j \in \{0, ..., d-1\}$.

Definition 6.1.2 (Family of mutually unbiased bases)**.** A family of bases of a d-dimensional Hilbert space are a *mutually unbiased family* if they are pairwise mutually unbiased.

Definition 6.1.3 (Unitary error basis [Kni96])**.** A *unitary error basis* on a d-dimensional Hilbert space is a family of d^2 unitary operators U_{ij} where $i, j \in \{0, ..., d-1\}$ such that:

$$\mathrm{tr}(U_{ij}^\dagger \circ U_{mn}) = \delta_{im}\delta_{jn}d. \tag{6.1}$$

In this chapter we make extensive use of the canonical basis as an indexing set. We denote the associated canonical †-SCFA as a black dot . In Section 6.4 we start by proving that the following diagrammatic equation completely characterizes maximal families of MUBs using the computational basis tensor, where M is a linear map of type $\mathcal{H} \otimes \mathcal{H} \to \mathcal{H}$:



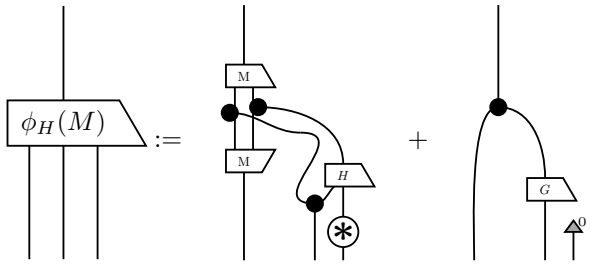
(6.2)

Unitary error bases (UEBs) are fundamental to protocols such as teleportation and dense coding as well as finding application in quantum error correction [Wer01, KR03, MV15, Ste96].

Partitioned UEBs [BBRV02] are unitary error bases containing the identity operator equipped with a partition into the identity and $d+1$ disjoint classes each containing $d-1$ commuting operators. From a partitioned UEB we can obtain a maximal family of MUBs by taking the common eigenbases of each of the commuting classes of operators [BBRV02]. We denote the map taking a partitioned UEB to its eigenbases by θ.

Later in Section 6.4, making use of our diagrammatic maximal families of MUBs, we introduce the following converse map ϕ_H : (Maximal family of MUBs) $\to$ (Partitioned UEBs) given extra data in the

form of a family of Hadamards G and H_i (here $*$ is a projector defined using):



(6.3)

We show that given a family of Hadamards H_i the composition $\theta \circ \phi_H$ is the identity and thus conclude that all maximal families of MUBs can be obtained in this way up to a choice of H_i which we identify with eigenvalues. Each maximal MUB is associated with an infinite family of partitioned UEBs which are not necessarily equivalent.

Related work. In their 2002 paper, Bandyopadhyay et al [BBRV02] introduced partitioned UEBs and showed how to obtain maximal families of MUBs from them.

6.2 Background

We begin by reviewing the definitions of mutually unbiased bases and unitary error bases (UEBs). The following result was given a particularly simple and elegant proof by Bandyopahyay et al [BBRV02].

Theorem 6.2.1. *The largest family of MUBs that can exist on a d-dimensional Hilbert space is a family of $d+1$ MUBs.*

In Section 6.4 we prove the correctness of the diagrammatic characterization of maximal families of MUBs given in the introduction. We now define the equivalence of pairs of UEBs.

Definition 6.2.2 (Equivalent UEBs [Wer01])**.** Given UEBs X_{ij} and Y_{ij} they are *equivalent* if there exist unitary operators U and V, complex numbers with unit absolute value c_{ij} and permutation p such that:

$$X_{ij} = c_{ij} U Y_{p(i,j)} V. \tag{6.4}$$

Later we will formally define partitioned UEBs in Definition 6.4.3, and give a diagrammatic characterization of UEBs [Mus14] in Proposition 6.4.2, with an additional diagrammatic axiom for partitioned UEBs given in Lemma 6.4.4.

Definition 6.2.3 (Hadamard)**.** A *Hadamard* matrix of order d is a $d \times d$ matrix H, such that $|H_{ij}| = 1$ and $HH^\dagger = H^\dagger H = d\mathbb{I}_d$ [BN08].

6.3 Diagrammatic controlled Hadamards and permutations

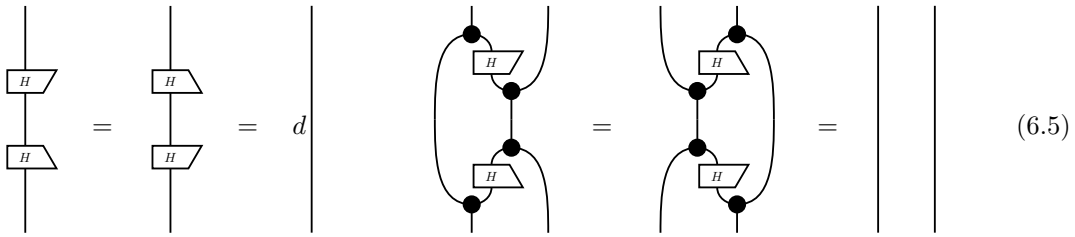
Hadamards with the addition of a normalization constant, are precisely change of basis matrices between pairs of mutually unbiased bases [BBE+07]. To see how mutually unbiased bases can be recovered from Definition 6.2.3, consider the following. Given a Hadamard H, the matrix $\frac{1}{\sqrt{d}}H$ is unitary, since $HH^\dagger = H^\dagger H = d\mathbb{I}_d$. So $\frac{1}{\sqrt{d}}H$ is a change of basis matrix between two orthonormal bases. Let $H' := \frac{1}{\sqrt{d}}H$, represent the computational basis states by $|a_i\rangle$ and define $H'|a_i\rangle := |b_i\rangle$. The other Hadamard condition gives us that for all i, j we have $|H_{ij}| = 1$ thus $|H_{ij}|^2 = 1$ and so:

$$|\langle a_j|b_i\rangle|^2 = |\langle a_j|H'|a_i\rangle|^2 = |\langle a_j|\frac{1}{\sqrt{d}}H|a_i\rangle|^2 = \frac{1}{d}|\langle a_j|H|a_i\rangle|^2 = \frac{1}{d}|H_{ij}|^2 = \frac{1}{d}.$$

This gives us back Definition 6.1.1.

We now introduce a diagrammatic axiomatisation of Hadamards and controlled Hadamards which are indexed families of Hadamards. Recall from Chapter 5 that both of these structures are biunitary. For the rest of this chapter black wires will represent the d-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^d$. We will take the black †-SCFA to be the †-SCFA corresponding to the computational basis of $\mathcal{H}$.

Lemma 6.3.1 (Hadamard)**.** *Given a †-SCFA on a d-dimensional Hilbert space $\mathcal{H}$, a linear map of type $H : \mathcal{H} \to \mathcal{H}$ is a Hadamard if and only if the following equations hold:*



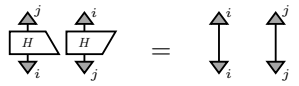
(6.5)

Proof. The left hand side of (6.5) is simply a diagrammatic translation of $HH^\dagger = H^\dagger H = d\mathbb{I}_d$. We now show the equivalence of the right hand side (6.5) and the other condition of Definition 6.2.3 namely; for all i, $j \in [d]$ we have $|H_{ij}| = 1$.

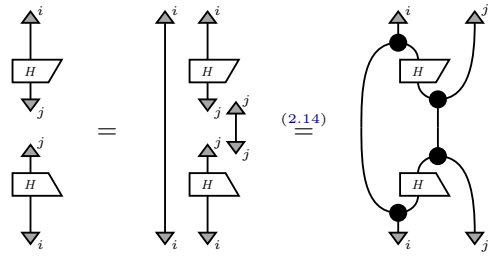
For all $i, j \in [d]$:

$$\begin{aligned} & |H_{ij}| = 1 \\ \Leftrightarrow\ & |\langle i|H|j\rangle| = 1 \\ \Leftrightarrow\ & \langle i|H|j\rangle\langle j|H^\dagger|i\rangle = 1 \\ \Leftrightarrow\ & \langle i|H|j\rangle\langle j|H^\dagger|i\rangle = \langle i|i\rangle\langle j|j\rangle. \end{aligned}$$

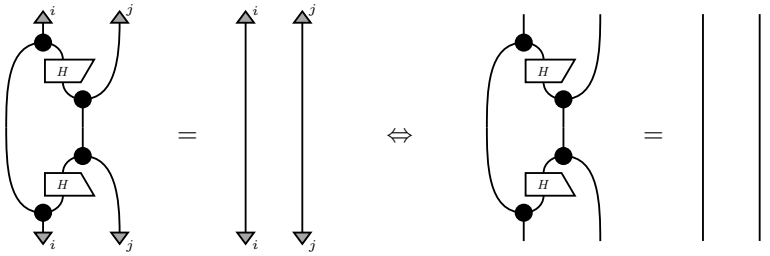
We now translate this final equation into the graphical calculus; for all $i, j \in [d]$:



Rearranging the left hand side we have; for all $i, j \in [d]$:

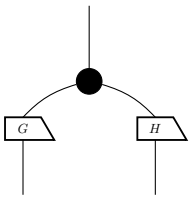


Thus we have that; for all $i, j \in [d]$:



Since $\langle i|H|j\rangle\langle j|H^\dagger|i\rangle = \langle i|i\rangle\langle j|j\rangle \Leftrightarrow \langle j|H^\dagger|i\rangle\langle i|H|j\rangle = \langle i|i\rangle\langle j|j\rangle$ the other part of the right hand side of (6.5) follows similarly. □

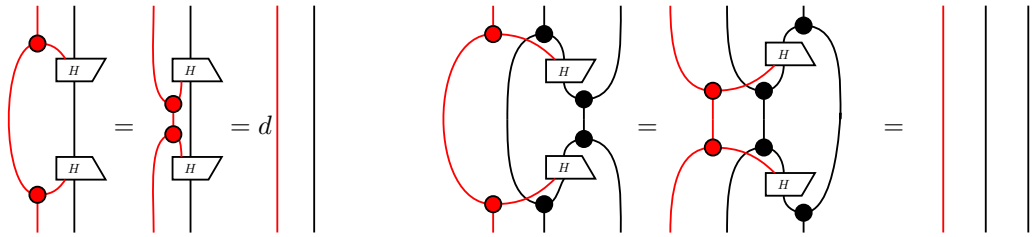
Remark 10. *Notice the similarity between equations* (6.5) *and the diagrammatic characterization of QLS given in Chapter 3 by equations* (3.6)*. We already know that Hadamards and QLS are both types of biunitary, the following composite of two Hadamards G and H with the computational †-SCFA as discovered by Reutter and Vicary can easily be shown to be a QLS [RV16]:*



We now introduce a mathematical object which captures the idea of an indexed family of Hadamards. We introduce another Hilbert space which we will represent with a red wire, equipped with a †-SCFA. The states copyable by this †-SCFA will index the Hadamards in the family.

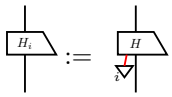
Definition 6.3.2 (Controlled Hadamard)**.** Given a †-SCFA on a d-dimensional Hilbert space $\mathcal{H}$ and

another †-SCFA, on a, possibly different, Hilbert space $\mathcal{G}$, a linear map $H : \mathcal{G} \otimes \mathcal{H} \to \mathcal{G}$ is a *controlled Hadamard* if the following equations hold.



(6.6)

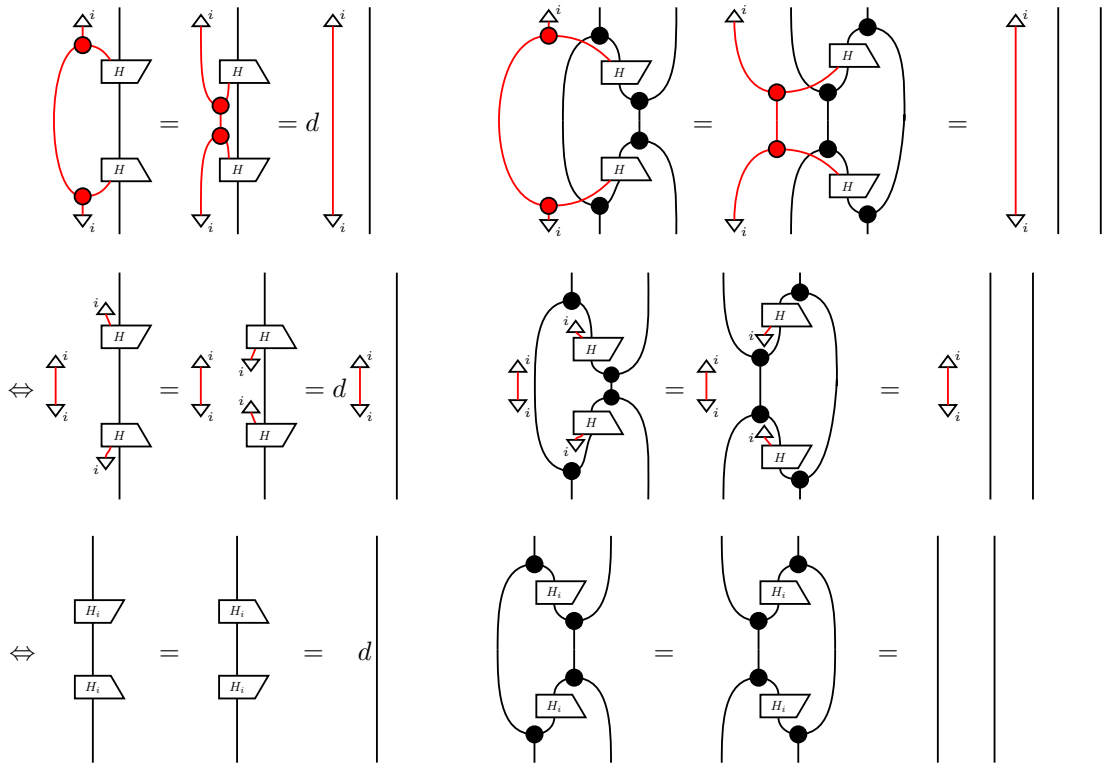
Controlled Hadamards are indexed families of Hadamards in the following sense. Given a controlled Hadamard H and some state $|i\rangle$ copyable by , we define H_i as follows:



(6.7)

For all copyable states $|i\rangle$, H_i as defined above is a Hadamard.

Proof. If we pre-compose equations (6.6) with $|i\rangle \otimes \mathbb{I}$ and post-compose by $\langle i| \otimes \mathbb{I}$ we obtain:

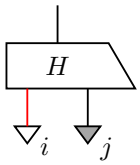


So by Lemma 6.3.1, for all i, H_i is a Hadamard. □

Thus given a controlled Hadamard, the number of Hadamards in the family is equal to the dimension of the red Hilbert space, which in practice, for our purposes is often the same as the black Hilbert space.

Considering the above lemma and the discussion below Definition 6.2.3 we have the following corollary.

Corollary 6.3.3. *Given a controlled Hadamard H with black †-SCFA and n-dimensional red †-SCFA define the following bases $\mathcal{B}^i := |b^i_j\rangle | j \in [n]$; where $|b^i_j\rangle$ is defined as follows:*

$$|b^i_j\rangle := \frac{1}{\sqrt{d}}$$ 

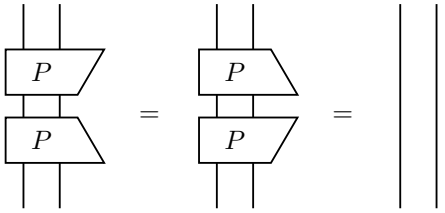
(6.8)

Then each basis $\mathcal{B}^i$ is mutually unbiased to the black basis.

Definition 6.3.4 (Permutation)**.** A *permutation* with respect to a †-SCFA is a cohomomorphism of the †-SCFA which is unitary.

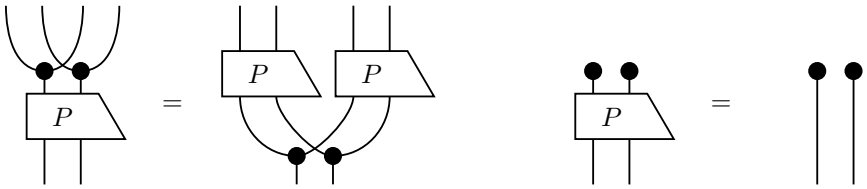
Remark 11. *In* **FHilb** *Definition 6.3.4 gives the usual notion of a permutation matrix where the †-SCFA is a choice of basis.*

We will later require a diagrammatic characterization for a permutation P of type $\mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ with respect to the tensor product of the standard black †-SCFA, with itself. The condition that P must be unitary becomes:



(6.9)

Referring to Definition 2.1.7 we require the following equations:



(6.10)

This ensures that given black basis states $|i\rangle$ and $|j\rangle$ we have $P(|i\rangle \otimes |j\rangle) = |m\rangle \otimes |n\rangle$ for some n, m also black basis states.

6.4 Maximal families of MUBs and partitioned UEBs

We now move on to the discussion of maximal MUBs. For this section we will use only black wires and all wires will represent the Hilbert space $\mathcal{H} \cong \mathbb{C}^d$. We consider the black basis states of the †-SCFA

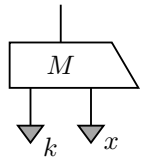
as the computational basis denoted by $\downarrow_i$, $i \in [d]$ and use them as an indexing set in the way described in the previous section.

6.4.1 Diagrammatic characterizations

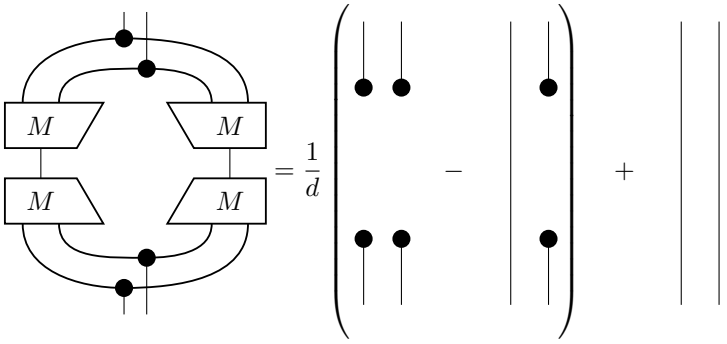
We now give a graphical characterization of a maximal MUB, which we will show to be equivalent to Definition 6.1.1. We characterize a maximal family of MUBs as a linear map M of type $\mathcal{H} \otimes \mathcal{H} \to \mathcal{H}$ together with the computational basis †-SCFA $\curvearrowleft$. Let the $d+1$ bases of a maximal MUB be denoted $\mathcal{B}^i, i \in \{*, 0, 1, ...d-1\}$, where the kth basis state of $\mathcal{B}^x$ is denoted $|b_x^k\rangle$.

We take the states of the basis $\mathcal{B}^*$ to be those copyable by $\curvearrowleft$, so $\downarrow_i := |b_i^*\rangle$. The linear map M encodes the d^2 basis states of the remaining d bases in the following way. Given black basis states $\downarrow_k$ and $\downarrow_x$:

$$|b_x^k\rangle = \tag{6.11}$$

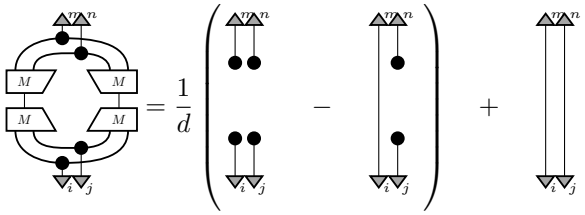


Theorem 6.4.1 (Diagrammatic maximal MUBs)**.** *Given a †-SCFA $\curvearrowleft$ on a d-dimensional Hilbert space $\mathcal{H}$, a linear map M of type $\mathcal{H} \otimes \mathcal{H} \to \mathcal{H}$ is a maximal family of MUBs iff $\sqrt{d}M$ is a controlled Hadamard and the following equation holds.*

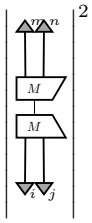


(6.12)

Proof. Consider composition by arbitrary black basis states $\downarrow_i \downarrow_j$ and effects $\uparrow_m \uparrow_n$ on both sides of the equation (6.12).



$$\Leftrightarrow \quad \left| \right|^2 = \frac{1}{d}(1-\delta_{im}) + \delta_{im}\delta_{jn}.$$



Since i, j, m and n were chosen arbitrarily this holds for all values of i, j, m and n. So our diagrammatic axiom is equivalent to the following; for all $i, j, m, n \in [d]$:

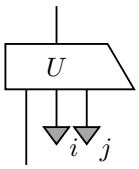
$$|\langle b_j^i | b_n^m \rangle|^2 = \frac{1}{d}(1-\delta_{im}) + \delta_{im}\delta_{jn}. \tag{6.13}$$

For $i = m$ we have $|\langle b_j^i | b_n^i \rangle|^2 = \delta_{jn}$, which indicates that for all i, $\mathcal{B}^i$ is an orthonormal basis. For $i \neq m$ we have $|\langle b_j^i | b_n^m \rangle|^2 = 1/d$, in other words $\mathcal{B}^i$ and $\mathcal{B}^m$ are mutually unbiased.

The requirement that $\sqrt{d}M$ is a controlled Hadamard ensures that each basis is mutually unbiased to the black basis by Corollary 6.3.3. □

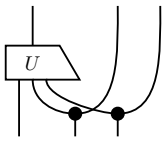
We now give a diagrammatic characterization of unitary error bases which first appeared in the author's masters thesis [Mus14] and is equivalent to Definition 6.1.3 as we show.

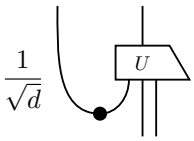
Proposition 6.4.2 (Diagrammatic unitary error bases)**.** *Given a d-dimensional Hilbert space $\mathcal{H}$ with a †-SCFA* *, and linear map $U : \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H} \to \mathcal{H}$, define the following family of linear maps $U_{ij} | i, j \in [d]$:*

$$U_{ij} :=$$ 

(6.14)

The linear maps U_{ij} are a unitary error basis iff the linear maps are unitary:



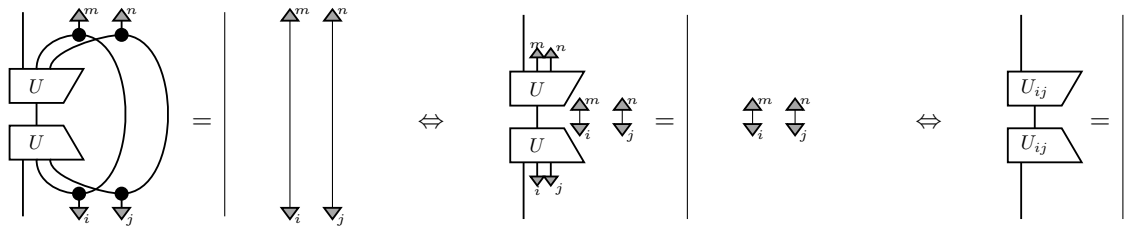


(6.15)

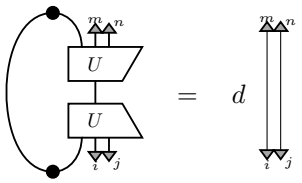
Proof. We first show that the left hand equation of equation (6.15) is equivalent to each U_{ij} being unitary.

We compose the left hand linear map with its adjoint and with the black states and effects 

as follows; for all i, j, m, n:

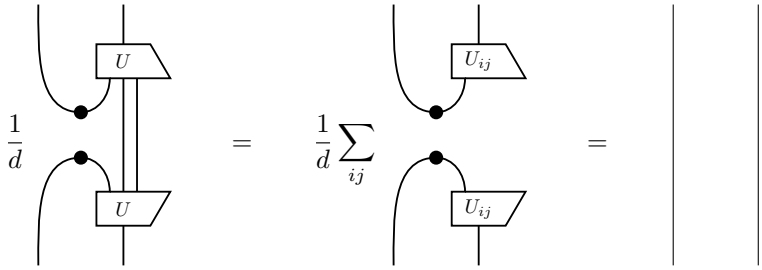


So it is equivalent to all U_{ij} being isometric operators, precomposing by the adjoint gives the other direction. We now show that the right hand diagram (6.15) being unitary is equivalent to equation (6.1). We again compose by its adjoint and by black states and effects to obtain; for all i, j, m, n:



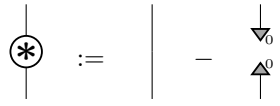
$$\Leftrightarrow \qquad \mathrm{tr}(U_{ij}^{\dagger} \circ U_{mn}) = \delta_{im}\delta_{jn}d.$$

Composing in the opposite direction gives the following:



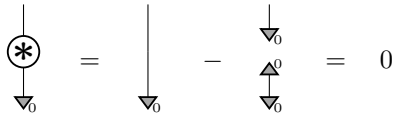
This is the condition that the linear operators U_{ij} span the space of operators $\mathcal{B}(\mathcal{H}) \cong \mathcal{H}^* \otimes \mathcal{H} \cong \mathcal{H} \otimes \mathcal{H}$. Given that the U_{ij}s are orthogonal and that there are n^2 of them this must be the case. This completes the proof. □

We now introduce notation for a projector which we will require in our description of partitioned UEBs:



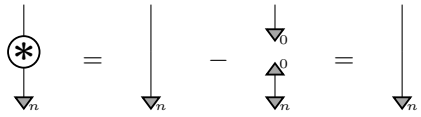
(6.16)

Note that:



(6.17)

Also note that for $n \neq 0$:



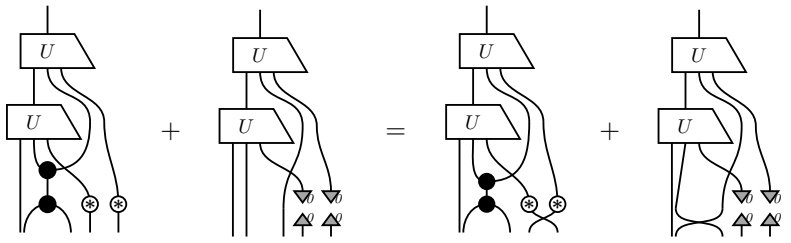
(6.18)

It can easily be shown that there exists a maximum of d commuting unitary operators in dimension d [BBRV02]. We now define partitioned UEBs (partitioned UEBs).

Definition 6.4.3 (Partitioned unitary error basis [BBRV02])**.** A *partitioned unitary error basis* (partitioned UEB), is a d-dimensional UEB containing the identity, with a partition $\{\mathrm{id}_d\} \sqcup C_* \sqcup C_0 \sqcup ... \sqcup C_{d-1}$, such that each class $C_i, i \in \{*\} \sqcup [d]$ contains exactly $d-1$ matrices, which together with $\mathbb{I}_d$ form maximal classes of d commuting operators.

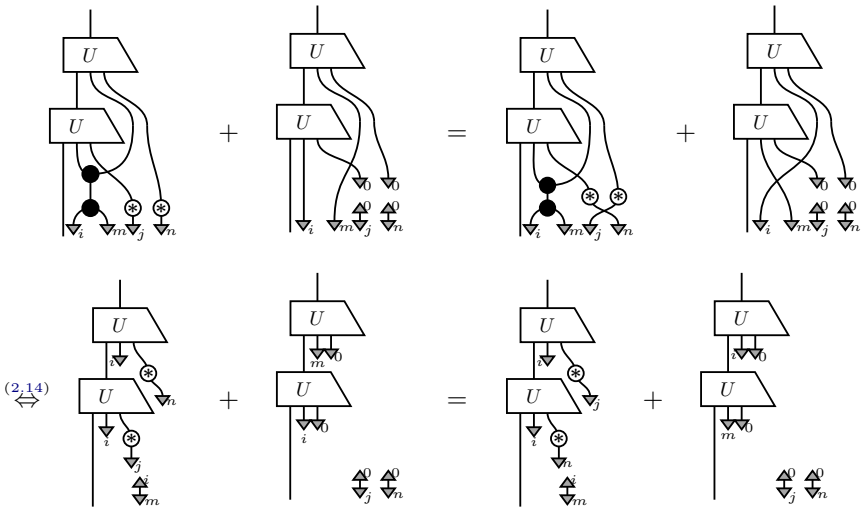
We now give a diagrammatic characterization of partitioned UEBs. We assume that the partitioned UEB has been ordered such that $U_{00} = \mathbb{I}_d$, $C_* = \{U_{a0} | a \in [d] \backslash \{0\}$ and for $i \in [d]$, $C_i = \{U_{ik} | k \in [d] \backslash \{0\}\}$. Up to equivalence (see Definition 6.4) any partitioned UEB can be written in this way. We also choose the computational basis †-SCFA  such that the class C_* is diagonal with respect to it.

Lemma 6.4.4. *A unitary error basis U, with U_{00} equal to the identity, is a partitioned UEB iff the following diagrammatic equation holds.*



(6.19)

Proof. To show the equivalence with Definition 6.4.3 we compose with black states  in the following way; for all $i, j, m, n \in [d]$:



If $j = 0$ and $n \neq 0$ we obtain $0 + 0 = 0 + 0$, the first zero in each summand being due to equation (6.17), the second summands are multiplied by $\langle 0|n\rangle = 0$. Similarly if $j \neq 0$ and $n = 0$ we obtain $0 + 0 = 0 + 0$. So no condition is imposed by equation (6.19) unless either, case one $j = n = 0$ or case two $j \neq 0$ and $n \neq 0$.

Case one. For $j = n = 0$, again by equation (6.17) we obtain for all i, m:

$$\begin{aligned} 0 + \langle 0|0\rangle^2 U_{m0} U_{i0} &= 0 + \langle 0|0\rangle^2 U_{i0} U_{m0} \\ \Leftrightarrow \quad U_{m0} U_{i0} &= U_{i0} U_{m0}. \end{aligned}$$

This shows that the class C_* together with the identity, U_{00} form a maximal class of commuting operators.

Case two. For $j \neq 0$ and $n \neq 0$ by equation (6.18) we obtain for all i, m:

$$\begin{aligned} \langle i|m\rangle U_{in} U_{ij} + \langle 0|j\rangle\langle 0|n\rangle U_{m0} U_{i0} &= \langle i|m\rangle U_{ij} U_{in} + \langle 0|j\rangle\langle 0|n\rangle U_{i0} U_{m0} \\ \Rightarrow \quad \delta_{im} U_{in} U_{ij} &= \delta_{im} U_{ij} U_{in}. \end{aligned}$$

For $i \neq m$ this gives $0 = 0$, for $i = m$ we have that for each i the $d-1$ operators U_{ik} with $k \in \{1, ..., d-1\}$ pairwise commute. Thus the classes C_i with $i \in [d]$ together with the identity U_{00} form maximal classes of commuting operators. This completes the proof. □

6.5 Main results

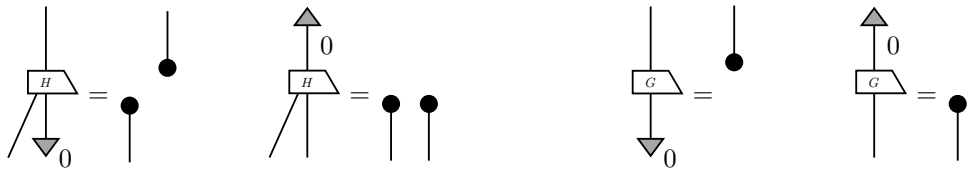
We first present the following theorem due to Bandyopadhyay et al [BBRV02].

Theorem 6.5.1. *Given U, a partitioned UEB, the common eigenbases $|b_k^i\rangle$ for each class $C_i | i \in [d]$ form a maximal family of MUBs.*

As a notational point we introduce θ to represent the map from partitioned UEBs to maximal families of MUBs given by Theorem 6.5.1. In their paper Banyopadhyay et al also give a construction which takes a maximal MUB in dimension d and the Fourier matrix for the cyclic group $\mathbb{Z}_d$ and gives a partitioned UEB. The following construction generalizes theirs.

In the following construction we will use a Hadamard G and a controlled Hadamard H (see Definition 6.3.2). Every Hadamard is equivalent to a Hadamard with ones along the first column and first row [BBE+07]. We assume that each Hadamard in the controlled family as well as G are in this

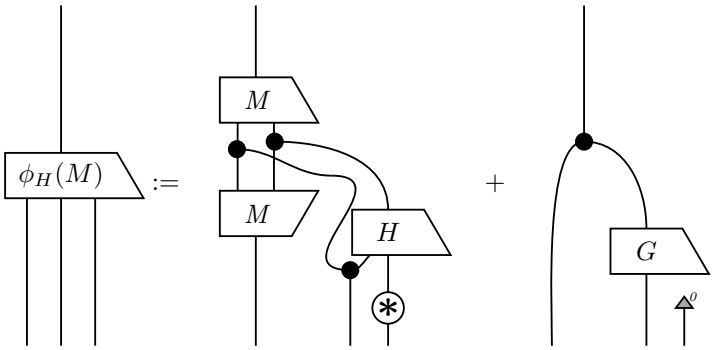
form. This gives us the following axioms.



(6.20)

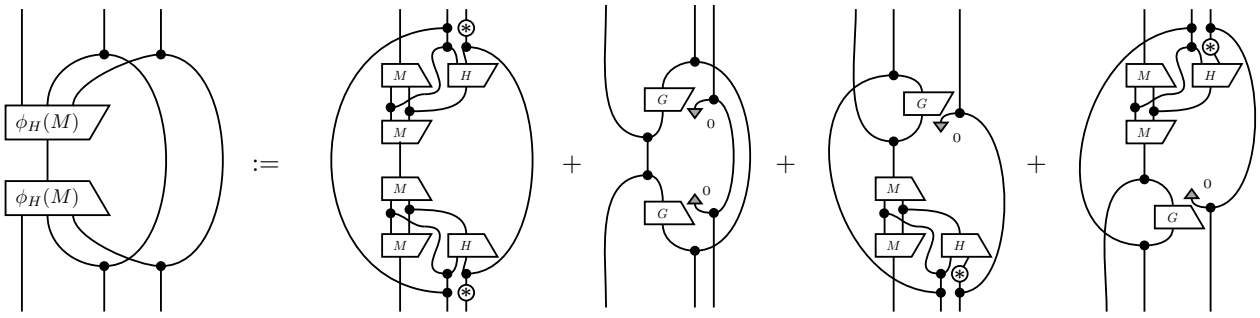
We now provide the main result of this section, a converse to Theorem 6.5.1 taking a maximal MUB and a controlled Hadamard to construct a partitioned UEB. We will later show in Theorem 6.5.3, that if we start with a partitioned UEB and then obtain a maximal MUB by taking the eigenbases (see Theorem 6.5.1) and then perform the following construction we recover the partitioned UEB we started with.

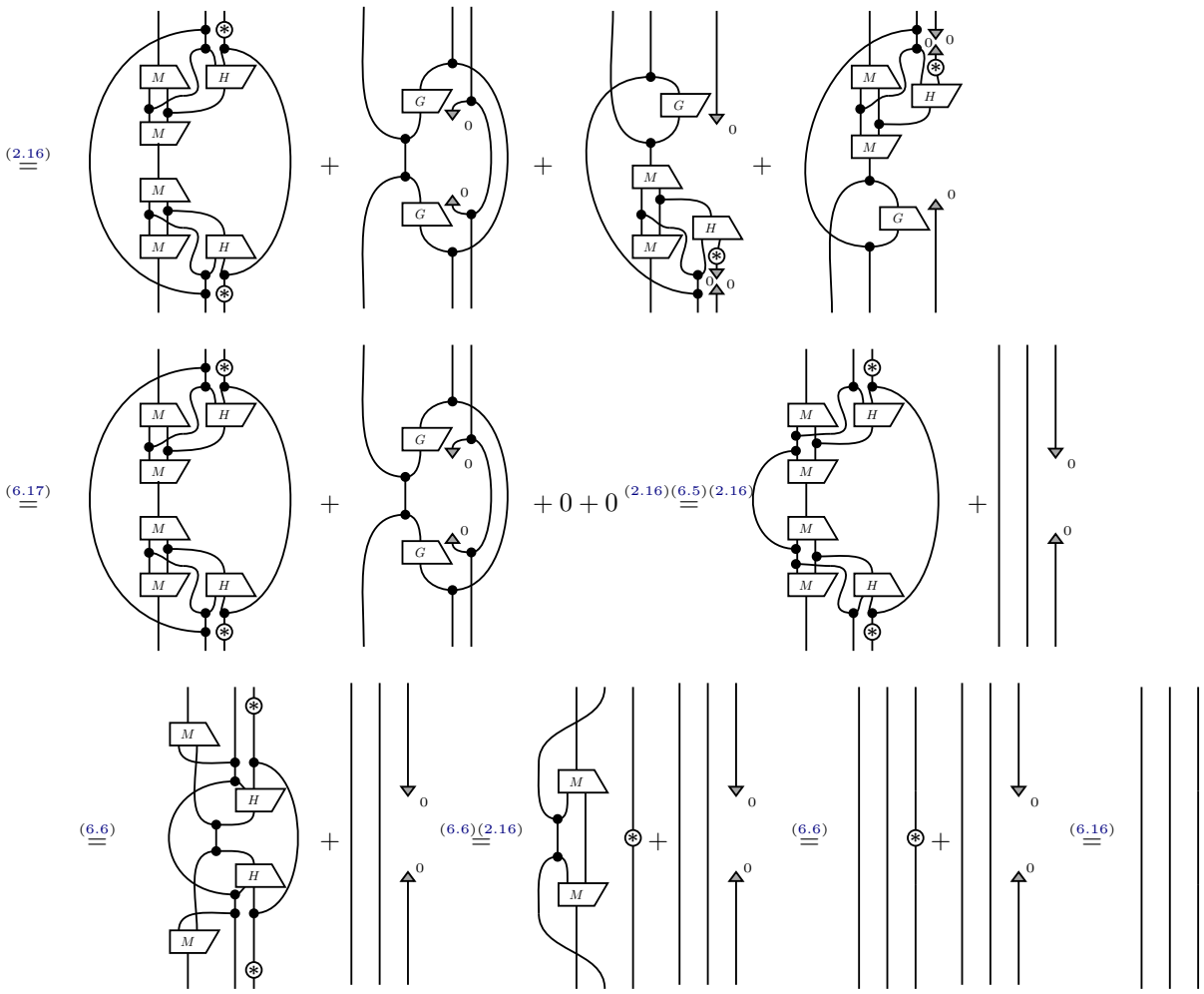
Theorem 6.5.2. *Given a maximal MUB on a d-dimensional Hilbert space, a controlled Hadamard H and an additional Hadamard G the following map ϕ_H gives a partitioned UEB:*



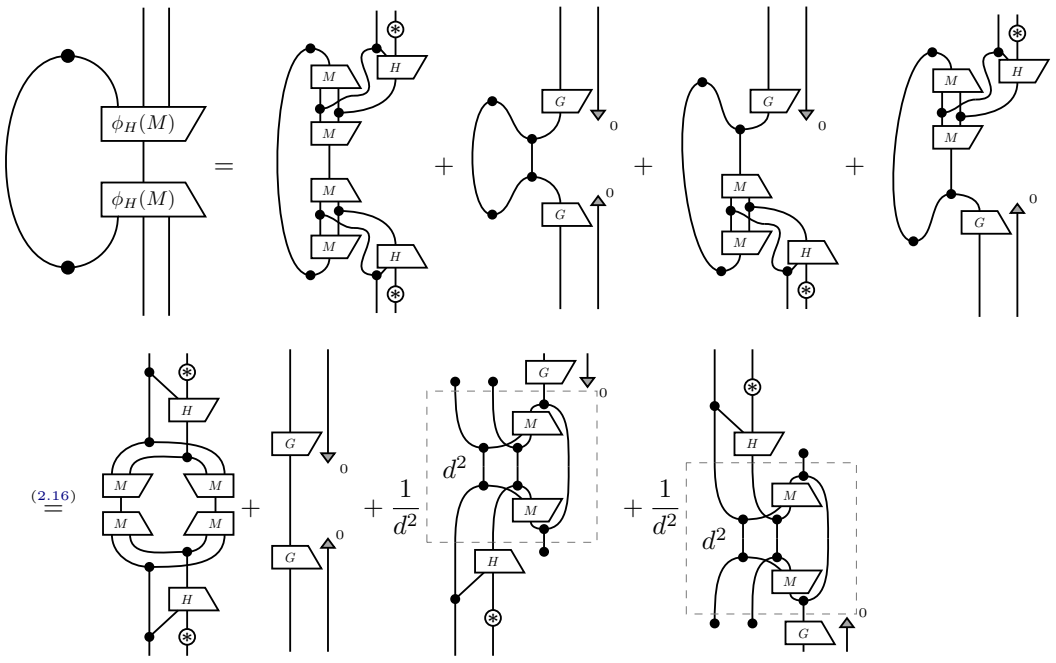
(6.21)

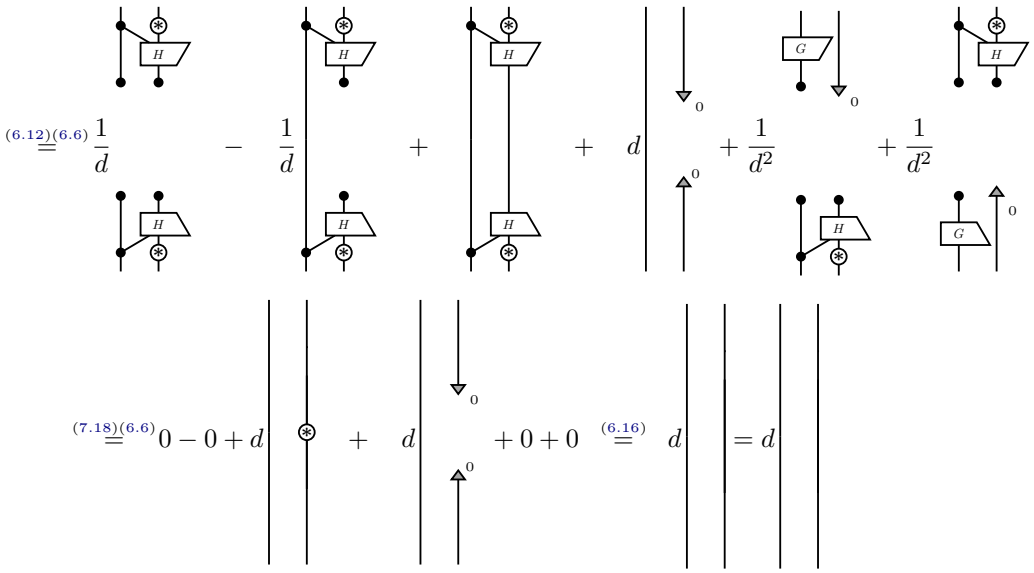
Proof. We now show that $\phi_H(M)$ is a UEB. First the left hand equation of (6.15).



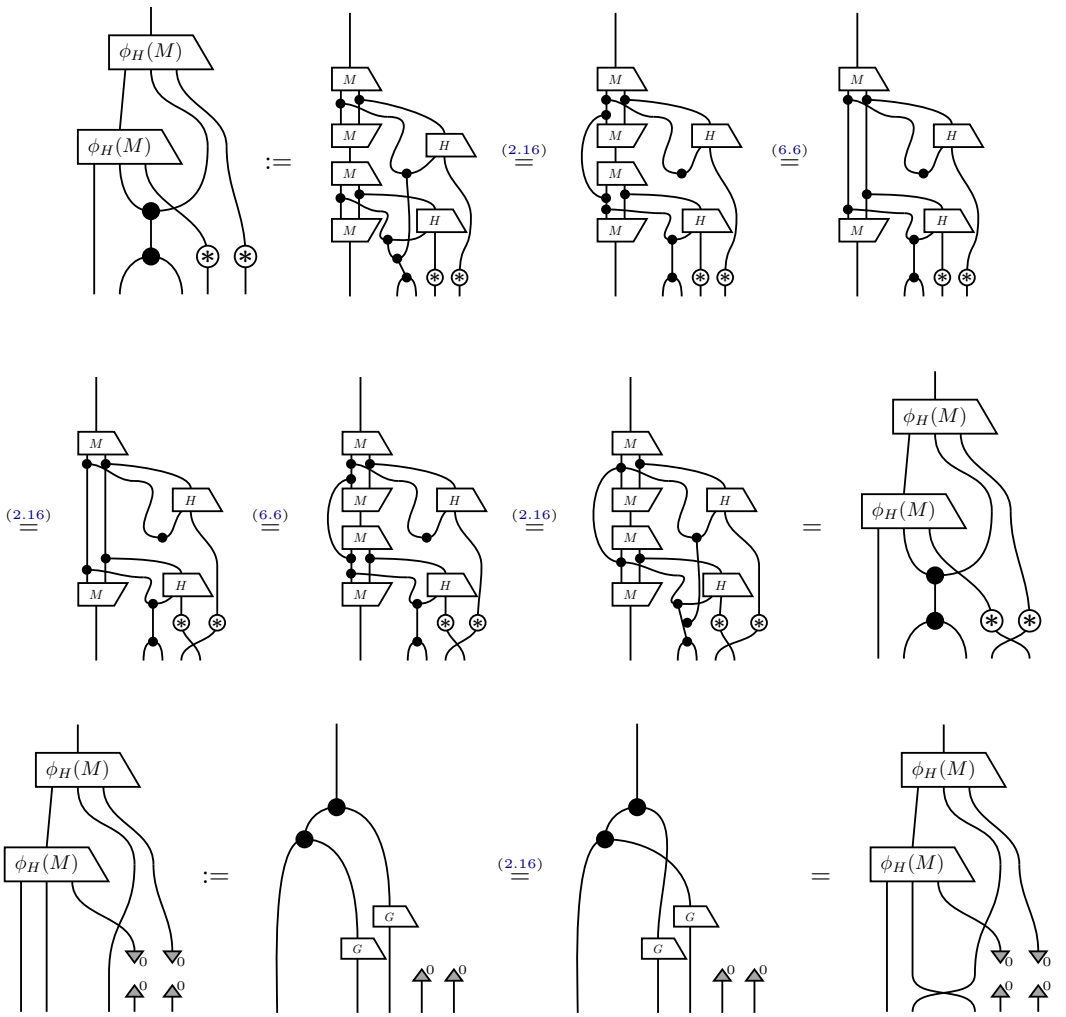


Now the right hand equation of (6.1.3):





We now show that equation (6.19) holds:



□

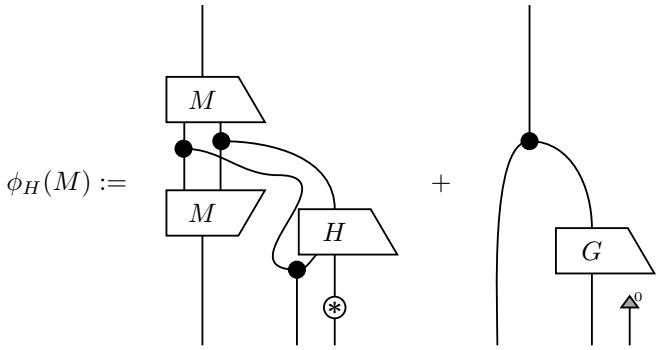
Let θ be the map that takes a partitioned UEB and gives the corresponding maximal family of MUBs

according to Theorem 6.5.1. We now investigate the map θ and the infinite family of maps ϕ_H each taking a maximal family of MUBs and giving a partitioned UEB, given by Theorem 6.5.2 above. Given a controlled Hadamard, H and a maximal family of MUBs we now consider the effect of the composition $\theta \circ \phi_H$ on the maximal family of MUBs:

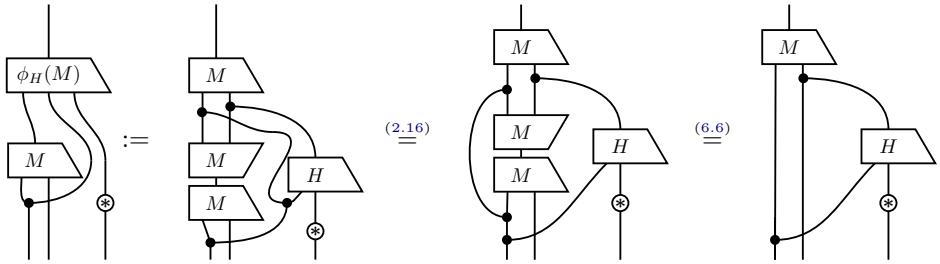
Theorem 6.5.3. *Given a maximal family of MUBs M and a controlled Hadamard H:*

$$\theta \circ \phi_H(M) = M. \tag{6.22}$$

Proof. By definition we have:



By design we have a partition $\{U_{00}\} \sqcup C_* \sqcup C_0 \sqcup ... \sqcup C_{d-1}$, where $C_* = \{U_{i0} | i \in \{1, ..., d-1\}\}$ and for $k \in [d], C_a = \{U_{aj} | j \in \{1, ..., d-1\}\}$. Clearly the eigenbasis of C_* is the black basis. Let $|b_k^i\rangle$ be the kth state of the ith basis of M. We claim that $|b_k^i\rangle$ is the kth eigenstate of C_i. To see this consider the following composite linear map.



If we input black states i, j, k with $k \neq 0$ the above equation becomes $[\phi_H(M)]_{ik} |b_j^i\rangle = [H^i]_{jk} |b_k^i\rangle$. Thus the bases of the original maximal family of MUBs are the eigenbases of $\phi_H(M)$ as required. □

Given that the composite map $\theta \circ \phi_H$ is the identity we conclude that θ is surjective and for all controlled Hadamards H, the map ϕ_H is injective. Given some maximal family of MUBs M and controlled Hadamard H, the proof to Theorem 6.5.3 allows us to identify the eigenvalues of the partitioned UEB $\phi_H(M)$ with the entries of the controlled Hadamard. This is precisely the information lost by the map θ. So every maximal family of MUBs corresponds to an infinite family of partitioned UEBs for

different choices of eigenvalues. These UEBs are in general inequivalent. Also, every partitioned UEB corresponds to a maximal family of MUBs with a particular choice of controlled Hadamard. This holds in any dimension, so the existence problem for maximal families of MUBs in arbitrary dimension can be phrased in terms of partitioned UEBs. Similarly for non-maximal families of MUBs we have corresponding UEBs with partial partition into maximally commuting sub-families.

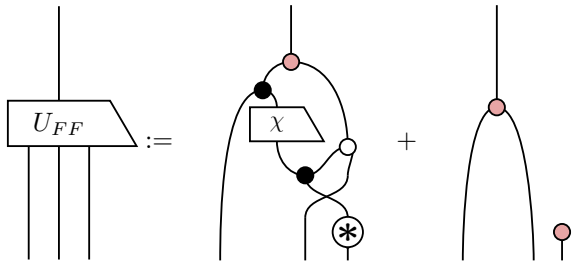
Chapter 7

A new construction

7.1 Introduction

In this chapter we use the machinery developed in Chapter 6 to present a construction of a partitioned UEB from a finite field. In order to achieve this we first introduce a diagrammatic characterization of finite fields, so that we can interpret finite fields as algebraic structures in Hilbert space. We take as our starting point the way the complex character theory of Abelian groups can be recovered using the graphical calculus as described in Section 2.2 of the background chapter. This gives us a diagrammatic representation of Abelian complex group algebras, and the usual complex character theory [GZ15, CDKW12]. We then build on this framework to discuss finite fields as algebraic structures defined over Hilbert spaces.

We use our characterization to prove that U_{FF} as defined below is a partitioned UEB and thus gives rise to a maximal family of MUBs.



(7.1)

Here  represents the computational basis as usual,  and  are the linear extension of the addition and multiplication respectively of the finite field and χ is the Fourier transform for the additive group. We end the chapter by giving an example of our construction in dimension $d = 4$.

Related work Gogioso and Zeng gave a diagrammatic characterization of complex group algebras in their 2015 paper [GZ15]. We have extended this to finite fields in this chapter.

7.2 Finite fields

We now define a finite field.

Definition 7.2.1 (Finite field [LN97])**.** A finite set A together with closed binary operators $\bullet$ and $\circ$ is a *finite field* if:

- **Addition**: The operator $\bullet$ is an Abelian group on the set A with unit $0 \in A$;
- **Multiplication**: The operator $\circ$ is an Abelian group on the subset $A' := A \backslash \{0\}$;
- **Distributivity**: For all $a, b, c \in A$, $a \circ (b \bullet c) = (a \bullet b) \circ (a \bullet c)$.

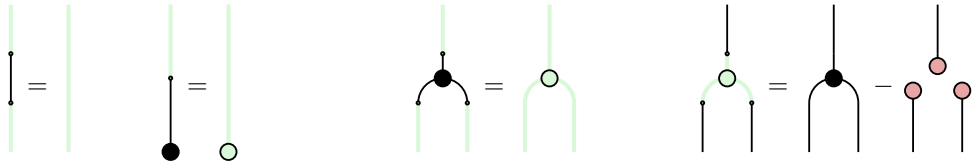
Finite fields only exist in prime power dimensions [LN97] so we take $d = p^n$ for some prime p and $n \in \mathbb{N}$, and as usual take the black wires to represent the Hilbert space $\mathcal{H} \cong \mathbb{C}^d$.

Addition. In formulating a diagrammatic notation for finite fields as algebraic structures defined over Hilbert spaces we start with an Abelian group algebra representing addition. We therefore take  and  to be a pair of strongly complementary †-commutative Frobenius bialgebras with black special, red quasi-special and red $\bullet$-real . As seen in Section 2.2  copies the additive characters which form the columns of a Fourier Hadamard matrix on $\mathcal{H}$ which we will again call χ with the formal definition given by equation (2.21).

Multiplication. The multiplication of a finite field also forms an Abelian group on the non-zero elements. We introduce another Hilbert space, $\mathcal{H}' \cong \mathbb{C}^{d-1}$ which we represent as green wires, and a †-SCFA . We also introduce linear maps to relate the green and black Hilbert spaces:

$p :=$ $\iota :=$ (7.2)

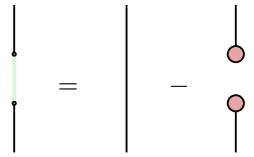
We require the following relationships between p, ι, ,  and :

 (7.3)

We will assume that the black basis has been ordered such that  := . This makes p and ι an isomorphism between $\mathcal{H}'$ and the $d-1$-dimensional subspace of $\mathcal{H}$ spanned by the non-zero black states. This isomorphism takes the green basis states to the non-zero black states. The Hilbert space $\mathcal{H}'$ is the analogue of the set A' in Definition 7.2.1.

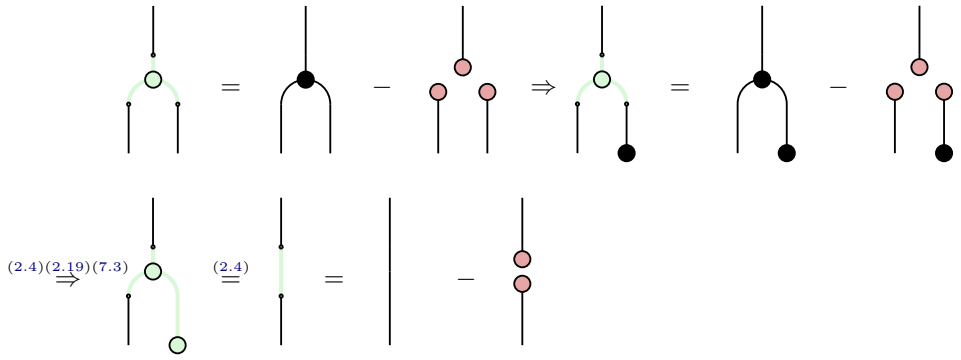
The following lemma shows that the linear map given by $\iota \circ p$ is equal to the projector defined by equation (6.16), we will make use of this projector.

Lemma 7.2.2. *The following equation holds.*



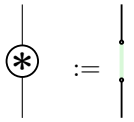
(7.4)

Proof. By the 4th equation of (7.3):

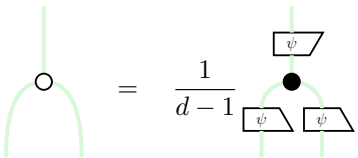


□

In light of this lemma we will again use $*$ to denote this projector.



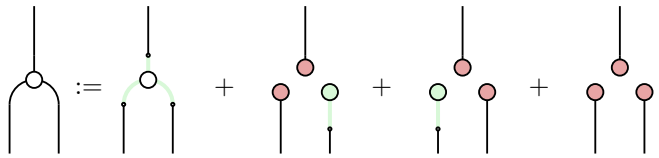
We now introduce the multiplication acting on the subspace $\mathcal{H}'$ which we represent as . We require that is a †-qSCFA, and that and are a strongly complementary bialgebra. Thus is an Abelian group on the green basis states. This also tells us that the white unit is a green basis state and thus isomorphic to a black basis state not equal to the red unit. We corrupt notation slightly to represent this state as . We denote the multiplicative character Fourier Hadamard matrix as ψ formally defined as follows:



(7.5)

We now introduce the multiplication on the whole Hilbert space $\mathcal{H}$, which we denote . We define

and as follows:

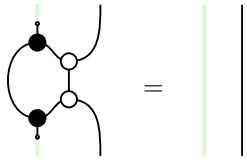


(7.6)



(7.7)

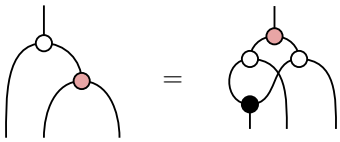
This ensures that agrees with on the subspace isomorphic to $\mathcal{H}'$. The linear map is associative, commutative and unital with unit , as can easily be proven from the axioms and the definition of . We also require that and form a bialgebra (this implies the requirement already made that and form a bialgebra). Although and are not strongly complementary, the following condition can easily be derived from the definitions:



(7.8)

Distributivity. Finally we relate and as follows:

Definition 7.2.3 (Left distributivity)**.** Let and each form a bialgebra with . White *left distributes over* red if the following equation holds:



(7.9)

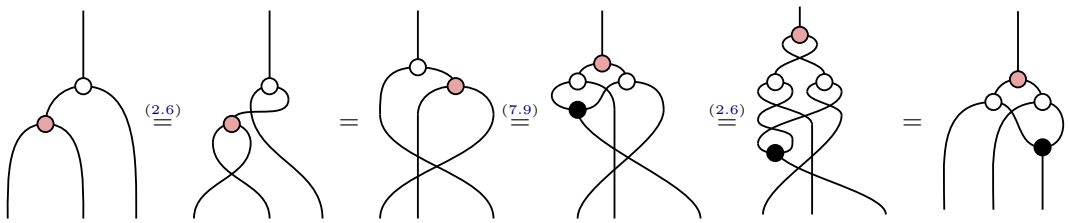
Right distributivity is defined by reflecting both sides of equation (7.9) in a vertical axis. We now show that right distributivity follows from left distributivity and commutativity.

Lemma 7.2.4. *If , and are commutative and white left distributes over red, then white right distributes over red; so the following equation holds:*



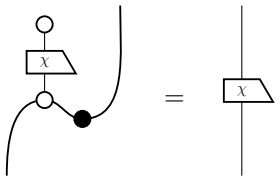
(7.10)

Proof.



□

Additive characters. We also require the following interaction between the white unit and χ:



(7.11)

This corresponds to the the following algebraic equation which can be recovered by composing by computational basis states: $\chi_a(b) = \chi_1(a \circ b)$.

Definition 7.2.5 (Complex finite field)**.** Given a d-dimensional Hilbert space represented by black wires and a $d-1$-dimensional Hilbert space represented by green wires, *a complex finite field* is a pair of †-SCFAs and , a pair of †-qSCFAs and as well as as defined by equation (7.7), linear maps χ and ψ defined by equations (2.21) and (7.5), linear maps p and ι defined by equation (7.2) and obeying equations (6.16) such that equations (7.9) and (7.11) hold. We denote a complex finite field (, , , , , , χ, ψ).

We summarize the results of this subsection in the following theorem.

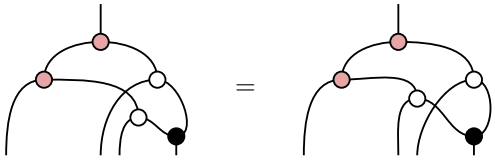
Theorem 7.2.6. *Given a complex finite field (, , , , , , χ, ψ), and are the linear extension of the addition and multiplication respectively of a finite field with the underlying set of elements given by the states copyable by . χ and ψ are the complex Fourier Hadamards for the additive and multiplicative group respectively.*

Proof. The binary operator forms an Abelian group on the states copyable by , which is the first axiom of Definition 7.2.1. . On the subspace of $\mathcal{H}$ isomorphic to $\mathcal{H}'$ which is spanned by the non-zero black states agrees with and thus forms an Abelian group, thus fulfilling the second axiom of Definition 7.2.1. Equation (7.9) is precisely the linear extension of distributivity, the third axiom of Definition 7.2.1. The properties of χ and ψ were proven by Gogioso and Zeng [GZ15]. □

7.2.1 A construction of $d+1$ MUBs

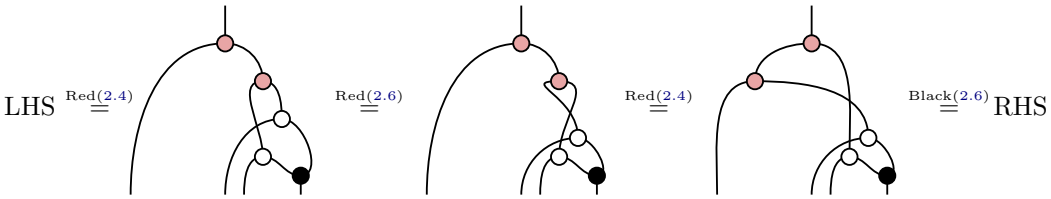
We now give an application of the complex finite fields developed in the previous subsection to the problem of constructing maximal families of MUBs. First we present two lemmas which will be necessary to proving the main result of this section.

Lemma 7.2.7. *Given a complex finite field* (, , , , , χ, ψ)*, the following equation holds:*



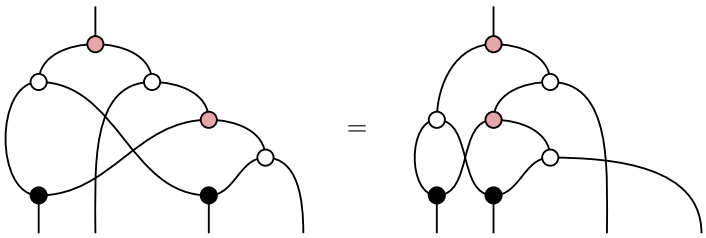
(7.12)

Proof.



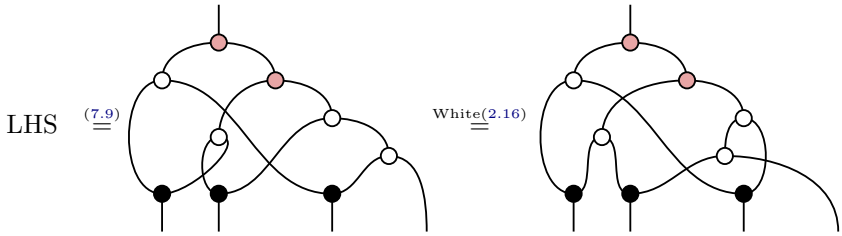
□

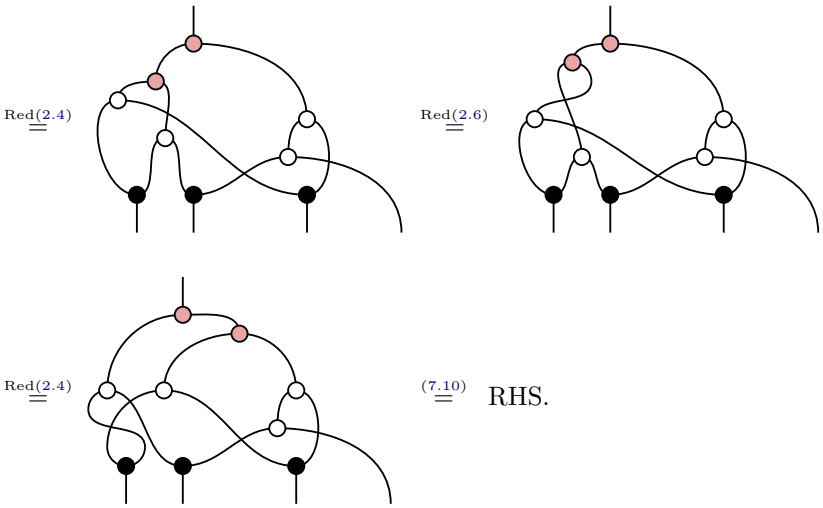
Lemma 7.2.8. *Given a complex finite field* (, , , , , χ, ψ)*, the following equation holds:*



(7.13)

Proof.

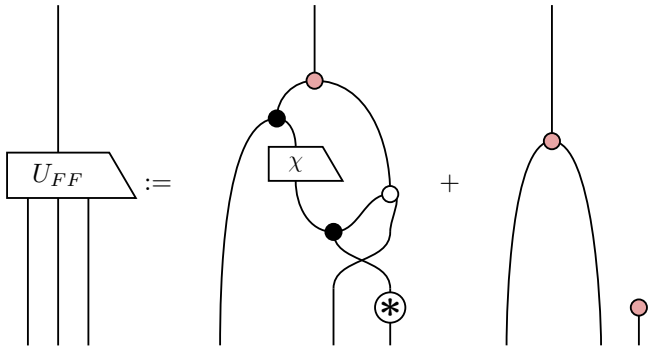




□

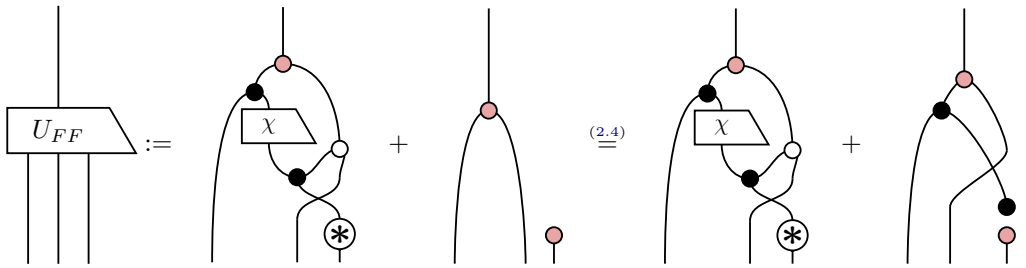
We construct a partitioned UEB as follows:

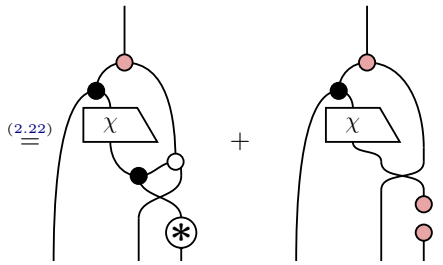
Theorem 7.2.9. *Given a complex finite field* ($\mathbb{F}$, $+$, $\cdot$, 0, 1, χ, ψ) *the following is a partitioned UEB:*



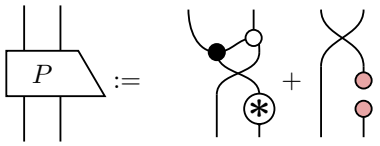
(7.14)

Proof. We first prove that U_{FF} is a UEB. We do this by showing that U_{FF} is equivalent to a *shift-and-multiply basis*. First we rearrange equation (7.14).

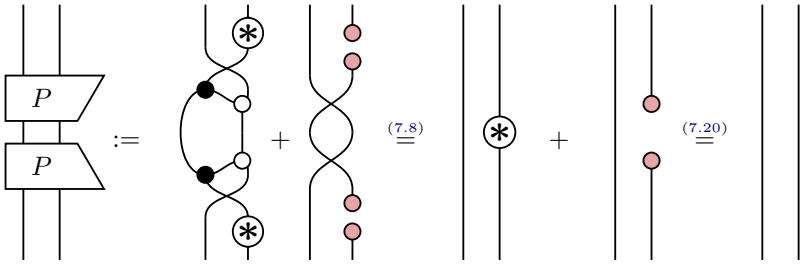




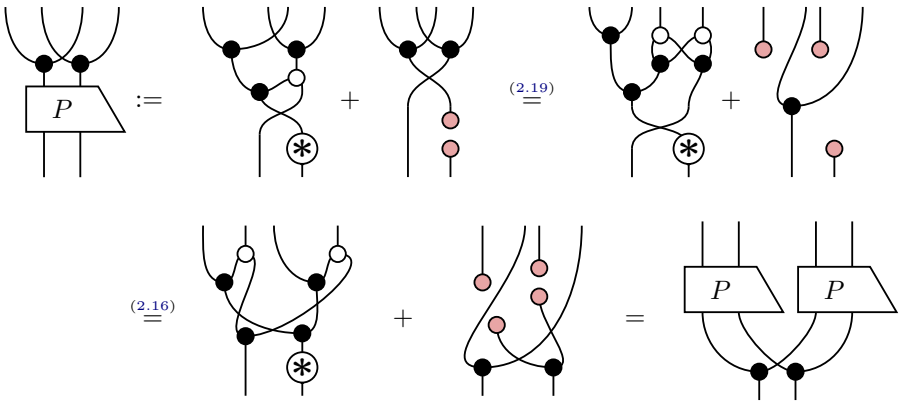
We now prove that the following linear map P, as defined below, is a permutation (see equations (6.9) and (6.10) in Chapter 6).



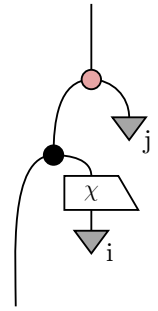
First we show that equation (6.9) holds for P.



Now we show that equation (6.10) holds for P.



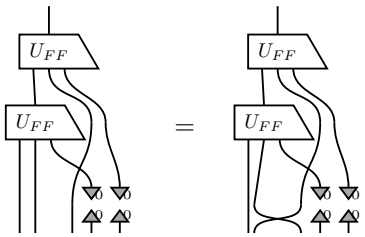
So P is a permutation and so U_{FF} is equal to $V_{P(i,j)}$, where V_{ij} is given by the following:

$V_{ij} :=$ 

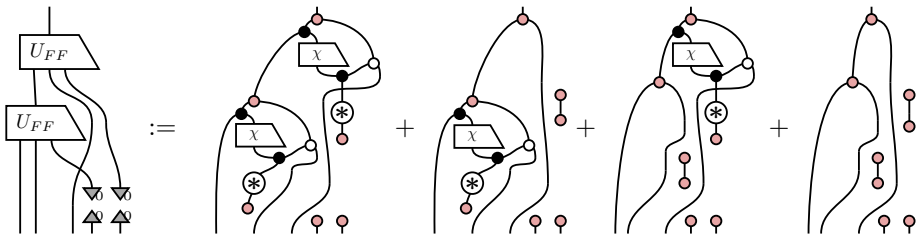
(7.15)

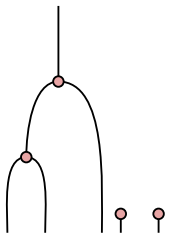
Since  is a finite Abelian group it is a finite quasigroup and thus a Latin square. χ is a Hadamard and so V is a shift and multiply basis, and therefore a UEB [Wer01, Mus14, MV15]. V and U_{FF} are equivalent by equation (6.4), and so U_{FF} is a UEB.

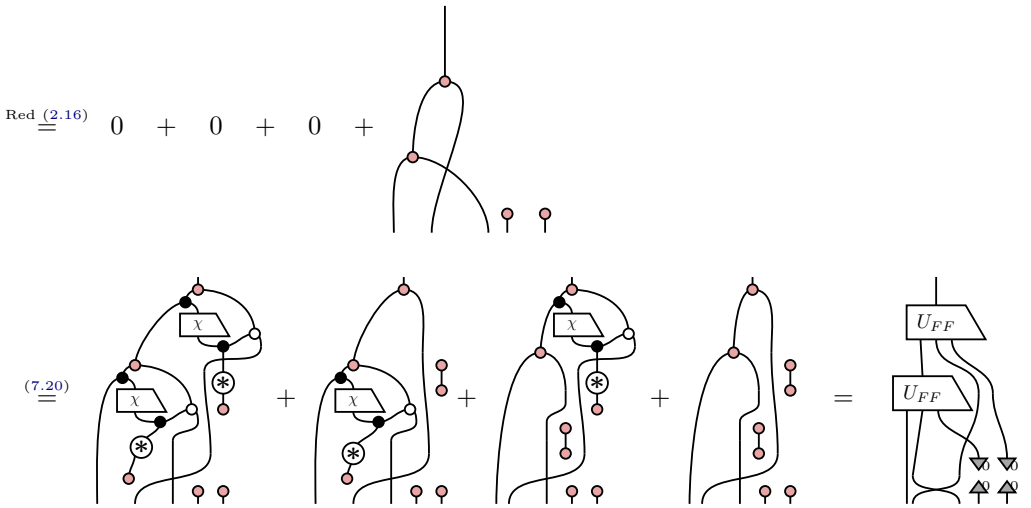
Commuting property. We now prove the following:



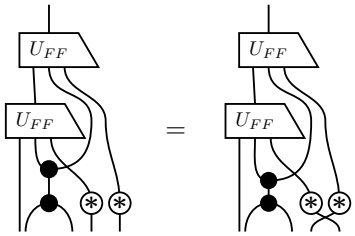
(7.16)



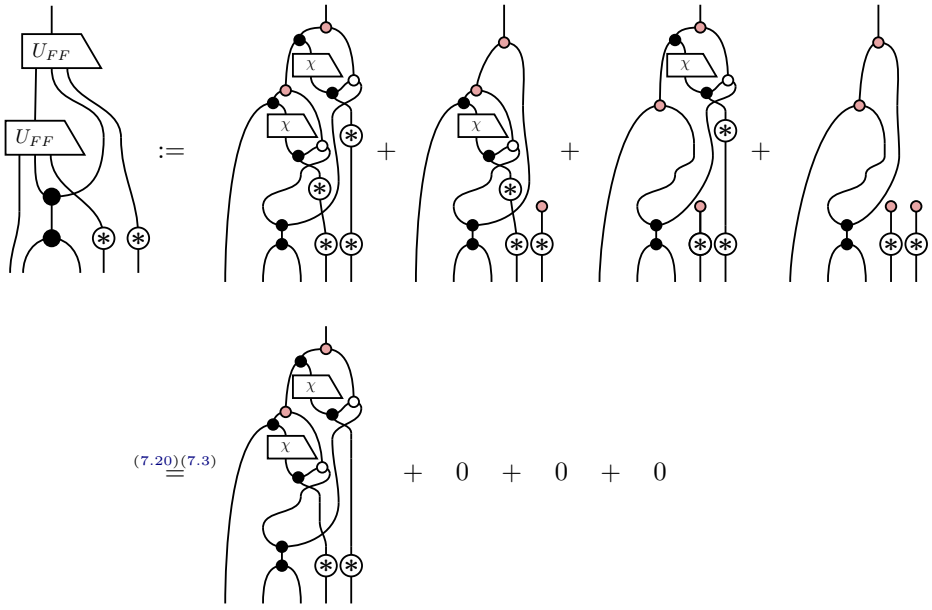
$\overset{(7.20)}{=} 0 + 0 + 0 +$ 



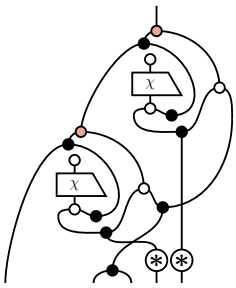
We now show that:



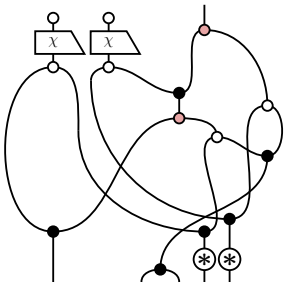
(7.17)



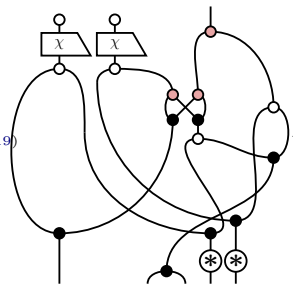
(7.11) =



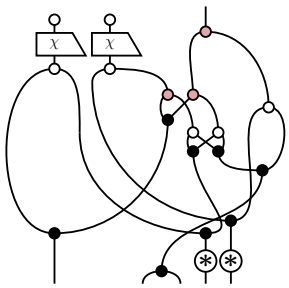
Black, white(2.16) =



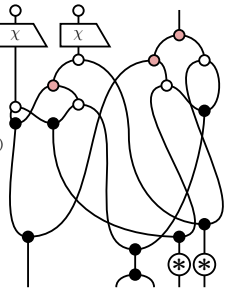
Red, black(2.19) =



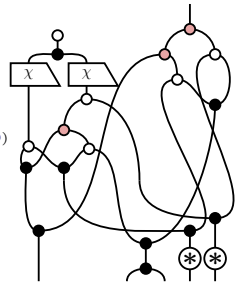
White, black(2.19) =



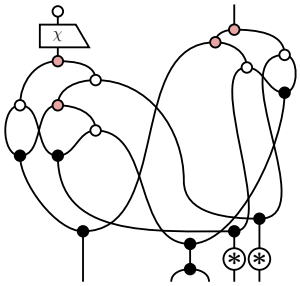
(2.16) =



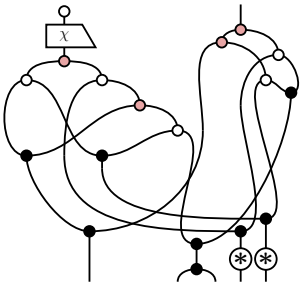
White, black(2.19) =



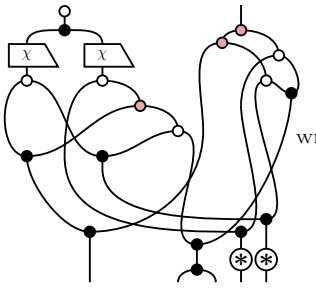
(2.22) =



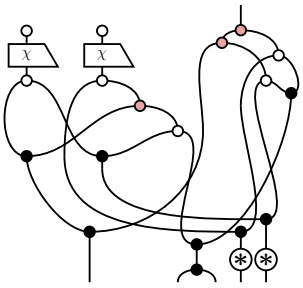
(7.12)(7.13) =

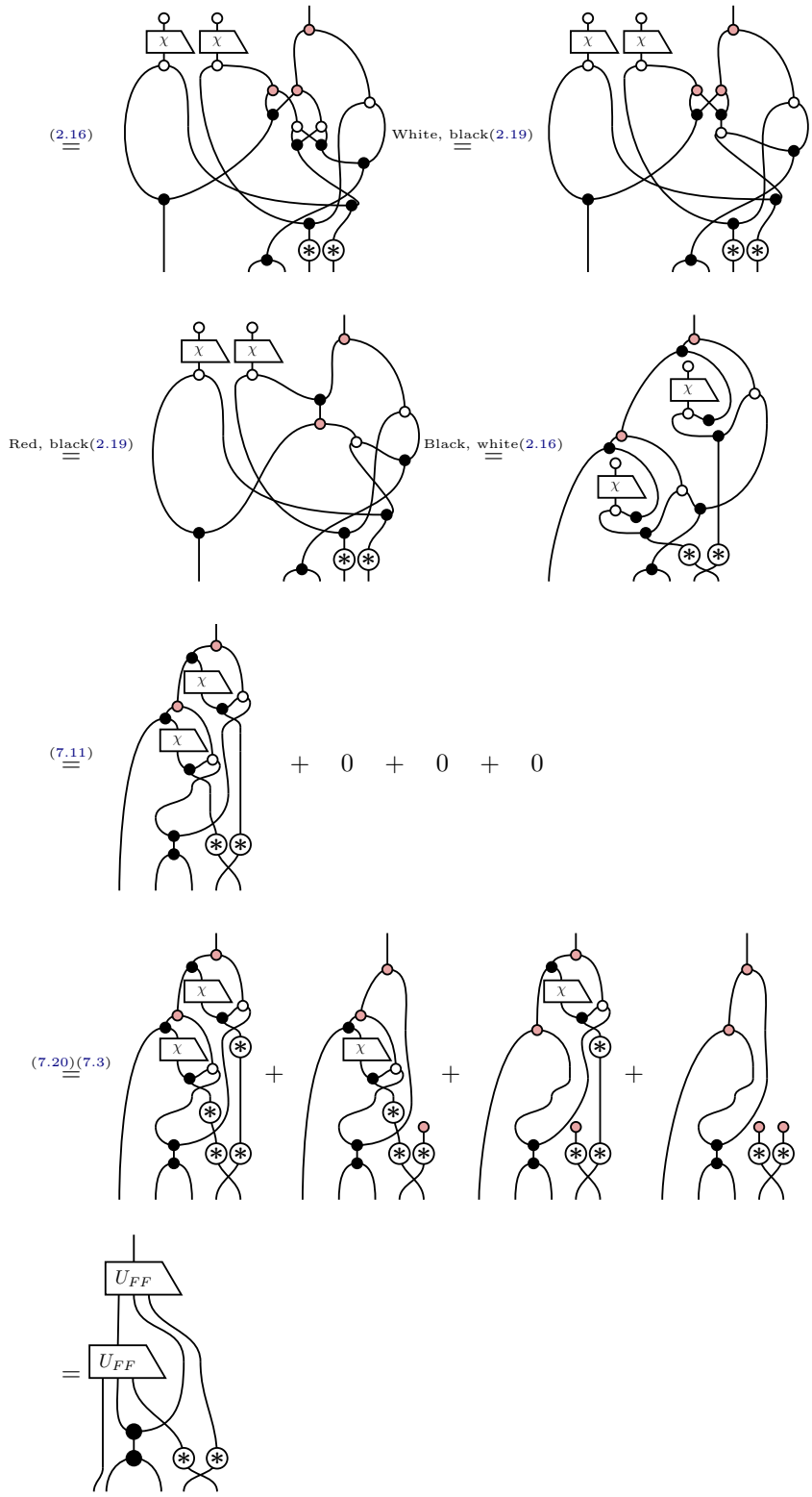


(2.22) =

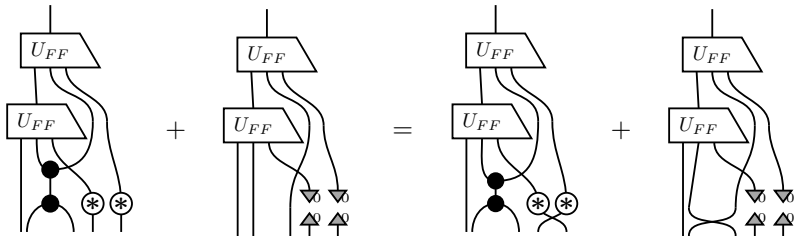


White, black(2.19) =





We can now combine equations (7.16) and (7.17) to obtain the following:

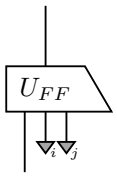


This concludes the proof. □

We now present an example of a partitioned UEB in dimension $d = 4$ constructed from the finite field $\mathbb{F}_4$.

Example 7.2.10. The Fourier transform for the additive group of $\mathbb{F}_4$ is given by the following Hadamard matrix.

$$\chi := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

Let $\mathcal{M}_{ij} :=$ 

with U_{FF} as defined in equation (7.14), then the partitioned UEB, with partitions $C_x, x \in \{*, 0, ..., 3\}$, is as follows:

$$\mathcal{M}_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{M}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \mathcal{M}_{02} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{M}_{03} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\mathcal{M}_{10} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \mathcal{M}_{11} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \mathcal{M}_{12} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{M}_{13} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{20} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \mathcal{M}_{21} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \mathcal{M}_{22} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{M}_{23} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathcal{M}_{30} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{M}_{31} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{M}_{32} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \mathcal{M}_{33} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

The partitions are:

$$C_* := \{\mathcal{M}_{10}, \mathcal{M}_{20}, \mathcal{M}_{30}\},$$

$$C_0 := \{\mathcal{M}_{01}, \mathcal{M}_{02}, \mathcal{M}_{03}\},$$
$$C_1 := \{\mathcal{M}_{11}, \mathcal{M}_{12}, \mathcal{M}_{13}\},$$
$$C_2 := \{\mathcal{M}_{21}, \mathcal{M}_{22}, \mathcal{M}_{23}\},$$
$$C_3 := \{\mathcal{M}_{31}, \mathcal{M}_{32}, \mathcal{M}_{33}\}.$$

Thus since $\mathcal{M}_{00} = \mathbb{I}_4$, we have:

$$U_{FF} = \{\mathbb{I}_4\} \sqcup C_* \sqcup C_0 \sqcup C_1 \sqcup C_2 \sqcup C_3.$$

It can easily be verified that this is a partition into maximal commuting sub-families and that U_{FF} is a UEB.

7.3 Conclusion

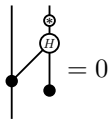
In Part II we have introduced a diagrammatic characterization of maximal families of MUBs, partitioned unitary error bases, Hadamards and controlled Hadamards. As an application of these diagrammatic characterizations we have introduced a new construction for a partitioned UEB from a maximal family of MUBs extending work by Bandyopadhyay [BBRV02], which makes clear the exact nature of the correspondence between partitioned UEBs and maximal families of MUBs. Each partitioned UEB gives rise to a unique maximal family of MUBs. Each maximal family of MUBs gives rise to an infinite family of possibly inequivalent partitioned UEBs, with each partitioned UEB corresponding to a choice of controlled Hadamard. Further work is required to investigate whether the property of monomiality of UEBs introduced by Wocjan et al [BSTW05], is invariant under the choice of controlled Hadamard in our construction and therefore a well defined notion.

We have also introduced a diagrammatic characterization of finite fields as algebraic structures defined over Hilbert spaces, extending existing characterizations of Abelian groups [GZ15]. As an application of this and a further application of the diagrammatic characterizations of partitioned UEBs we introduced a new construction of partitioned UEBs and thus maximal families of MUBs from a finite field. This is different from the construction due to Bandyopadhyay et al [BBRV02], with the partition being easier to calculate. Further work is necessary to investigate whether this construction could be adapted to one requiring less structure than that of a finite field.

7.4 Minor lemmas

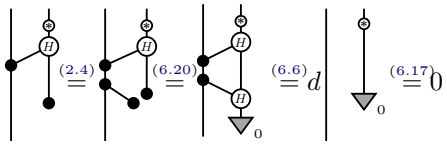
In this section we present a number of minor diagrammatic lemmas that are essential to the proofs of the main theorems. We assume throughout that all wires are d-dimensional Hilbert spaces and the operators are as defined in the main body of the chapter.

Lemma 7.4.1. *Given a controlled Hadamard H and †-SCFA* *, the following equation holds.*



(7.18)

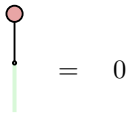
Proof. We take the LHS of equation (7.18):



(7.19)

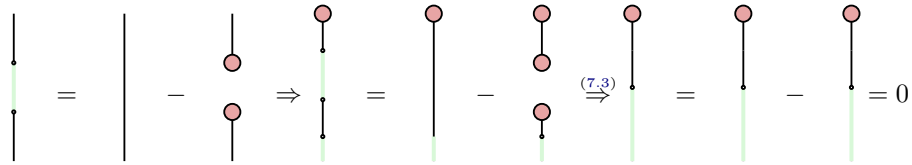
□

Lemma 7.4.2. *The following equation holds.*



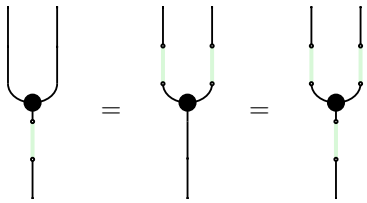
(7.20)

Proof. By Lemma 7.2.2:



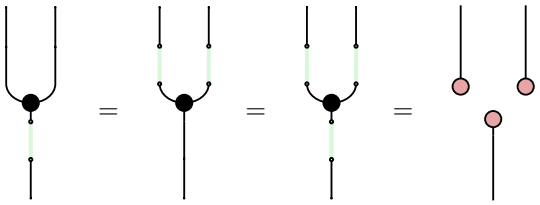
□

Lemma 7.4.3. *The following equation holds.*



(7.21)

Proof. By Lemma 7.2.2 and Definition 2.2.2:



□

Part III

Quantum functions

Chapter 8

Quantum functions

Quantum functions are a non-commutative generalization of functions. *Quantum sets* are a non-commutative generalization of sets. Quantum functions exist between quantum sets but they also exist between sets. Quantum functions between sets have a concrete operational interpretation which offers some intuition on the abstractly derived mathematical objects of this chapter for the general reader. As will be shown in Section 8.3.1, quantum functions between sets X and Y can be thought of as families of projective measurements having outcomes in Y and being controlled on X. In this way we can see quantum functions between sets as non-deterministic functions which, given an input from X obtain an output in Y probabilistically via a projective measurement on some underlying Hilbert space.

A central theme of this thesis has been to generalize Abelian complex group algebras by viewing them as the interaction of a †-SCFA and a †-qSCFA. We have gradually taken away structure from the †-qSCFA which we see as a *generalized multiplication algebra* revealing various structures. We have Latin squares, which are still algebraic structures although not algebras. Generalizing further we have quantum Latin squares (see Chapter 3) which cannot be seen as closed algebraic structures at all but still, in some way give rise to a form of generalized multiplication and comultiplication. Next we introduced quantum isometry Latin squares, which no longer resemble multiplication but can still be seen as a grid of linear maps. Up until now we have not taken any structure away from the †-SCFA that via finite-dimensional Gelfand duality we have identified with an indexing set of elements. In this chapter we will see the affect of replacing the underlying †-SCFA or set with a general †-SSFA or *quantum set*.

8.1 Introduction

In this chapter we introduce *quantum sets*, *quantum functions*, *quantum elements* and *quantum bijections*. We show that these objects naturally fit into a 2-categorical structure, **QSet**. We also introduce *quantum graphs*, *quantum homomorphisms* and *quantum isomorphisms*, and an analogous 2-categorical structure,

QGraph. Finally we generalize to *quantum relations* of quantum sets.

We show that our approach to quantization coincides with various notions of quantum morphisms which have recently been studied in the areas of noncommutative topology, zero error quantum communication and quantum metric spaces [AMR+19, Wan98, DSW13, Wea10]. We thereby introduce a unified framework within which these structures may be explored further.

8.1.1 Quantization

In this chapter and the next we show that various notions of quantization, despite being formulated very differently are instances of the same technique in different contexts and can be captured within a single categorical framework. Since the early days of quantum mechanics, going from the classical world to the quantum world has been associated with a move from commutative to non-commutative variables. In line with the work of Wang, Bichon, Banica and others on quantum compact groups we regard C^*-algebras as quantum generalizations of topological spaces and thus finite-dimensional C^*-algebras as quantized finite sets. Under Gelfand duality and the categorical view of finite-dimensional C^*-algebras [Vic10] (see Background Section 2.1.3), this will manifest itself in passing from †-SCFAs which correspond to finite sets to general †-SSFA which we take as *quantum sets*.

Another approach to quantization is that used in non-local games. The basic idea is to define a non-local game such that a perfect strategy corresponds to a particular mathematical object such as a graph homomorphism. Then, by allowing the players access to quantum resources, a quantum graph homomorphism can be defined as a *perfect quantum strategy*. Quantum analogues of both graph homomorphisms and graph isomorphisms have been introduced in this way [AMR+19, MR16]. In Chapter 9 we will show that these structures are precisely the restriction of our quantum homomorphisms and quantum isomorphisms to classical graphs.

The quantization of functions and bijections in this chapter leads back to some of the mathematical objects introduced earlier in this thesis. We will see that QILS, when *projected out* (see below for a precise definition) are precisely quantum bijections between classical sets. Continuing the scheme of generalization that started with Abelian complex group algebras, went through Latin squares, quantum Latin squares and quantum isometry Latin squares, we will also see quantum bijections between quantum sets. This is a move away from the grids of operators seen previously with the indexing set being replaced by a quantum set.

Remark 12. *Consider the generalization from a Latin square to a quantum Latin square. For each there are two input wires upon which a †-SCFA is defined and this is the underlying set of grid coordinates. For Latin squares, from equations* (3.3) *and* (3.4) *we see that the output wire also carries the same †-SCFA. The output wire of a quantum Latin square is of the same dimension as the †-SCFA carrying input wires (unlike the output wire for a QILS). Up until now we have not made a distinction between*

these Hilbert spaces and they are of course isomorphic. However, as can be seen from equations (3.6) it is not necessary for the output Hilbert space to carry a †-SCFA. This is what allows the output to be a quantum superposition of the computational basis states of the input set. This justifies the name 'quantum' Latin square.

8.1.2 Notation

In this chapter we introduce various quantum analogues of combinatorial structures. In order to disambiguate we will often refer to ordinary sets, functions, graphs and so on as *classical*. We will also be using the correspondence induced by finite-dimensional Gelfand duality to pass between finite sets and †-SCFAs and associated Hilbert space freely and will often denote both by the same capital Roman letter. This notational freedom also extends to the quantum set and Hilbert space associated to a particular †-SSFA. So for example X may stand for a finite quantum set, equivalently a †-SSFA or the induced Hilbert space. In practice this will not cause ambiguity in context.

8.1.3 Related work

Quantum permutation groups and quantum automorphisms of a graph. In noncommutative topology, an active area of research surrounds quantized analogues of the permutation groups S_n known as quantum permutation groups, and quantum analogues of the automorphism groups of finite graphs. Quantum permutation groups were developed by Wang, Bichon and Banica as well as others [Wan98, Ban05, BBC07b, BB07, Bic03, BB09, BBC07a]. Both quantum permutation groups and quantum automorphism groups correspond to infinite-dimensional Hopf C^*-algebras denoted $A_{aut}(n)$ and $A_{aut}(G)$ respectively for $n \in \mathbb{N}$ and G a finite graph. In this chapter we show that our category $\mathbf{QBij}([n],[n])$, the category of quantum bijections from an n element set to itself, corresponds to the finite-dimensional representations of the Hopf C^*-algebra $A_{aut}(n)$. Similarly, given a finite graph G, the finite-dimensional representations of the Hopf C^*-algebra $A_{aut}(G)$ are given by our category $\mathbf{QIso}(G,G)$.

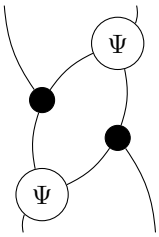
Quantum information theory. In a recent paper by Abramsky et al [ABdSZ17] a categorical approach to quantum graph homomorphisms was taken. There are similarities to that approach and ours, and in particular their Kleisli category corresponds to composition of 1-morphisms in **QSet**. This work brings to light connections between quantum functions and contextuality in quantum mechanics.

In Section 8.5 we generalize our quantum graphs to quantum relations. We show that this notion coincides with the quantum relations of Weaver and Kuperberg [KW12, Wea15]. This also allows us to see that our quantum graphs generalize the non-commutative graphs of Duan, Severini and Winter [DSW13], which are used for zero error quantum communication. In Chapter 9 we discuss in more detail connections to non-local games and quantum pseudo telepathy and prove that the quantum graph homomorphisms

and isomorphisms of Mančinska, Roberson and others [MR16, AMR+19] are specific instances of our 2 category **QGraph**.

8.1.4 Splitting and projecting

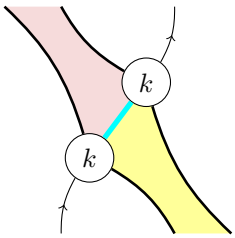
As mentioned above, QILS and QLS appear in this chapter in their *projected out* form. This is the composition of a QILS or a QLS with its adjoint. We have already encountered this in the case of QLS. Given a QLS Ψ, we refer to the following as a projective QLS (see Definition 5.3.1):



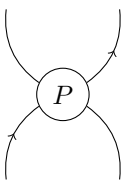
Note that for a QLS with entries $|\Psi_{ij}\rangle$, the associated projective QLS is a grid of operators $|\Psi_{ij}\rangle\langle\Psi_{ij}|$. Recall that an orthogonal projector p on a Hilbert space is a linear map that is idempotent and self-adjoint so $p^2 = p$ and $p = p^\dagger$. It comes from the definition of a QLS that a projective QLS is a grid of one-dimensional orthogonal projectors which form a projective measurement on each row and column.

Similarly we can project out a QILS. We do this by forming a skew PPM (see Definition 5.4.4, equation (5.23)) from two copies of the same QILS.

Definition 8.1.1. Given a quantum isometry Latin square k, a *projective permutation matrix* (or *projected out QILS*) is given by the following:



From now on we represent projective permutation matrices (PPMs) as the following node with the †-SCFA defined on the unoriented wire being represented as a black dot:



(8.1)

We refer to the oriented wire as the *underlying Hilbert space* and say that the dimension of a PPM is the dimension of its underlying Hilbert space.

Proposition 8.1.2. *An n-by-n PPM is precisely a grid of projectors P_{ij} with $i, j \in [n]$ such that the following hold:*

$$P_{jk}P_{ik} = \delta_{ij}P_{ik}, \qquad \sum_n P_{nj} = \mathbb{I}, \tag{8.2}$$

$$P_{ik}P_{ij} = \delta_{jk}P_{ij}, \qquad \sum_m P_{im} = \mathbb{I}. \tag{8.3}$$

Proof. Each isometry k_{ij} gives rise to a projector $P_{ij} := k_{ij}k_{ij}^\dagger$. From equation (5.18) we have:

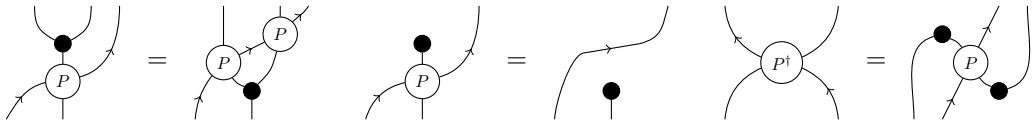
$$\begin{aligned} k_{ik}^\dagger k_{ij} &= \delta_{jk}\mathbb{I}_{a_{ij}} \\ \Leftrightarrow k_{ik}k_{ik}^\dagger k_{ij}k_{ij}^\dagger &= \delta_{jk}k_{ik}k_{ij}^\dagger \\ \Leftrightarrow P_{ik}P_{ij} &= \delta_{jk}P_{ij}. \end{aligned}$$

The other equations follow similarly from equations (5.19) and (5.20). □

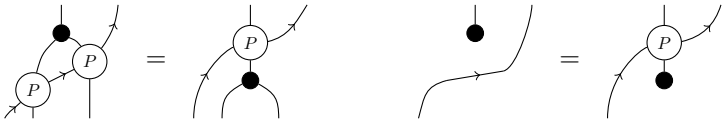
So for a PPM the projectors form projective measurements on the rows and columns like projective QLS, although now the projectors are not necessarily one-dimensional.

We now formulate the properties of PPMs graphically:

Lemma 8.1.3. *Given a 4-valent tensor P with type as shown in diagram 8.1, P is a PPM if and only if the following equations hold:*



(8.4)



(8.5)

Proof. These graphical equations can be translated algebraically as follows, for all $i, j, k \in [n]$:

$$\delta_{ij}P_{ik} = P_{jk}P_{ik}, \qquad \sum_n P_{nj} = \mathbb{I}, \qquad P_{ij}^\dagger = P_{ij}, \tag{8.6}$$

$$P_{ik}P_{ij} = \delta_{jk}P_{ij}, \qquad \mathbb{I} = \sum_m P_{im}. \tag{8.7}$$

□

We can also move in the opposite direction. Given a node as in diagram (8.1), such that equations (8.4) and (8.5) hold, we can split the idempotents on the underlying Hilbert space to recover the QILS k. This splitting is uniquely determined up to isomorphism [Sel08]. We therefore consider QILS and PPMs (or

QLS and projective QLS) to be essentially the same mathematical objects. For the rest of this chapter it will usually be the projected out objects that we consider.

We will see later that PPMs correspond to quantum bijections between finite classical sets and in Chapter 9 we will see that they are also quantum isomorphisms between finite classical graphs.

8.2 Quantum sets, functions and bijections

In this section we introduce quantum analogues of sets, functions, elements and bijections. First we introduce quantum functions and quantum elements. We will see that quantum elements are naturally collected into categories from which data, quantum sets can be reconstructed. We then introduce quantum bijections between quantum sets.

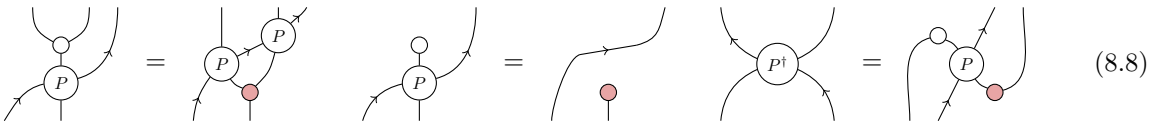
We begin by defining *finite quantum sets* as non-commutative finite sets. Recall that by finite-dimensional Gelfand duality a finite set is associated to a finite-dimensional commutative C^*-algebra (see Section 2.1.3, Theorem 2.1.12). Recall also that finite-dimensional C^*-algebras correspond to †-SSFAs and finite dimensional commutative C^*-algebras correspond to †-SCFAs (See Section 2.1.2, Theorem 2.1.4).

Definition 8.2.1. A *finite quantum set* is a finite-dimensional C^*-algebra or, equivalently a dagger special symmetric Frobenius algebra.

8.2.1 Quantum functions

We are now ready to introduce quantum functions.

Definition 8.2.2 (Quantum function)**.** A *quantum function* between quantum sets A and B is a pair $(H, P) : A \to B$ where H is a Hilbert space and P is a linear map $P : H \otimes A \to B \otimes H$ such that the following equations hold:



(8.8)

Here A is represented by red and B is represented by white.

Recall that functions between finite classical sets correspond to $*$-cohomomorphisms of †-SCFAs (See Definition 2.1.7). In order to quantize equations (2.1.7) we have added an additional Hilbert space H. We refer to H as the *underlying Hilbert space* and we will see that this is precisely the underlying Hilbert space introduced in Section 8.1.4 in the context of PPMs. Graphically this gives us an elegant way to denote quantization of morphisms. We draw the underlying Hilbert space as an oriented wire, this

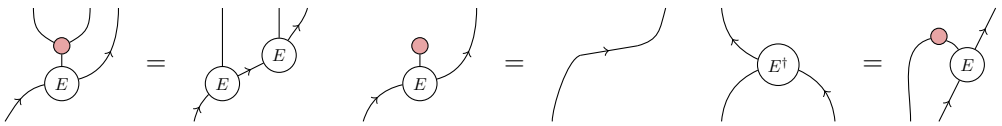
disambiguates from the unoriented wires representing the Hilbert spaces A and B on which the algebras are defined.

Remark 13. *We observe that the graphical representation of quantum functions leads to an interesting topological perspective: a quantum function behaves like a braiding or crossing between the directed and the undirected wire; equation* (8.8) *allows us to pull the comultiplication and counit through the directed wire. Note that we cannot yet pull the multiplication and unit through the directed wire; this must wait for the quantum bijections of Section 8.2.2.*

An element of a classical set A is a function from the one-element set $\{*\}$ to A, or equivalently a $*$-homomorphism from $\mathbb{C}$ to A. We define a quantum element analogously.

Definition 8.2.3 (Quantum element)**.** A quantum element of a finite quantum set A is a quantum function (H, E) from $\mathbb{C}$ to A.

Explicitly, given a quantum element (H, E) of finite quantum set A the following equations hold:



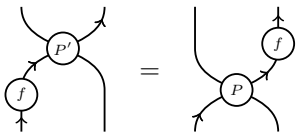
(8.9)

Definition 8.2.4. The *dimension* of a quantum function (H, P) is the dimension of the underlying Hilbert space H.

Note that equations (8.9) give a quantum element the structure of a left comodule (or left co-representation) of the algebra A. By comparing equations (8.8) and (2.11) we see that a one-dimensional quantum function is a cohomomorphism of Frobenius algebras. Thus, via Gelfand duality, a one-dimensional quantum function between classical finite sets is a function. Similarly a one-dimensional quantum element of a classical set is an element.

The introduction of an extra wire leads us to consider linear maps on this Hilbert space that interact with our quantum functions. We therefore give the following definition.

Definition 8.2.5 (Intertwiners of quantum functions)**.** An *intertwiner* of quantum functions $(H, P) \to (H', P')$ is a linear map $f : H \to H'$ such that the following equation holds:



(8.10)

Whilst the functions from one classical set to another form a set, the quantum functions from one finite quantum set to another are more naturally arranged into a category to keep track of the intertwiners.

Definition 8.2.6. Given a pair of quantum sets A and B, the category $\mathbf{QFunc}_{A,B}$ of quantum functions from A to B is defined as follows:

- **objects** - quantum functions $(H, P) : A \to B$;
- **morphisms** - intertwiners of quantum functions.

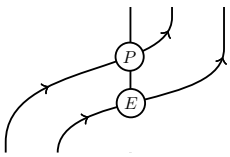
A forgetful functor $F : \mathbf{QFunc}_{A,B} \to \mathbf{FHilb}$ can be defined, which takes quantum functions to their underlying hilbert spaces and intertwiners to their underlying linear maps.

A classical set is uniquely determined by its elements. Consider the category of quantum elements of a quantum set A given by $\mathbf{QFunc}_{\mathbb{C},A}$. We now show that A can be reconstructed from $\mathbf{QFunc}_{\mathbb{C},A}$ together with the forgetful functor F.

Proposition 8.2.7. *Up to isomorphism, a quantum set A can be reconstructed from its category of elements $\mathbf{QFunc}_{\mathbb{C},A}$ and the forgetful functor $F : \mathbf{QFunc}_{\mathbb{C},A} \to \mathbf{FHilb}$.*

Proof. By definition, $\mathbf{QFunc}_{\mathbb{C},A}$ is the category of left comodules of the special symmetric dagger Frobenius algebra A. This is equivalent to the category of modules of A. The proposition therefore follows from existing results on Tannaka duality, which state that a semisimple algebra can be reconstructed from its category of modules and a forgetful functor [JS91]. □

We note that a quantum function from A to B takes a quantum element of A to a quantum element of B.

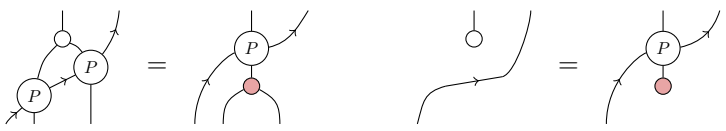


In particular, a quantum function between two quantum sets A and B induces a functor between their categories of quantum elements.

8.2.2 Quantum bijections

We now quantise bijective functions. As explained in Section 2.1.2 bijections between finite sets correspond to isomorphisms between †-SCFAs. We now quantize isomorphisms.

Definition 8.2.8. Given quantum sets A and B, a quantum function $(H, P) : A \to B$ is a *quantum bijection* if the following equations hold:



(8.11)

Again A is represented by red and B is represented by white.

In the next section we will see that quantum bijections between finite classical sets are PPMs. First we give an example of quantum bijections between quantum sets. Unitary error bases on n-dimensional Hilbert spaces give rise to quantum bijections from the matrix algebra $\mathbb{M}_n$ to the set $[n^2]$. Recall that a UEB can be characterised as follows (see Chapter 6, Proposition 6.4.2):

Definition 8.2.9 (UEB)**.** Given an n-dimensional Hilbert space H and a finite set (or †-SCFA), X of cardinality n^2, the following linear map $U : H \otimes X \to H$ is a unitary error basis on H if the following linear maps are unitary:

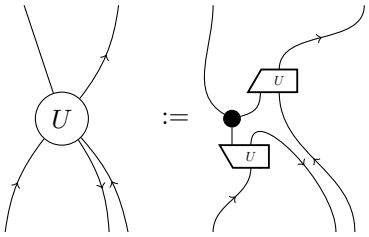


(8.12)

X is represented as black and H is an oriented wire.

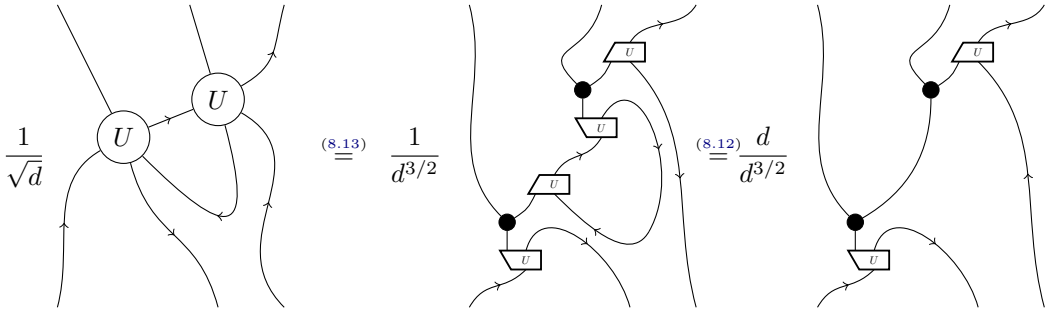
Note that we have varied from our usual convention of drawing unitary error bases as a wedge pointing to the right with the indexing leg on the right. This is purely a notational choice which will make the diagrams that follow easier to read.

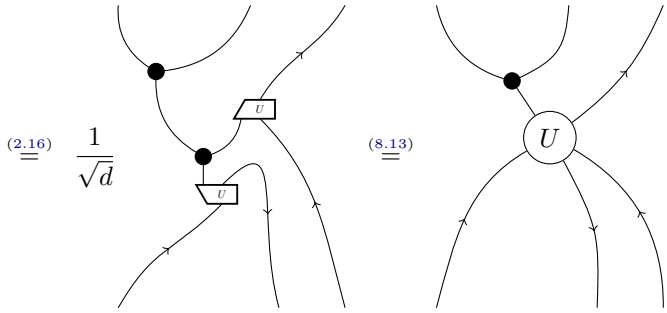
Proposition 8.2.10. *Given a unitary error basis U on an n-dimensional Hilbert space H, U defines a quantum bijection $(H, U) : \mathbb{M}_n \to [n^2]$ as follows:*



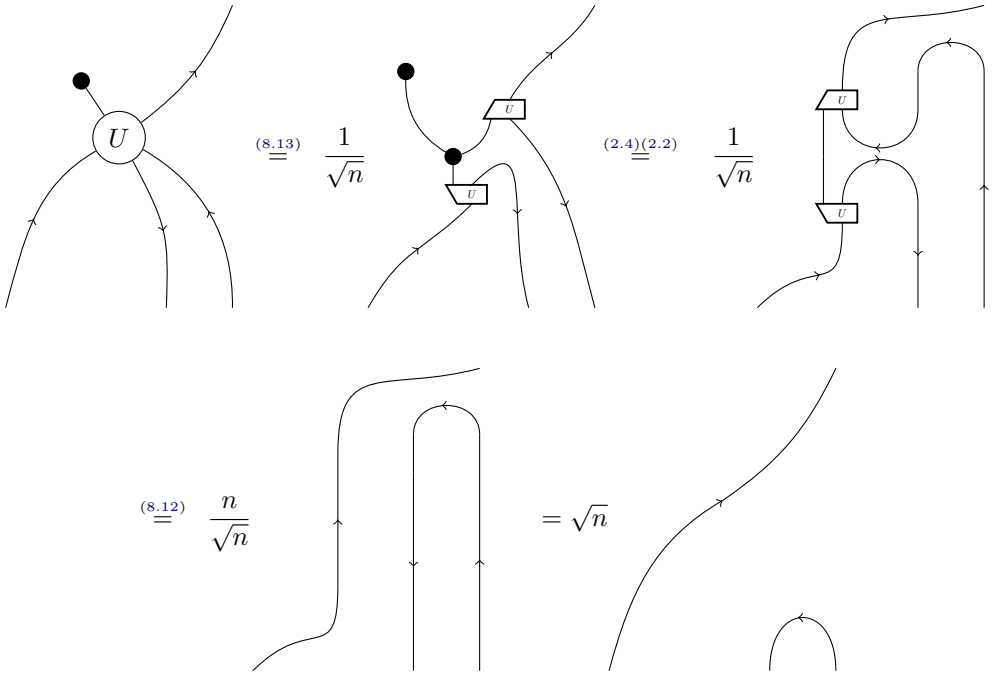
(8.13)

Proof. For a graphical description of the matrix algebra $\mathbb{M}_n$ see Example 2.1.5. We need to show that equations (8.4) and (8.5) hold for U as defined above. The first equation follows:





Now for the second equation:



The other equations can be shown similarly. □

8.2.3 The 2-category QSet

While classical functions $f : A \to B$ form a set, we have seen that quantum functions $(P, H) : A \to B$ should be organized into a *category*, keeping track of the additional layer of structure introduced by the intertwiners. Therefore, we expect the quantum analogue of the category of sets and functions to be a *2-category* of quantum sets and quantum functions, again keeping track of the intertwiners between quantum functions.

As a general trend, we observe that our version of quantization naturally leads to categorification.

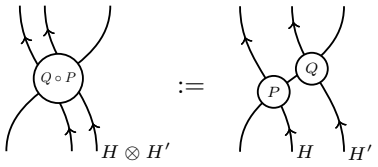
Definition 8.2.11. The 2-category* **QSet** is defined as follows:

- **objects** are quantum sets A, B, ...;
- **morphisms** $A \to B$ are quantum functions $(H, P) : A \to B$;

*Strict 2-category if we use a strict version of **FHilb**.

- **2-morphisms** $(H, P) \to (H', P')$ are intertwiners of quantum functions.

We compose a pair of quantum functions $(H, P) : A \to B$ and $(H', Q) : B \to C$ to obtain the quantum function $(H \otimes H', Q \circ P) : A \to C$ as follows:



(8.14)

Standard composition and tensor product of linear maps respectively, give the vertical and horizontal composition of 2-morphisms.

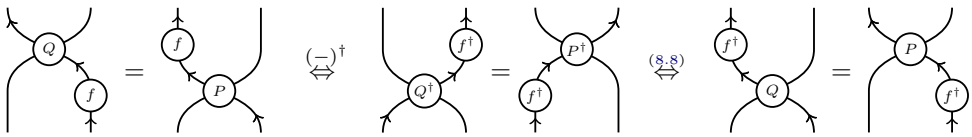
We observe that $\mathbf{QSet}(A, B) = \mathbf{QFunc}_{A,B}$.

Remark 14. *Given a monoidal category* $\mathbf{C}$ *the delooping of* $\mathbf{C}$*, denoted* $\mathbf{BC}$ *is defined to be the 2-category with a single object* $*$ *and endomorphism category* $\mathrm{Hom}(*, *) = \mathbf{C}$*. Given a 2-category* $\mathbb{B}$*, Street defined the 2-category* $\mathbf{CoMnd}(\mathbb{B})$ *to be the category of comonads, comonad maps and comonad transformations in* $\mathbb{B}$ *[Str72].*

Quantum sets are Frobenius algebras and therefore comonoids in **FHilb** *and comonads in* **BFHilb***. The first two equations of* (8.8) *define a comonad map in* **BFHilb***, it can easily be shown that our intertwiners are comonad transformations in* **BFHilb***. We therefore observe that* **QSet** *is a sub-2-category of* $\mathbf{CoMnd}(\mathbf{BFHilb})$*.*

Theorem 8.2.12. **QSet** *is a dagger 2-category.*

Proof. The category $\mathbf{CoMnd}(\mathbf{BFHilb})$ is well known to be a 2-category, see for example a proof due to Street in the strict case [Str72]. Remark 14 therefore gives us that **QSet** is a 2-category. We define a dagger on 2-morphisms by taking the usual linear algebraic adjoint. For this to be well defined we need the adjoint of an intertwiner $f : (H, P) \to (H', Q)$ to be an intertwiner $f^\dagger : (H', Q) \to (H, P)$. We show this below.



(8.15)

□

Definition 8.2.13. Given a dagger monoidal category $\mathbf{C}$ and a faithful dagger monoidal functor $F : \mathbf{C} \to \mathbf{FHilb}$. We say that the pair $(\mathbf{C}, F)$ form a *concrete dagger monoidal category.*

Similarly we have the following higher categorical definition.

Definition 8.2.14. Given $\mathbb{B}$ a dagger 2-category and a locally faithful dagger 2-functor $F : \mathbb{B} \to \mathbf{BFHilb}$ then $(\mathbb{B}, F)$ is a *concrete dagger 2-category*.

So a concrete dagger 2-category is a 2-category such that every Hom-category is a concrete dagger monoidal category in a consistent way.

$\mathbf{QFunc}_{\mathbf{A},\mathbf{B}}$ together with F as in Proposition 8.2.7 is a concrete dagger monoidal category. The underlying Hilbert space of the composite of two quantum functions is the tensor product of the underlying Hilbert spaces of the quantum functions. Vertical and horizontal composition of 2-morphisms is precisely the composition and tensor product of linear maps. Thus we have a forgetful 2-functor:

$$F : \mathbf{QSet} \to \mathbf{BFHilb}. \tag{8.16}$$

from **QSet** to the delooping of **FHilb** (see Remark 14) taking all quantum sets to the unique object in **BFHilb**. Together with F, **QSet** is a *concrete dagger 2-category*. The 2-functor $F : \mathbf{QSet} \to \mathbf{BFHilb}$ can be identified with the functor appearing in Proposition 8.2.7.

Remark 15. *Functions between sets can be seen, via Gelfand duality as one-dimensional quantum functions between †-SCFAs. Intertwiners for functions between sets in* **QSet** *are just complex scalars. There therefore exists a faithful inclusion 2-functor* $\mathbf{Set} \hookrightarrow \mathbf{QSet}$ *where we add identity 2-morphisms for every 1-morphism in* **Set** *to make it a 2-category. Given morphisms in* **Set** f *and* g *we have that* $\mathbf{QSet}(f, g) = \delta_{f,g}\mathbb{C}$.

Remark 16. *The category of sets and functions with the standard cartesian product is a symmetric monoidal category. Similarly, it can be shown that* **QSet**, *using the tensor product of the underlying algebras, becomes a symmetric monoidal 2-category.*

8.2.4 Quantum bijections in noncommutative topology

We now show that the monoidal categories $\mathbf{QBij}(B, B)$ of quantum bijections on a quantum set B correspond to an object studied previously in noncommutative topology.

Quantum symmetry groups of quantum sets were introduced by Wang as quantum analogues of the symmetric groups [Wan98]. We now show that our categories $\mathbf{QBij}(B, B)$ correspond to the categories of finite-dimensional representations of Wang's quantum symmetry groups.

Proposition 8.2.15. *Given a quantum set* B, $\mathbf{QBij}(B, B)$ *is the category of finite-dimensional representations of* $A_{aut}(B)$, *the Hopf* C^**-algebra corresponding to Wang's quantum symmetry group.*

Proof. We prove the proposition for classical sets $[n]$; the proof for quantum sets in general follows in exactly the same way but involves more indices.

Wang's quantum permutation groups of sets $[n]$ are defined to be C^*-algebras with generators $a_{i,j}$ $(i,j \in [n])$ and relations:

$$a_{i,j}^2 = a_{i,j} = a_{i,j}^*, \qquad \sum_{i=1}^{n} a_{i,j} = 1, \quad \forall j \in [n], \qquad \sum_{j=1}^{n} a_{i,j} = 1, \quad \forall i \in [n]. \tag{8.17}$$

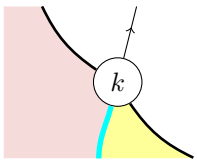
See [Wan98, Theorem 3.1]. Given that a family of projectors summing to the identity must be mutually orthogonal, Corollary 8.3.8 shows that our categories $\mathbf{QBij}([n],[n])$ are the categories of finite-dimensional representations of $A_{aut}([n])$. □

8.3 Quantum morphisms of classical sets

In this section we explore quantum functions and quantum bijections between finite classical sets. First we define quantum isometry Latin squares.

8.3.1 Quantum functions on sets

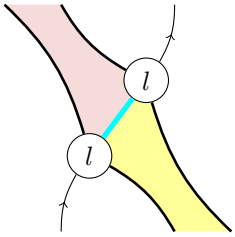
Definition 8.3.1. An n-by-m array of isometries $l_{ij} : (H_{ij} \cong \mathbb{C}^{a_{ij}}) \to (H \cong \mathbb{C}^d)$ with $i \in [n]$, $j \in [m]$, is a *left-sided quantum isometry Latin square (left-sided QILS)*, denoted (l_{ij}, a_{ij}, d) if the following linear map is unitary:



From Lemma 5.4.2 in Chapter 5 we can see the justification for the name left-sided QILS. We could also define right-sided QILS similarly by requiring that the right hand linear map of diagram (5.22) be unitary. QILS therefore, are both left and right-sided in this sense.

Given a left-sided QILS l, consider the result of projecting out as discussed in Section 8.1.4.

Definition 8.3.2 (Left-sided PPM)**.** Given a left-sided QILS l the following linear map is a *left-sided PPM:*



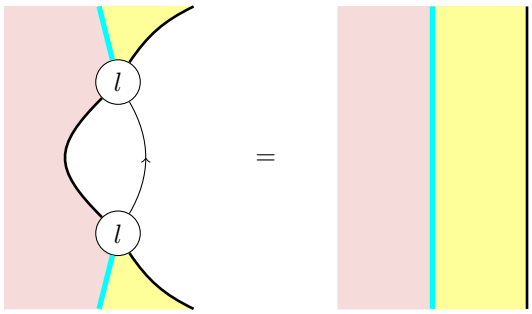
(8.18)

Proposition 8.3.3. *An n-by-m left-sided PPM is precisely a rectangular grid of projectors P_{ij} with*

$i \in [n]$ and $j \in [m]$ such that the following hold for all $i \in [n]$ and $j, k \in [m]$:

$$P_{ik}P_{ij} = \delta_{jk}P_{ij}, \qquad \sum_q P_{iq} = \mathbb{I}\,. \tag{8.19}$$

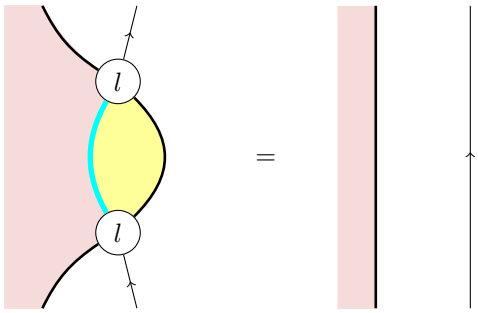
Proof. For each entry l_{ij} define P_{ij} as follows $P_{ij} := l_{ij}l_{ij}^\dagger$. First note that $P_{ij}^\dagger = (l_{ij}l_{ij}^\dagger)^\dagger = l_{ij}l_{ij}^\dagger = P_{ij}$. Definition 8.3.1 gives us the following equation:



By entering i in the pink region and j and k in the bottom and top yellow regions on both sides of this equation we obtain:

$$\begin{aligned} l_{ij}^\dagger l_{ik} &= \delta_{jk}\mathbb{I}_{a_{ij}} \\ \Leftrightarrow l_{ij}l_{ij}^\dagger l_{ik}l_{ik}^\dagger &= \delta_{jk}l_{ij}l_{ik} \\ \Leftrightarrow P_{ij}P_{ik} &= \delta_{jk}P_{ij}. \end{aligned}$$

Composing in the opposite direction gives:



By entering i in the pink region we obtain:

$$\sum_j l_{ij}l_{ij}^\dagger = \sum_j P_{ij} = \mathbb{I}\,.$$

□

Proposition 8.3.4. *A quantum function $X \to Y$ between classical sets X and Y is exactly a family of*

projectors $\{P_{x,y}\}_{x\in X, y\in Y}$ *on a Hilbert space* H *such that the following holds:*

$$P_{xy}P_{xy'} = \delta_{yy'}P_{xy}, \qquad \sum_{y\in Y} P_{xy} = \mathbb{I}_H. \tag{8.20}$$

Proof. Equations (8.8) translate as equations (8.20) with the addition of $P_{ij}^\dagger = P_{ij}$ for all $i \in [n]$ and $j \in [m]$ as required for P_{ij} to be orthogonal projectors. □

We can now see that projected out left-sided QILS are precisely quantum functions between finite classical sets.

Corollary 8.3.5. *Given †-SCFAs* X *and* Y*, a Hilbert space* H*, and a linear map* $P : H \otimes X \to Y \otimes H$ *the following are equivalent:*

- (P, H) *is a quantum function* $X \to Y$*;*
- P *is a left-sided PPM for some left-sided QILS* $(l_{ij}, a_{ij}, dim(H))$ *with* $i \in [dim(X)]$ *and* $j \in [dim(Y)]$*.*

Proof. The result follows by combining Proposition 8.3.3 and Proposition 8.3.4. □

Remark 17. *Following Proposition 8.3.5 we see that quantum functions between finite classical sets are rectangular grids of orthogonal projectors which are orthogonal and span the underlying Hilbert space along each row. Thus quantum functions between finite classical sets* $X \to Y$ *are families of projective measurements with outcomes in* Y*, controlled by the set* X*.*

We can think of a quantum function as a non-deterministic function from a set X *to a set* Y *which uses quantum measurements on an underlying Hilbert space to determine the outcome it produces from a given input.*

Remark 18. *Given that a quantum element* Q *on a classical set* X *is a quantum function from the one element set to* X*,* Q *is a projective measurement with outcomes in* X*. In this case, examples of intertwiners* $Q \to Q$ *are given by projectors onto subspaces which are left undisturbed by the measurement.*

8.3.2 Quantum bijections on sets

We now consider quantum bijections between finite classical sets.

Corollary 8.3.6. *Given †-SCFAs* X *and* Y *and a Hilbert space* H*, and a linear map* $P : H \otimes X \to Y \otimes H$ *the following are equivalent:*

- (P, H) *is a quantum bijection* $X \to Y$*;*
- P *is a PPM for some QILS* $(k_{ij}, a_{ij}, dim(H))$ *with* $i \in [dim(X)]$ *and* $j \in [dim(Y)]$*.*

Proof. The result is obtained by combining Lemma 8.1.3 and Proposition 8.2.8. □

In light of this we can identify quantum bijections between sets and grids of orthogonal projectors such that every row and column is a projective measurement. We now show that quantum bijections only occur between classical sets of the same cardinality.

Proposition 8.3.7. *If there is a quantum bijection from a classical set X to a classical set Y, then $|X| = |Y|$. In other words, every projective permutation matrix is square.*

Proof. By Corollary 8.3.6, a quantum bijection is a PPM. PPMs are biunitary by Proposition 5.4.8 and so in particular $P : X \otimes H \to H \otimes Y$ is unitary. Thus, $|X| \dim(H) = \dim(X \otimes H) = \dim(H \otimes Y) = |Y| \dim(H) \Rightarrow |X| = |Y|$. □

We now have the following corollary:

Corollary 8.3.8. *A quantum bijection $X \to Y$ is precisely a grid of projectors P_{ij} with $i, j \in [n]$ (with $|X| = |Y| = n$) such that the following hold:*

$$P_{jk}P_{ik} = \delta_{ij}P_{ik}, \qquad \sum_n P_{nj} = \mathbb{I}, \tag{8.21}$$

$$P_{ik}P_{ij} = \delta_{jk}P_{ij}, \qquad \sum_m P_{im} = \mathbb{I}. \tag{8.22}$$

Proof. The result follows from Corollary 8.3.6 and Proposition 8.1.2 □

In the work of Banica et al, matrices of projectors obeying equations (8.21) and (8.22) are called *magic unitaries* [BBC07b], while the term *projective permutation matrices* first appeared in the work of Atserias et al [AMR+19]. We will refer to quantum bijections between classical sets as projective permutation matrices from now on.

Remark 19. *In terms of the underlying projectors, the composition of quantum functions $P : X \to Y$ and $Q : Y \to Z$ (see equation (8.14)) takes the following form:*

$$(Q \circ P)_{x,z} = \sum_{y \in Y} Q_{y,z} \otimes P_{x,y}. \tag{8.23}$$

This is precisely composition of quantum functions in the Kleisli category of Abramsky et al [ABdSZ17].

Examples of projective permutation matrices are provided by projecting out any example of a QLS or QILS in this thesis.

8.4 Quantum graph theory

In this section we continue the programme of quantization from earlier in the chapter. We have introduced quantized finite set theory which we now extend to include the quantum theory of finite undirected graphs. We begin by rephrasing classical graph theory in terms of adjacency matrices and †-SCFAs representing the sets of vertices. We then consider *quantum graphs* over quantum sets or †-SSFAs with quantum adjacency matrices.

Classical graph homomorphisms can be seen as functions between the sets of vertices with additional compatibility with the structure of the graphs. By analogy we define quantum homomorphisms of quantum graphs to be quantum functions of the quantum sets of vertices with an additional axiom involving the quantum adjacency matrices. We show that quantum graphs, quantum homomorphisms and intertwiners form a concrete dagger 2-category **QGraph** which is a full sub-2-category of **QSet**.

Through the framework of **QGraph** we recover various other theories of quantum graphs from noncommutative topology [Ban05, BB09, BB07, Bic03], operator algebras [Wea10, KW12, Wea15] and quantum information [DSW13, Sta16]. In the restriction of **QGraph** to quantum homomorphisms between classical graphs we recover recent work in non-local games [CMN$^+$07, MR16, AMR$^+$19]. This connection will be proven and further explored in Chapter 9.

A more usual approach to quantizing a classical graph is to quantize the relational structure the edges encode on the set of vertices [Wea10, KW12, DSW13, Wea15, Sta16]. In Section 8.5 we show that our framework coincides with and generalizes previous work using the quantum relation approach.

8.4.1 Quantum graphs and quantum adjacency matrices

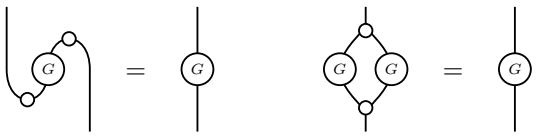
We denote the set of vertices of a classical graph G, by V_G and as usual we also use V_G to denote the associated †-SCFA and Hilbert space. Given vertices $v, w \in V_G$ we denote by $v \sim_G w$ the existence of an edge between v and w in G. We will denote by $G : V_G \to V_G$ the *adjacency matrix* of G a linear map which encodes the connectivity of G as follows.

Definition 8.4.1. For $v, w \in V_G$ the linear map $G : V_G \to V_G$ is the *adjacency matrix* for G if the following to conditions hold:

$$\langle w|G|v\rangle = 1 \quad \text{if} \quad v \sim_G w,$$
$$\langle w|G|v\rangle = 0 \quad \text{if} \quad v \nsim_G w.$$

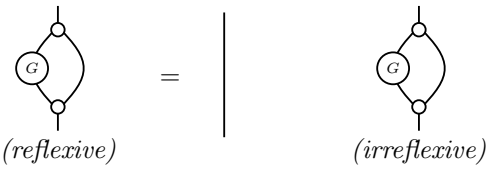
Given a classical graph G it is completely characterized by its set of vertices V_G and its adjacency matrix. We now give a diagrammatic axiomatization of a graph using the adjacency matrix and vertex set †-SCFA .

Proposition 8.4.2. *Given a †-SCFA V_G and linear map $G : V_G \to V_G$, G is an undirected finite graph if and only if the following hold:*



(8.24)

In addition a graph G is said to be reflexive or irreflexive respectively if one of the following holds:

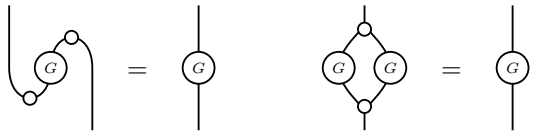


(8.25)

Proof. Equations (8.24) translate as: for all $v, w \in V_G$ we have $\langle w|G|v\rangle = \langle v|G|w\rangle$ and $(\langle w|G|v\rangle)^2 = \langle w|G|v\rangle$. Reflexivity is $\langle v|G|v\rangle = 1$ and irreflexivity is $\langle v|G|v\rangle = 0$ as expected. □

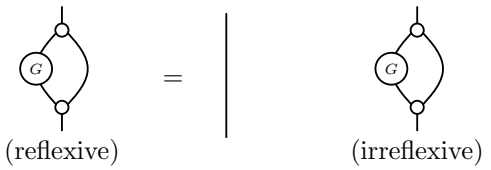
Given this characterization the following quantization is natural.

Definition 8.4.3. Let the pair (A, G) be a quantum set A denoted by  (the *quantum set of vertices*) and a self-adjoint linear map $G : A \to A$ (the *quantum adjacency matrix*). The pair (A, G) is a *quantum graph* if the following hold:



(8.26)

In addition a quantum graph is said to be *reflexive* or *irreflexive* if one of the following holds:



(8.27)

Remark 20. *As mentioned above there are various definitions of non-commutative graphs in the literature. In Section 8.5 we show the following:*

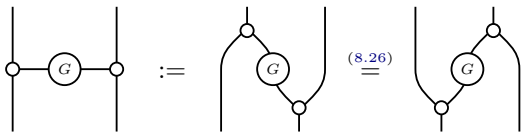
- *The reflexive quantum graphs defined above are precisely Weaver's finite-dimensional quantum graphs [Wea15], derived as symmetric and reflexive quantum relations [KW12, Wea10].*
- *The restriction of our reflexive quantum graphs to matrix algebras $(\mathbb{M}_n, G)$ are precisely the non-commutative graphs of Duan, Severini and Winter [DSW13].*

8.4.2 Quantum homomorphisms

In this section we quantize graph homomorphisms. We also show that our quantum and classical homomorphisms between quantum graphs are the restriction to pure states of Stahlke's *homomorphisms* and *entanglement assisted homomorphisms* between non-commutative graphs which are defined in terms of CPTP maps [Sta16].

As with quantum graphs we begin by translating the properties of classical graph homomorphisms into the language of string diagrams making use of Gelfand duality in the usual way.

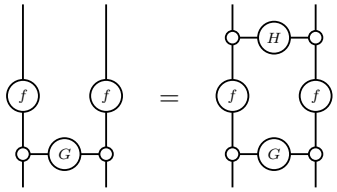
We begin with some notation. Given a quantum graph (A, G) with A represented by a white dot as usual, we define the following:



(8.28)

For a classical graph (V_G, G) the linear map (8.28) is a projector onto the subspace of $V_G \otimes V_G$ spanned by $|v\rangle \otimes |w\rangle$ such that $v \sim_G w$. We now make use of these projectors to characterize classical graph homomorphisms diagrammatically.

Proposition 8.4.4. *Let (V_G, G) and (V_H, H) be classical graphs. A graph homomorphism $G \to H$ is a cohomomorphism of Frobenius algebras $f : V_G \to V_H$ such that the following equation holds:*

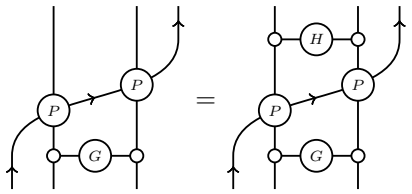


(8.29)

Proof. The linear map (8.28) is a projector onto the linear span of the subset of connected pairs of vertices. Thus equation (8.29) expresses that if $v \sim_G w$, then $f(v) \sim_H f(w)$. □

This leads naturally to the following quantization.

Definition 8.4.5. Given quantum graphs (A, G) and (B, H) a quantum function $(H, P) : A \to B$ satisfying the following additional equation is a *quantum homomorphism*:



(8.30)

Stahlke [Sta16] considers homomorphisms [Sta16, Definition 7] and so called *entanglement assisted homomorphisms* [Sta16, Definition 15] between *non-commutative graphs on operator spaces* and relates

them to zero-error strategies for quantum source-channel coding in various scenarios. In Section 8.5 we show that these non-commutative graphs on operator spaces are precisely our quantum graphs over matrix algebras (see Corollary 8.5.7).

Stahlke's homomorphisms and entanglement assisted homomorphisms are defined in terms of completely positive trace preserving (CPTP) maps in the mixed state setting. If we restrict to the pure state setting of $*$-homomorphisms of C^*-algebras then Stahlke's homomorphisms correspond to classical graph homomorphisms between matrix algebras (in our sense). The pure state $*$-homomorphism version of Stahlke's entanglement assisted homomorphisms agrees with our quantum homomorphism if the entangled resource is a maximally entangled state. In the terminology of Stahlke the entanglement resource being maximally entangled is equivalent to the positive operator Λ used to define the entanglement assisted homomorphism (see [Sta16, Definition 15]) being the identity on some finite-dimensional Hilbert space V.

8.4.3 Quantum isomorphisms

A classical *graph isomorphism* is a graph homomorphism that is invertible and whose inverse is also a graph homomorphism. It is well known that this conditation is equivalent to the following.

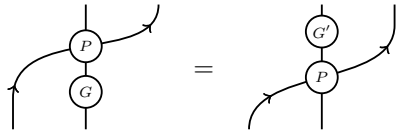
Proposition 8.4.6. *Let G and H be classical graphs. Under Gelfand duality, a graph isomorphism $G \to H$ corresponds to an isomorphism of Frobenius algebras $f : V_G \to V_H$ fulfilling the following equation:*



(8.31)

This leads to the following quantization.

Definition 8.4.7. Given quantum graphs (A, G) and (A', G') a quantum bijection $(H, P) : A \to A'$ fulfilling the following additional equation is a *quantum isomorphism* $(H, P) : (A, G) \to (A', G')$:



(8.32)

8.4.4 The 2-category QGraph

Quantum graphs and quantum homomorphisms with the addition of intertwiners form a 2-category under composition. We call this 2-category **QGraph**.

Definition 8.4.8. The 2-category **QGraph** is as follows:

- **objects** are quantum graphs $(A, G), (A', G')$, ...;

- **1-morphisms** $(A, G) \to (A', G')$ are quantum homomorphisms $(H, P) : (A, G) \to (A', G')$;
- **2-morphisms** $(H, P) \to (H', P')$ are intertwiners of the underlying quantum functions (see Definition 8.2.5).

Remark 21. *Every quantum homomorphism between quantum graphs (A, G) and (B, H) is a quantum function between the underlying quantum sets of vertices A and B. Since an intertwiner of quantum homomorphisms is exactly an intertwiner of the underlying quantum functions, it follows that the category* $\mathbf{QGraph}((A, G), (B, H))$ *is a full subcategory of the category* $\mathbf{QSet}(A, B)$*. In other words, there is a forgetful 2-functor* $\mathbf{QGraph} \to \mathbf{QSet}$ *which is locally fully faithful.*

Many of the same structures follow through from **QSet**. Analogously to $\mathbf{QBij} \subset \mathbf{QSet}$, we define a subcategory $\mathbf{QIso} \subset \mathbf{QGraph}$ of quantum graphs, quantum isomorphisms and intertwiners.

The same forgetful dagger 2-functor $F : \mathbf{QGraph} \to \mathbf{BFHilb}$ which maps each quantum homomorphism to its underlying Hilbert space and each intertwiner to its corresponding linear map also carries through from **QSet**. As expected the pair $(\mathbf{QGraph}, F)$ form a concrete dagger 2-category (see Definition 8.2.14).

Recall that our categories $\mathbf{QBij}(B, B)$ correspond to the categories of finite-dimensional representations of Wang's quantum symmetry groups (see Section 8.2.4). In 2005 Banica [Ban05] introduced *quantum automorphism groups* of classical finite graphs, building upon the definition of quantum symmetry groups. We now show that our categories $\mathbf{QIso}((V_G, G), (V_G, G))$ for classical graphs G are the categories of finite-dimensional representation categories of these quantum automorphism groups.

Proposition 8.4.9. *Given a classical graph (V_G, G), the category* $\mathbf{QIso}((V_G, G), (V_G, G))$ *is the category of finite-dimensional representations of the quantum automorphism group Hopf C^*-algebra $A_{aut}(G)$ (see e.g. [BB07, Definition 2.1]).*

Proof. Given a graph G, let $a_{i,j}$ $(i, j \in [n])$ be the generators of $A_{aut}(G)$ where $n = |V_G|$. The relations are as follows (see Theorem 2.1 and Example 2.2 in [Ban05]):

$$a_{i,j}^2 = a_{i,j} = a_{i,j}^* \sum_{i=1}^{n} a_{i,j} = 1 \quad \text{for all } j \in [n], \qquad \sum_{j=1}^{n} a_{i,j} = 1, \quad \text{for all } i \in [n],$$

$$\sum_{k=1}^{n} \langle k|G|i\rangle \; a_{k,j} \;=\; \sum_{k=1}^{n} a_{i,k} \; \langle j|G|k\rangle.$$

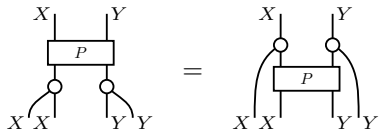
As usual we have denoted the adjacency matrix by G. As in the proof of Proposition 8.2.15 we compare these relations with equations (8.21), (8.22) and equation (9.5) from Chapter 9 to show that $\mathbf{QIso}((V_G, G), (V_G, G))$ is the category of finite-dimensional representations of $A_{aut}(G)$. □

8.5 Quantum graphs and quantum relations

Finite undirected classical graphs are alternatively defined to be reflexive and symmetric relations on the set of vertices. In the final section of this chapter we define *quantum relations* by phrasing relations in the language of †-SCFAs and then generalizing to †-SSFAs. We then show that the reflexive symmetric quantum relations obtained in this manner correspond to our definition of quantum graphs. This approach is similar to that of previous authors [KW12, Wea10, Wea15, DSW13, OP16]. We show that our definition of reflexive symmetric quantum relations is equivalent to that of Kuperberg and Weaver [KW12, Wea15] and thus generalize the non-commutative graphs of Duan, Severini and Winter [DSW13].

We begin with the following characterization of relations between sets in terms of bimodules over †-SCFAs.

Proposition 8.5.1. *A binary relation between two finite sets X and Y can be expressed, via Gelfand duality, as a projector $P\colon X\otimes Y\to X\otimes Y$ such that the following equation holds:*

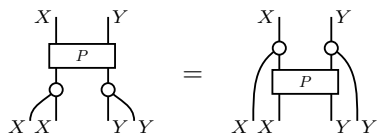


(8.33)

Proof. Projectors encode subspaces of Hilbert spaces. The condition (8.33) ensures that the subspace encoded by P is a linear span of a subset of the set $X\times Y$, which corresponds to the usual definition of a binary relation. Note that condition (8.33) makes P a bimodule over X and Y. □

This leads to the following quantization.

Definition 8.5.2. Given quantum sets A and B a projector $P : A\otimes B\to A\otimes B$ is a quantum relation on A and B if the following equation holds:



(8.34)

In the case $A = B$ we call P a *quantum relation on the quantum set A*.

We now show that this definition coincides with that of Kuperberg and Weaver [Wea10, KW12]. They define a quantum relation on a von Neumann algebra $\mathcal{M}\subseteq\mathcal{B}(H)$ to be a weak*-closed operator bimodule over the commutant $\mathcal{M}'$ (see Definition 2.1 in [Wea10]). In the finite-dimensional case (see Definition 5.1 in [Wea15]), this definition reduces to the following:

Definition 8.5.3. Let A be a finite-dimensional C^*-algebra and let $A' = \{b\in\mathcal{B}(A)\mid ba = ab\ \forall a\in A\}$ be the commutant of A with respect to the embedding $A\subseteq\mathcal{B}(A)$. A *quantum relation in the sense of Kuperberg and Weaver* is a subspace $V\subseteq\mathcal{B}(A)$ which fulfills $A'VA'\subseteq V$.

Note that in Kuperberg and Weavers' paper, Definition 8.5.3 is given in terms of an embedding into the operator space $\mathcal{B}(H)$ of an arbitrary Hilbert space H rather than $\mathcal{B}(A)$ as above. It is shown in Theorem 2.7 of [Wea10] that this definition is independent of the embedding $A \subseteq \mathcal{B}(H)$ and that if H and H' are finite-dimensional Hilbert spaces such that there are embeddings $A \subseteq \mathcal{B}(H)$ and $A \subseteq \mathcal{B}(H')$, then there is a canonical correspondence between the correspondingly defined quantum relations. We now show that this definition is equivalent to our own.

Proposition 8.5.4. *Given a finite-dimensional C^*-algebra A, our notion of a quantum relation on A (Definition 8.5.2) coincides with that of Kuperberg and Weaver (Definition 8.5.3).*

Proof. Given a finite-dimensional C^*-algebra A we have a †-SSFA as explained in Section 2.1.2 of the background chapter. This gives us a Hilbert space A and we have a C^*-algebra embedding $A \subseteq \mathcal{B}(A)$ given as follows; we map $a \in A$ to $L_a \in \mathcal{B}(A)$ with:

$$L_a(b) = ab \qquad \text{for all } b \in A.$$

The commutant A' of A is $*$-isomorphic to the opposite algebra of A denoted by A^{op} with multiplication given by $a \star b := ba$ as we will now show. First we give a faithful $*$-homomorphism $A^{op} \to A'$ which we will then show to be surjective. We take $a \in A^{op}$ to R_a in A' defined by:

$$R_a(b) = ba \quad \text{for all } b \in A.$$

Note that since $R_a L_a = L_a R_a$ for all $a \in A$ the linear operator R_a is indeed in A'.

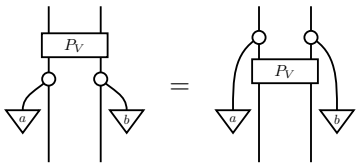
We now show that every element of A' arises as R_a for some $a \in A$ and so the faithful $*$-homomorphism is surjective and thus a $*$-isomorphism. Let $X \in A'$ and denote as $e \in A$ the unit of A. Since $X \in \mathcal{B}(A)$ we have that $X(e) \in A$. We now show that $X = R_{X(e)}$. For all $b \in A$ we have that $R_{X(e)}(b) = bX(e) = L_b X(e)$. Now since $X \in A'$ and $e \in A$ we have that $L_b X(e) = X L_b(e) = X(be) = X(b)$. So we have $X = R_{X(e)}$ as required and the $*$-homomorphism $A^{op} \to A'$ is faithful and surjective and is therefore a $*$-isomorphism.

Note that the †-SSFA structure on A induces a canonical isomorphism $A \cong A^*$ and so $\mathcal{B}(A) \cong A \otimes A$. We now have that a quantum relation as in Definition 8.5.3 is equivalent to a subspace $V \subseteq \mathcal{B}(A) \cong A \otimes A$ such that for all $a, b \in A$ we have $R_a V R_b \subseteq V$. For $a, b \in A$ under the isomorphism $\mathcal{B}(A) \cong A \otimes A$ left composition by R_a in $\mathcal{B}(A)$ becomes left multiplication by $(a \otimes e)$ in $A \otimes A$ and similarly right composition by R_b is equivalent to right multiplication by $(e \otimes b)$.

$$R_a \circ - : \mathcal{B}(A) \to \mathcal{B}(A) \quad - \circ R_b : \mathcal{B}(A) \to \mathcal{B}(A)$$

$$(a \otimes e) \cdot - : A \otimes A \to A \otimes A \quad - \cdot (e \otimes b) : A \otimes A \to A \otimes A$$

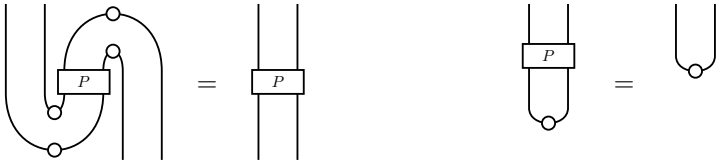
Diagrammatically V can be encoded by the projector P_V onto the subspace V which is as follows. For all $a, b \in A$:



This coincides with our Definition 8.5.2. □

As mentioned above a classical graph is a symmetric and reflexive binary relation on a set. Following Weaver [Wea10] we define the quantum analogues as follows.

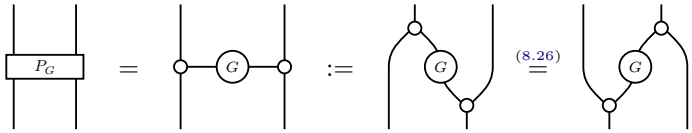
Definition 8.5.5. Given a quantum set A, a quantum relation $P : A \otimes A \to A \otimes A$ is *symmetric* or *reflexive* if one of the following holds:



(8.35)

a) symmetric b) reflexive

We now show that quantum graphs as in Definition 8.4.3 are indeed symmetric and reflexive quantum relations. For a quantum graph (A, G) as in Definition 8.4.3, we introduce the following linear map $P_G : A \otimes A \to A \otimes A$:

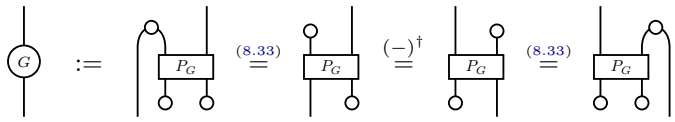


(8.36)

For a classical graph (V_G, G), it is easily verified that this map (8.36) is the projector onto the subspace of the symmetric and reflexive relation defining the graph:

$$\{(v, w) \mid v \sim_G w\} \subseteq V_G \times V_G. \tag{8.37}$$

Conversely, the adjacency matrix G can be recovered from this projector as follows:



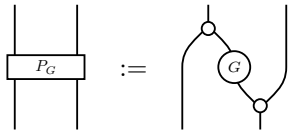
(8.38)

The same correspondence holds for general quantum graphs.

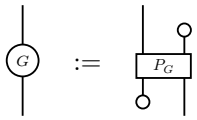
Theorem 8.5.6. *Given a quantum graph (A, G) as in Definition 8.4.3, the projector*

$P_G : A \otimes A \to A \otimes A$ defined by equation (8.36) is a symmetric and reflexive quantum relation as in Definition 8.5.2 and 8.5.5. Given a symmetric and reflexive quantum relation P on A, the map (8.38) defines a quantum adjacency matrix. These two constructions are mutually inverse.

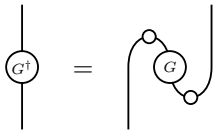
Proof. Given an arbitrary linear map $G : A \to A$, we define the following linear map $P_G : A \otimes A \to A \otimes A$ fulfilling (8.34):



Conversely, given a linear map $P_G : A \otimes A \to A \otimes A$ fulfilling (8.34), we define:



It follows easily from equation (8.34) that these two constructions are mutually inverse. In the following, we say that G is *real* if the following holds:



Simple graphical arguments then establish the following:

- G is real if and only if P_G is self-adjoint.
- G fulfills the first equation of (8.26) if and only if $P_G^2 = P_G$.
- G fulfills the second equation of (8.26) if and only if P_G is symmetric.
- G fulfills the last equation of (8.26) if and only if P_G is reflexive. □

Duan, Severini and Winter [DSW13] introduced a notion of quantum graph derived by introducing a non-commutative quantum analogue of the *confusability graphs* arising in classical zero-error communication.

Weaver showed in a 2015 paper [Wea15] that his symmetric and reflexive quantum relations (see Definition 8.5.3) defined over matrix algebras are precisely the quantum graphs of Duan Sevrini and Winter. The following corollary therfore follows from Proposition 8.5.4 and Theorem 8.5.6.

Corollary 8.5.7. *Given an n-dimensional Hilbert space H, Duan, Severini and Winters' quantum graphs on H are precisely quantum graphs of the form $(\mathbb{M}_n, G)$.*

Chapter 9

Quantum non-local games and pseudo-telepathy

In the study of quantum information and computation a great deal of effort has been expended in trying to find instances when quantum resources allow the completion of a particular task that is impossible classically. Quantum non-local games have proven to be a good formalism for the search for quantum advantage. In the context of non-local games, quantum pseudo telepathy refers to an instance of a game that admits a perfect strategy only when the participants are given access to quantum resources. In particular, for the quantum graph isomorphism game, pairs of graphs witness quantum pseudo telepathy if they admit a perfect quantum strategy but no perfect classical strategy. This is equivalent to pairs of graphs that are quantum isomorphic but not classically isomorphic. In this chapter we show that the 2-category **QGraph** introduced in Chapter 8 captures the quantum graph homomorphisms and isomorphisms of quantum non-local games and use this to restrict the class of pairs of classical graphs that can exhibit quantum pseudo-telepathy.

9.1 Introduction

A big motivation for us in the introduction of **QSet** and **QGraph** was recent work extending the ideas of graph homomorphism and graph isomorphism.

In the context of non-local games, quantum analogues of graph homomorphisms and isomorphisms were recently introduced [MR16, AMR+19] and have been extensively studied by Mančinska, Roberson, Severini, Winter and others [MR16, SS12, AHKS06, CMN+07, PT15, PSS+16, Rob16, AMR+19]. In Sections 9.2 and 9.3 of this chapter we prove the correspondence between perfect strategies for the quantum graph homomorphism and isosmorphism games and the quantum homomorphisms and quantum isomorphisms that we defined within the framework of **QGraph** in Chapter 8 (See Definitions 8.4.5

and 8.4.7) when restricted to classical graphs. We then illustrate this correspondence in Section 9.4 by showing that quantum functions and bijections can be captured within the formalism of quantum non-local games. Finally in Section 9.5 we use this correspondence and results about projective permutation matrices from previous chapters to give a new invariant of quantum isomorphic graphs which drastically reduces the number of pairs of graphs to check for quantum pseudo telepathy. As a point of notation we denote that two vertices $a, b \in V_G$ are connected by an edge in the graph G by $a \sim_G b$.

9.2 Quantum graph homomorphisms

In their 2016 paper Mančinska and Roberson [MR16] defined the *quantum graph homomorphism game*. A perfect strategy for this game was defined to be a *quantum graph homomorphism*. This generalized earlier work defining the quantum chromatic number of a graph via the quantum graph colouring game [AHKS06, CMN+07]. We begin this section by defining the quantum graph homomorphism game.

Definition 9.2.1. [MR16, Quantum graph homomorphism game] The following non-local game is the *quantum graph homomorphism game*. Alice and Bob share a maximally entangled quantum state on the system $\mathcal{H} \otimes \mathcal{H}$. Given graphs (V_G, G) and (V_H, H):

Step one. The verifier gives Alice and Bob g_1 and g_2 respectively with $g_1, g_2 \in V_G$.

Step two. Alice replies with h_1 and Bob replies with h_2.

Rules. Alice and Bob are space-like separated and cannot communicate once the game starts. However they are allowed to perform a projective measurement on their side of the entangled system.

Alice and Bob win if the following conditions hold:

- $h_1, h_2 \in V_H$;
- $g_1 = g_2 \Rightarrow h_1 = h_2$;
- $g_1 \sim_G g_2 \Rightarrow h_1 \sim_H h_2$.

Quantum homomorphisms between quantum graphs (A, G) and (B, H) in **QGraph** are defined to be quantum functions between the quantum sets A and B with an additional interaction with the quantum graphs given by equation (8.30). By Proposition 8.3.4 quantum functions between classical sets are precisely left-sided projective permutation matrices. By Proposition 8.3.3 left-sided PPMs are characterized by n-by-m grids of projectors satisfying equations (8.19). We now give a characterization of the restriction of quantum homomorphisms in **QGraph** to classical graphs in terms of the projectors of the underlying left-sided projective permutation matrices.

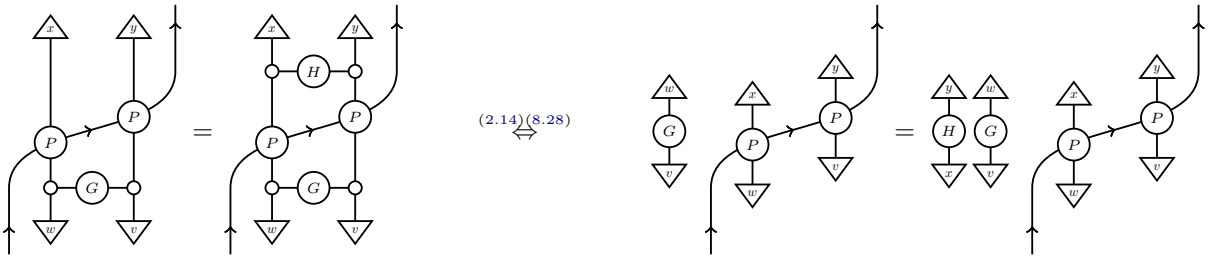
Proposition 9.2.2. *Given a quantum homomorphism in* **QGraph** *between classical graphs G and H, let the projectors associated with the underlying quantum function $V_G \to V_H$ be denoted by $P_{i,j}$ with $i \in V_G, j \in V_H$. The following conditions hold for all $v, w \in V_G$ and $x, y \in V_H$:*

$$P_{v,x}P_{v,y} = \delta_{yx}P_{v,y}, \qquad \sum_{z \in V_H} P_{v,z} = \mathbb{I}, \tag{9.1}$$

$$v \sim_G w \text{ and } x \not\sim_H y \qquad \Rightarrow \qquad P_{v,y}P_{w,x} = 0. \tag{9.2}$$

Conversely given projectors obeying equations (9.1) and condition (9.2) they form a quantum homomorphism.

Proof. The first condition (9.1) follows from Proposition 8.19. To obtain condition (9.2) we compose both sides of equation (8.30) by $|w\rangle \otimes |v\rangle$ and $\langle x| \otimes \langle y|$ as follows:



Here we denote the adjacency matrices as G and H respectively as usual. The RHS equation translates algebraically as $\langle w|G|v\rangle P_{v,y}P_{w,x} = \langle w|G|v\rangle\langle y|H|x\rangle P_{v,y}P_{w,x}$which is equivalent to condition (9.2). □

The correspondence with the non-local games definition then follows from the following result.

Proposition 9.2.3 ([MR16, Lemma 2.3])**.** *Given classical graphs G and H, there exists a perfect strategy for the quantum graph homomorphism game, if and only if there is a nonzero family of projectors $P_{v,w}$ with $v \in V_G, w \in V_H$ satisfying equations (9.1) and condition (9.2).*

Corollary 9.2.4. *Quantum homomorphisms in* **QGraph** *restrict precisely to the quantum graph homomorphisms of Mančinska and Roberson [MR16] when considered between classical graphs.*

9.3 Quantum graph isomorphisms

We now show that our quantum isomorphisms and the quantum graph isomorphisms of Atserias et al [AMR+19] are the same. First we give a definition of the quantum isomorphism game.

Definition 9.3.1. [AMR+19, Quantum graph isomorphism game] The following non-local game is the *quantum graph isomorphism game.* Alice and Bob share a maximally entangled quantum state on the system $\mathcal{H} \otimes \mathcal{H}$. Given graphs (V_G, G) and (V_H, H):

Step one. The verifier gives Alice and Bob x and y respectively with $x, y \in V_G \sqcup V_H$.

Step two. Alice replies with x' and Bob replies with y'.

Rules. Alice and Bob are space-like separated and cannot communicate once the game starts. However they are allowed to perform a projective measurement on their side of the entangled system.

Let a_1, a_2 be the vertices of G either received or returned by Alice and Bob respectively. Similarly let b_1 and b_2 be the vertices of H either received or returned by Alice and Bob respectively. Alice and Bob win if the following conditions hold:

- Alice and Bob both reply with a vertex from the other graph to which the vertex they received belonged.
- $a_1 = a_2 \Leftrightarrow b_1 = b_2$
- $a_1 \sim_G a_2 \Leftrightarrow b_1 \sim_H b_2$

Quantum ismomorphisms in **QGraph** are defined to be quantum bijections between the underlying quantum sets that also obey equation (8.32). By Corollary 8.3.6 and Corollary 8.3.8 quantum bijections between classical sets are precisely projective permutation matrices and are characterized by grids of projectors. We now give a characterization of the restriction of quantum isomorphisms in **QGraph** to classical graphs in terms of the projectors of the underlying projective permutation matrices.

Proposition 9.3.2. *Given a pair of classical graphs G and H and a quantum isomorphism P between them, let the projectors of the associated PPM be denoted by $P_{i,j}$ with $i \in V_G, j \in V_H$. The following conditions hold for all $v, w \in V_G$ and $x, y \in V_H$:*

$$P_{v,x}P_{w,x} = \delta_{vw}P_{w,x}, \qquad \sum_{n \in V_G} P_{n,x} = \mathbb{I}, \tag{9.3}$$

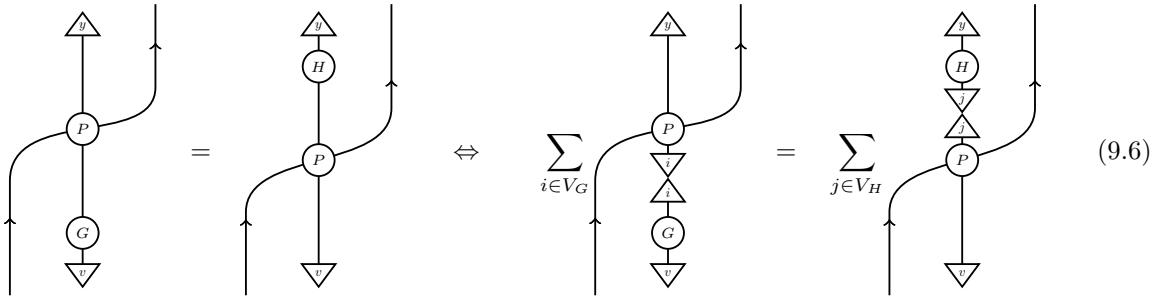
$$P_{v,x}P_{v,y} = \delta_{xy}P_{v,x}, \qquad \sum_{z \in V_H} P_{v,z} = \mathbb{I}. \tag{9.4}$$

And the following conditions are equivalent:

$$\begin{gathered} G \text{ and } H \text{ and } P \text{ obey equation (8.32)}, \\ (v \sim_G w \text{ and } x \not\sim_H y) \text{ or } (v \not\sim_G w \text{ and } x \sim_H y) \quad \Rightarrow \quad P_{v,x}P_{w,y} = 0. \end{gathered} \tag{9.5}$$

Proof. Equations (9.3) and (9.4) follow from Proposition 8.1.2 and Corollary 8.3.6. We obtain the fol-

lowing by composing both sides of equation (8.32) by $|v\rangle$ and $\langle y|$:



(9.6)

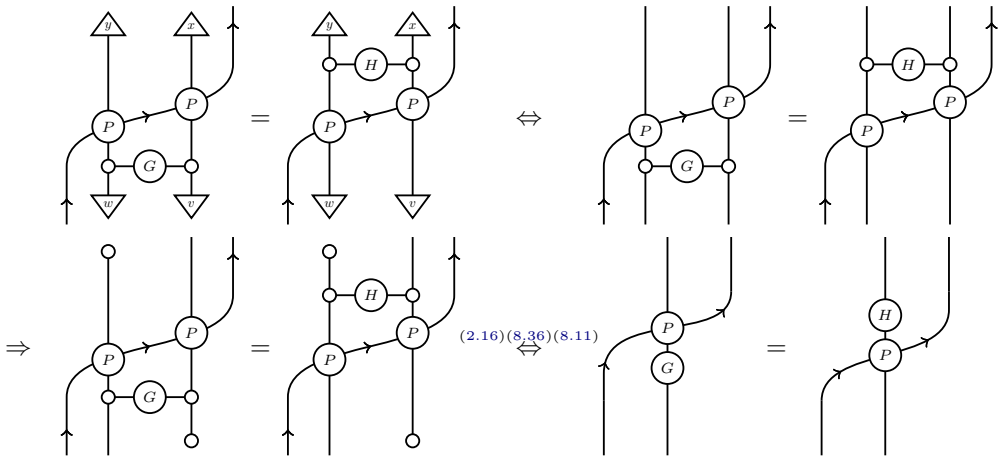
The equivalence of equations (9.6) is just a resolution of the identity. Translating the RHS algebraically we have $\sum_{i\in V_G}\langle i|G|v\rangle P_{i,y} = \sum_{j\in V_H}\langle y|H|j\rangle P_{v,j}$. For some $w \in V_G$ and $x \in V_H$, pre-composing both sides of the equation by $P_{w,y}$ and post-composing by $P_{v,x}$ we obtain the following:

$$\begin{aligned}
&\sum_{i\in V_G}\langle i|G|v\rangle P_{v,x}P_{i,y}P_{w,y} = \sum_{j\in V_H}\langle y|H|j\rangle P_{v,x}P_{v,j}P_{w,y}\\
\overset{(9.3)}{\Leftrightarrow}\ &\sum_{i\in V_G}\langle i|G|v\rangle \delta_{iw}P_{v,x}P_{w,y} = \sum_{j\in V_H}\langle y|H|j\rangle P_{v,x}P_{v,j}P_{w,y}\\
\overset{(9.4)}{\Leftrightarrow}\ &\sum_{i\in V_G}\langle i|G|v\rangle \delta_{iw}P_{v,x}P_{w,y} = \sum_{j\in V_H}\langle y|H|j\rangle \delta_{xj}P_{v,x}P_{w,y}\\
\Leftrightarrow\ &\langle w|G|v\rangle P_{v,x}P_{w,y} = \langle y|H|x\rangle P_{v,x}P_{w,y}.
\end{aligned}$$

The final equation implies condition (9.5). Conversely condition 9.5 is equivalent to the following equation:

$$\langle w|G|v\rangle P_{v.x}P_{w,y} = \langle y|H|x\rangle P_{v,x}P_{w,y}. \tag{9.7}$$

Equation (9.7) is equivalent by equation (2.14) to the following diagrammatic equation for all $v, w \in V_G$ and $x, y \in V_H$:



□

Atserias et al showed that a perfect strategy for the quantum graph isomorphism game exists if and only if there is a family of projectors fulfilling the requirements of a PPM and obeying condition (9.5).

Proposition 9.3.3 ([AMR+19, Theorem 5.4])**.** *Given classical graphs G and H, there exists a perfect strategy for the quantum graph isomorphism game, if and only if there is a nonzero family of projectors $P_{v,w}$ with $v \in V_G, w \in V_H$ which form a PPM and satisfy the condition (9.5).*

The correspondence between our quantum isomorphisms and the quantum graph isomorphisms of Atserias et al therefore follows from Propositions 9.3.2 and 9.3.3.

Corollary 9.3.4. *Quantum isomorphisms in* **QGraph** *restrict precisely to the quantum graph isomorphisms of Atserias et al [AMR+19] when considered between classical graphs.*

9.4 Quantum non-local games for QSet

We have seen that the restriction of **QGraph** to classical graphs gives the quantum graph homomorphisms and isomorphisms of non-local games. This equivalence has been shown through the correspondence of our quantum graph morphisms and those derived from quantum non-local games to grids of projectors obeying certain axioms. As noted in Remark 21, **QGraph** is a full sub 2-category of **QSet** and so, underlying every quantum homomorphism there is a quantum function. Similarly underlying every quantum isomorphism is a quantum bijection. While quantum graphs put additional constraints on the underlying quantum functions and bijections the fundamental mathematical structures are in **QSet**. Every quantum bijection of classical sets is a quantum isomorphism between pairs of complete or alternatively discrete graphs.

We now phrase quantum functions and quantum bijections within the non-local games formalism and prove equivalence. Of course, the resulting games are not particularly interesting in of themselves as there are classical functions between all sets and bijections between all sets of the same size. However, the examples are illustrative of how to move between the operational setting and our abstract framework. It is our belief that in this way many more quantum non-local games of interest will be derived from our framework and generalizations of it.

9.4.1 Quantum function game

Definition 9.4.1 (Quantum function game)**.** The following non-local game is the *quantum function game*:

The verifier has a pair of sets A and B. Alice and Bob share a maximally entangled quantum state on the system $\mathcal{H} \otimes \mathcal{H}$.

Step one. The verifier gives Alice and Bob each an element from a set A, say x to Alice and y to Bob.

Step two. Alice replies with x' and Bob replies with y'.

Rules. Alice and Bob are space-like separated and cannot communicate once the game starts. However they are allowed to perform a projective measurement on their side of the entangled system.

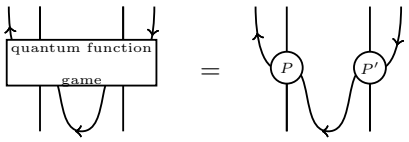
Alice and Bob win if the following conditions hold:

- $x', y' \in B$;
- $x = y \Rightarrow x' = y'$.

Classically, without recourse to quantum resources, a perfect strategy where Alice and Bob win with probability 1 is equivalent to a function between the sets $f : A \to B$. We now show the quantum analogue.

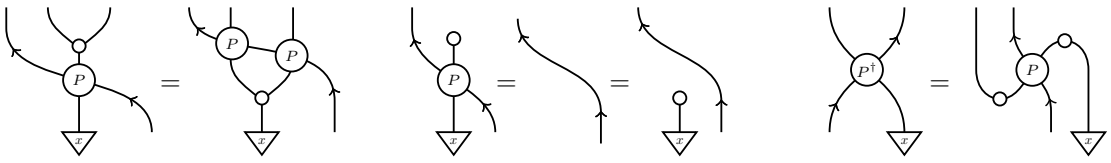
Lemma 9.4.2. *A perfect strategy for the quantum function game is equivalent to a quantum function.*

Proof. We now rephrase the game in our language. Alice has the left hand system of the entangled state and a †-SCFA on another system which we can interpret as another Hilbert space of possibly different dimension. She performs a projective measurement controlled on the element $x \in X$ giving an element $y \in Y$, so she performs a linear map of the form $P : \mathbb{C}^{|A|} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{|B|}$. Similarly, Bob has a linear map of the form $P' : \mathcal{H} \otimes \mathbb{C}^{|A|} \to \mathbb{C}^{|B|} \otimes \mathcal{H}$ where we have swapped the classical and quantum inputs as he has the right hand side of the maximally entangled state. We represent $\mathbb{C}^{|A|}$ and $\mathbb{C}^{|B|}$ as unoriented wires since we have dagger commutative Frobenius algebras corresponding to the sets A and B (represented below by white dots) defined on them. We represent $\mathcal{H}$ as an oriented wire. A round of the game is therefore represented by the following linear map F:

$F :=$ 

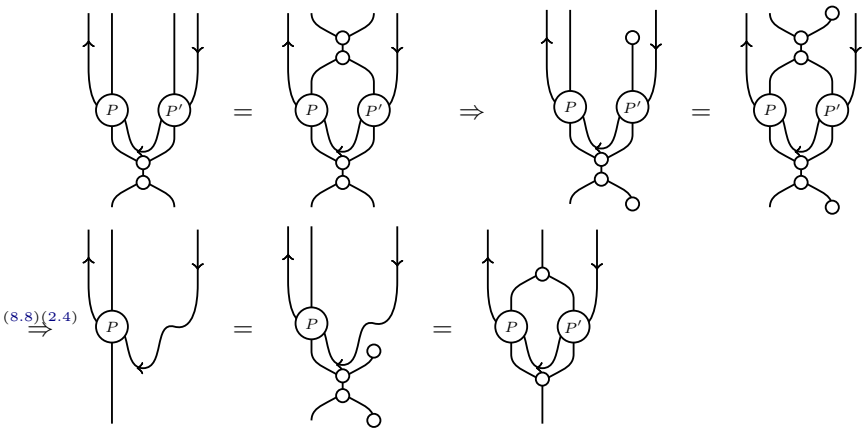
(9.8)

Recall that by Remark 18 a projective measurement is precisely a quantum element of a classical set. So for all $x \in A$ we have that $P|x\rangle$ is a quantum element:

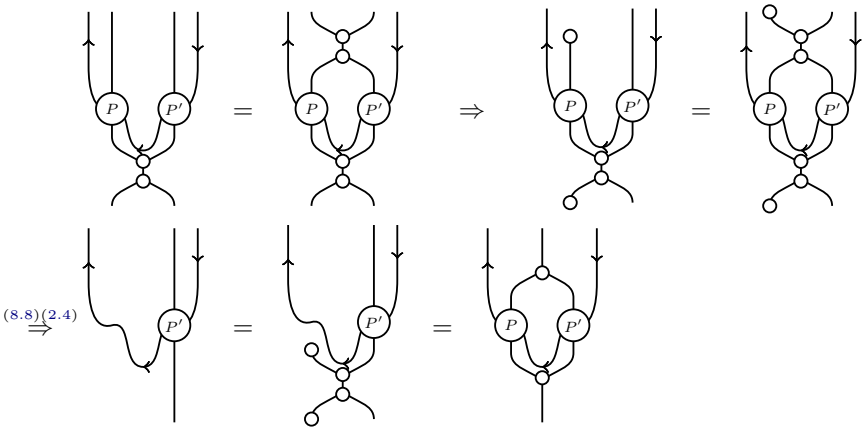


This is precisely the definition of a quantum function. Similarly P' is a quantum function. We now show that in fact $P' = P^T$. We require that if the verifier gives Alice and Bob the same element they return

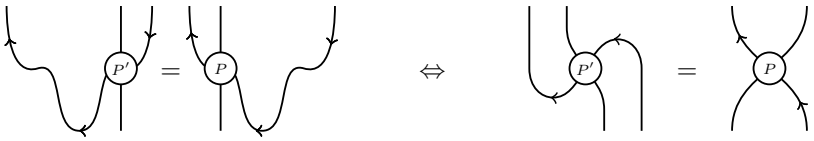
the same element. By projecting on to the diagonal, we obtain the following equation:



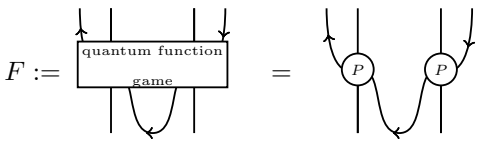
We also have that:



This now gives us that:



Thus we have that a perfect strategy for the quantum function game is characterised by P where P is a quantum function, and we have the following equation:



(9.9)

□

9.4.2 Quantum bijection game

We now introduce the quantum bijection game.

Definition 9.4.3 (Quantum bijection game)**.** The following non-local game is the *quantum bijection game*:

The verifier has two sets X and Y. Alice and Bob again share a maximally entangled quantum state on the system $\mathcal{H} \otimes \mathcal{H}$.

Step one. The verifier gives Alice and Bob x and y respectively with $x, y \in X \sqcup Y$.

Step two. Alice replies with x' and Bob replies with y'.

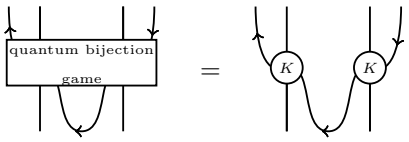
Rules. Alice and Bob are space-like separated and cannot communicate once the game starts. However they are allowed to perform a projective measurement on their side of the entangled system.

Alice and Bob win if the following conditions hold:

- Alice and Bob both reply with an element from the opposite set to which the element they received belonged.
- Let x_1, x_2 be the elements of X either received or returned by Alice and Bob respectively. Similarly let y_1 and y_2 be the elements of Y either received or returned by Alice and Bob respectively. To win they must have $x_1 = x_2 \Leftrightarrow y_1 = y_2$.

Lemma 9.4.4. *A perfect strategy for the quantum bijection game between sets X and Y is equivalent to a quantum bijection between X and Y.*

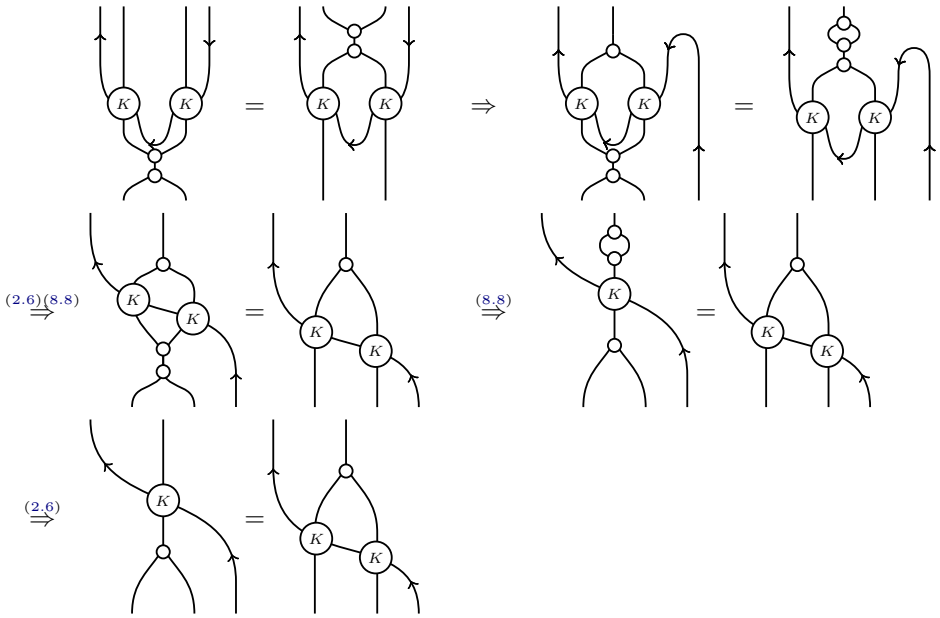
Proof. Now Alice and Bob can receive elements from either set so Alice performs a linear map of the form $K : (\mathbb{C}^{|X|} \oplus \mathbb{C}^{|Y|}) \otimes \mathcal{H} \to \mathcal{H} \otimes (\mathbb{C}^{|X|} \oplus \mathbb{C}^{|Y|})$. Similarly Bob performs a linear map of the form $K' : \mathcal{H} \otimes (\mathbb{C}^{|X|} \oplus \mathbb{C}^{|Y|}) \to (\mathbb{C}^{|X|} \oplus \mathbb{C}^{|Y|}) \otimes \mathcal{H}$. A perfect strategy for the quantum bijection game gives us a perfect strategy for the quantum function game between sets A and B given by $A = B = X \sqcup Y$. Thus $K^T = K'$ and K is a quantum function. The game is therefore represented by the linear map G:

$G :=$ 

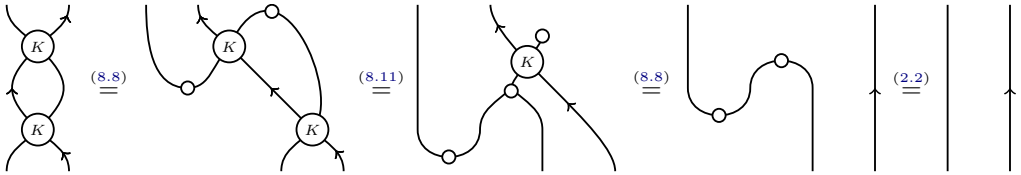
(9.10)

We now show the additional conditions for K to be a quantum bijection.

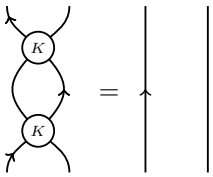
The rules imply that if Alice and Bob are each given the same element of $X \sqcup Y$ then they must reply with the same element of $X \sqcup Y$, graphically this is as follows:



The white dot is the †-SCFA $X \sqcup Y$. In order to show that the right hand of equation (8.11) holds we first show that K is unitary. Recall that a linear operator on a finite-dimensional Hilbert space is an isometry if and only if it is unitary. The following shows that K is an isometry:

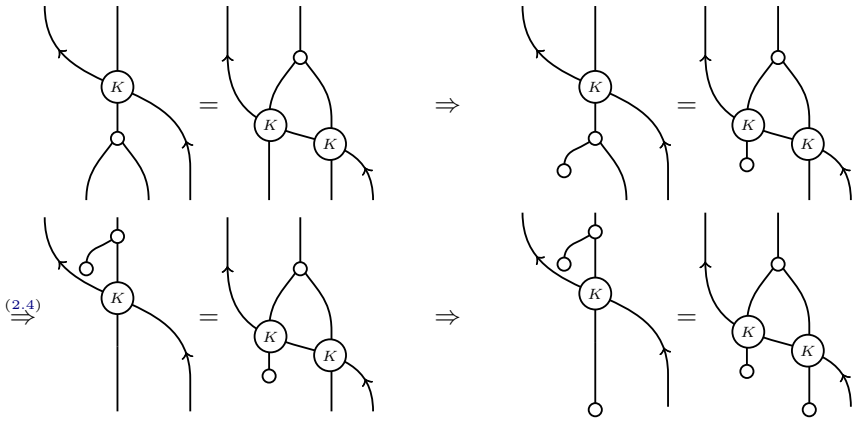


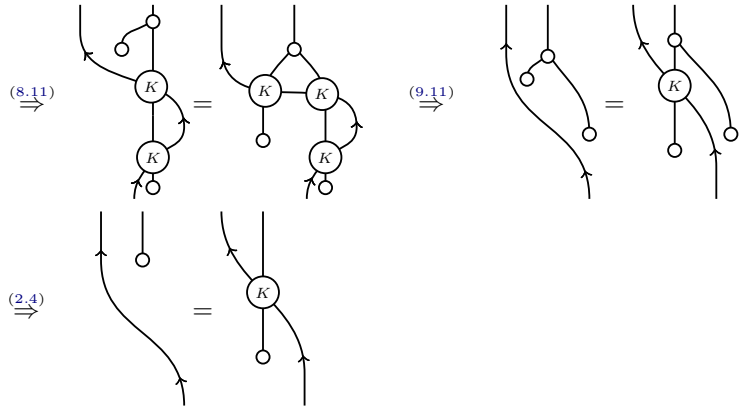
Thus we have:



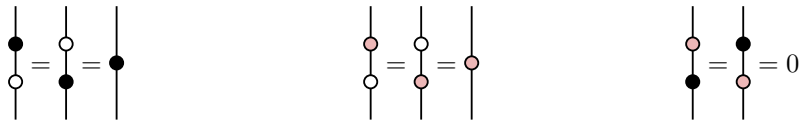
(9.11)

Now we use this to show the final condition.



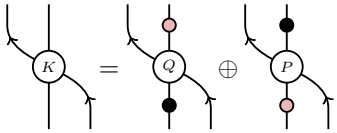


So K is a quantum bijection. Let the †-SCFA X acting on $\mathbb{C}^{|X|}$ be denoted by a black dot, and the †-SCFA Y acting on $\mathbb{C}^{|Y|}$ be denoted by a red dot. So the following equations hold:



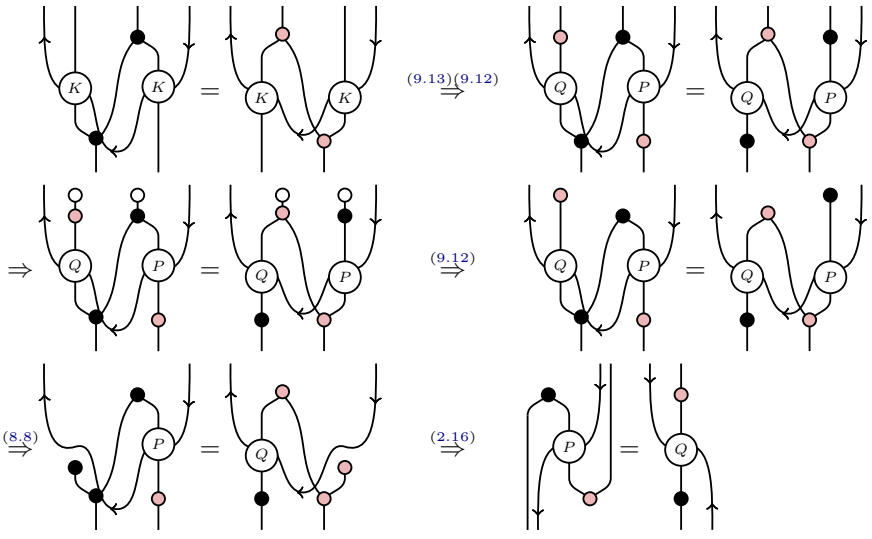
(9.12)

The fact that Alice and Bob must reply with a vertex from the opposite set to which the vertex they received is from, tells us that B must be composed as the direct sum of two linear maps Q and P as follows:



(9.13)

Both Q and P inherit the properties of a quantum bijection from K. This is an example of the semisimplicity of quantum functions (see [MRV18a], Section 6). We now show that $Q = P^\dagger$. If Alice is given an element $x \in X$ and Bob is given an element of $y \in Y$ then we know that under the perfect strategy K, Alice will reply with y if and only if Bob replies with x. This gives us the following equation:



□

9.5 Invariance results

Pairs of quantum isomorphic graphs which are not classically isomorphic exhibit quantum advantage and are therefore highly sought after. In order to reduce the number of graph pairs we must consider, it is useful to find properties of graphs which are invariant under quantum isomorphism. In this section we recall some known invariants and prove a new one regarding the number and size of connected components. This is by no means an exhaustive list of the invariants which have been discovered. As a notational point, given graphs G and H we denote the existence of a quantum isomorphism between them by $G \cong_q H$ and say that they are *quantum isomorphic*.

9.5.1 Existing results

The following result was already known.

Definition 9.5.1 (Cospectral [GM82])**.** Graphs G and H are *cospectral* if the multisets of eigenvalues for the adjacency matrices G and H are equal.

Theorem 9.5.2 ([AMR+19, Corollary 5.10])**.** *Given a pair of graphs G and H such that $G \cong_q H$, G and H are cospectral.*

In addition we have the following from Chapter 8.

Corollary 9.5.3. *Projective permutation matrices have the same number of projectors on the rows and the columns.*

Proof. This follows from Proposition 8.3.7 and Corollary 8.3.8. □

So we can conclude that quantum isomorphisms only exist between graphs with an equal number of vertices.

Corollary 9.5.4. *For graphs G and H such that $G \cong_q H$ we have that $|V_G| = |V_H|$.*

9.5.2 Composite quantum isomorphic graphs

In this final subsection we introduce a new quantum isomorphism invariant for classical graphs. We prove that the number and size of connected components of a graph is invariant under quantum isomorphism and that for pairs of graphs with fewer than 12 vertices the quantum isomorphism is made up of quantum isomorphisms between the components. This drastically reduces the number of candidate pairs when searching for quantum pseudo telepathy. In work that is to be published, the current author with David Reutter and Dominic Verdon have used Theorem 9.5.5 below as well as other techniques and results to prove that there are no pairs of graphs exhibiting pseudo-telepathy with fewer than 12 vertices.

First we require the following notation. Given a graph G having n connected components G_i with $i \in [n]$, let $M(G)$ denote the following multiset:

$$M(G) := \{|V_{G_0}|, ..., |V_{G_{n-1}}|\}.$$

Theorem 9.5.5. *Given graphs G and H, if $G \cong_q H$ then G and H have the same number of connected components and $M(G)$ and $M(H)$ are equal as multisets. Further, for all G with 11 or fewer vertices there exists a permutation $p \in S_n$ such that $G_{p(i)} \cong_q H_i$ for all $i \in [n]$.*

Proof. Let G and H be a pair of quantum isomorphic graphs. Let n be the number of connected components of G and m be the number of connected components of H. We will denote the connected components of G as G_i with $i \in [n]$ and the connected components of H as H_i with $i \in [m]$. Let $K_i := |V_{G_i}|$ and $L_i := |V_{H_i}|$. By Corollary 9.5.4 we have that G and H have the same number of vertices in total. Let $N := |V_G| = |V_H|$. Thus we have $\sum_{i=0}^{n-1} K_i = \sum_{i=0}^{m-1} L_i = N$.

Without loss of generality we assume that we have labelled the vertices of G with two indices as follows. For $i \in [n]$ and $\alpha \in [K_i]$ we have $g[i, \alpha] \in V_{G_i}$. Similarly for H, $j \in [m]$ and $\beta \in [L_j] \Rightarrow h[j, \beta] \in V_{H_j}$. We impose the following total order, for all a, b, c, α and β we have $a > b \Rightarrow g[a, \alpha] > g[b, \beta]$ and $\alpha > \beta \Rightarrow g[c, \alpha] > g[c, \beta]$. So the first index of a vertex, for which we will use a Roman letter, records which connected component it belongs to and the second index, for which we will use a Greek letter corresponds to an ordering within a connected component.

Let Q be a projective permutation matrix that witnesses the quantum isomorphism between G and H. Let $Q_{p,q}$ for $p \in V_G$ and $q \in V_H$ denote the projectors of Q and let $\mathcal{H}$ be the underlying Hilbert space. We can picture the projective permutation matrix as being broken up into a grid corresponding to the connected components as figure 9.1 illustrates. Let $p := g[i, \gamma]$ and $q := h[j, \delta]$ for some $\gamma \in [K_i]$ and $\delta \in [L_j]$.

For some $j \in [m]$ consider the jth connected component of H and the corresponding L_j rows of Q given by $Q_{g,h[j,\gamma]}$ for $\gamma \in [L_j]$ and $g \in V_G$. For the time being assume that $L_j \geq 2$, we will mention the case where $L_j = 1$ later. Choose α, $\beta \in [L_j]$ such that:

$$h[j, \alpha] \sim_H h[j, \beta]. \tag{9.14}$$

Such a choice is possible as H_j is a connected component. We will now fix the values of j, α and β and examine the corresponding rows of the projective permutation matrix.

Given any a, $b \in [n]$ such that $a \neq b$ we have that for all $\psi \in [K_a]$ and $\phi \in [K_b]$:

$$g[a, \psi] \not\sim_G g[b, \phi]. \tag{9.15}$$

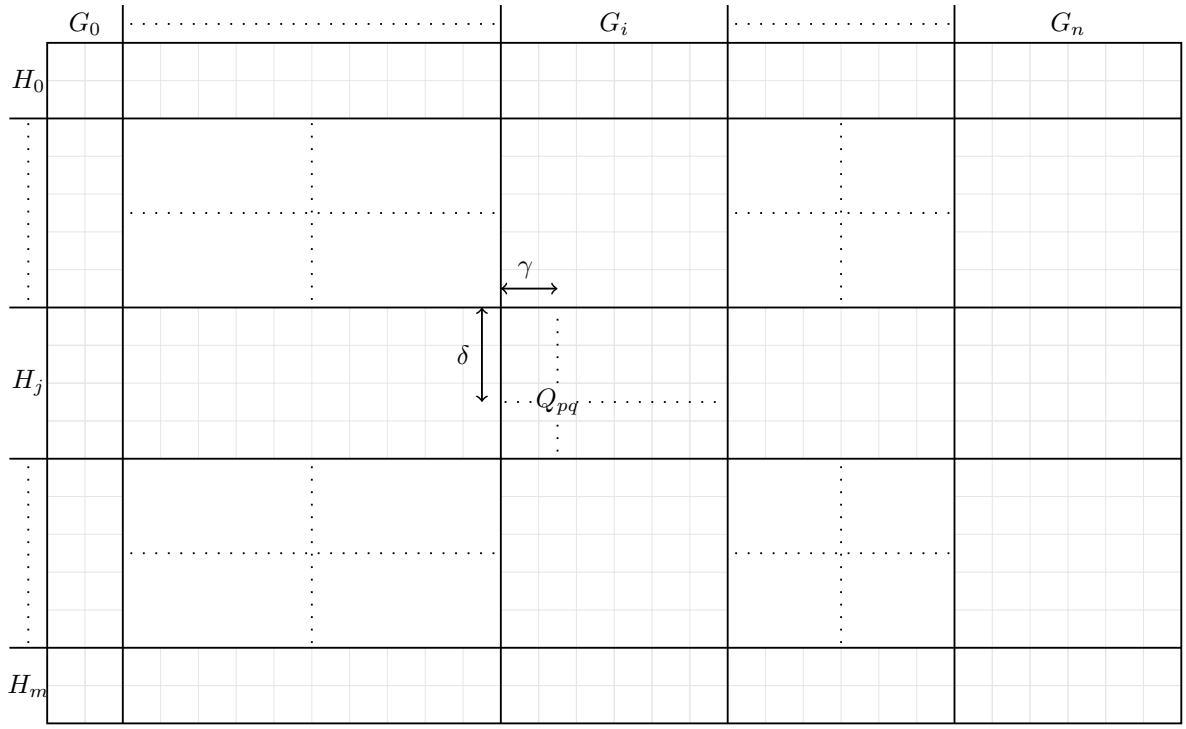


Figure 9.1: Showing the projective permutation matrix Q with the connected components of G and H.

This is true as the vertices $g[a, \psi]$ and $g[b, \phi]$ are in different connected components. Combining conditions (9.14) and (9.15) we see that, by the PPM condition in equation (9.5) for any a, $b \in [n]$ such that $a \neq b$ for all $\psi \in [K_a]$ and $\phi \in [K_b]$:

$$Q_{g[a,\psi],h[j,\alpha]} Q_{g[b,\phi],h[j,\beta]} = 0. \tag{9.16}$$

We now define the following projectors:

$$A_i := Q_{g[i,0],h[j,\alpha]} \oplus Q_{g[i,1],h[j,\alpha]} \oplus ... \oplus Q_{g[i,K_i-1],h[j,\alpha]}, \tag{9.17}$$

$$B_i := Q_{g[i,0],h[j,\beta]} \oplus Q_{g[i,1],h[j,\beta]} \oplus ... \oplus Q_{g[i,K_i-1],h[j,\beta]}. \tag{9.18}$$

Please refer to figure 9.2 below for another diagram of illustrating how the projectors A_i and B_i fit into the projective permutation matrix Q as a whole.

In the following we will subvert notation slightly and refer to the subspaces projected onto by projectors by the same symbols as the projectors. For any a and b with $a \neq b$ we have:

$$A_a \perp B_b, \tag{9.19}$$

$$A_a \perp A_b, \tag{9.20}$$

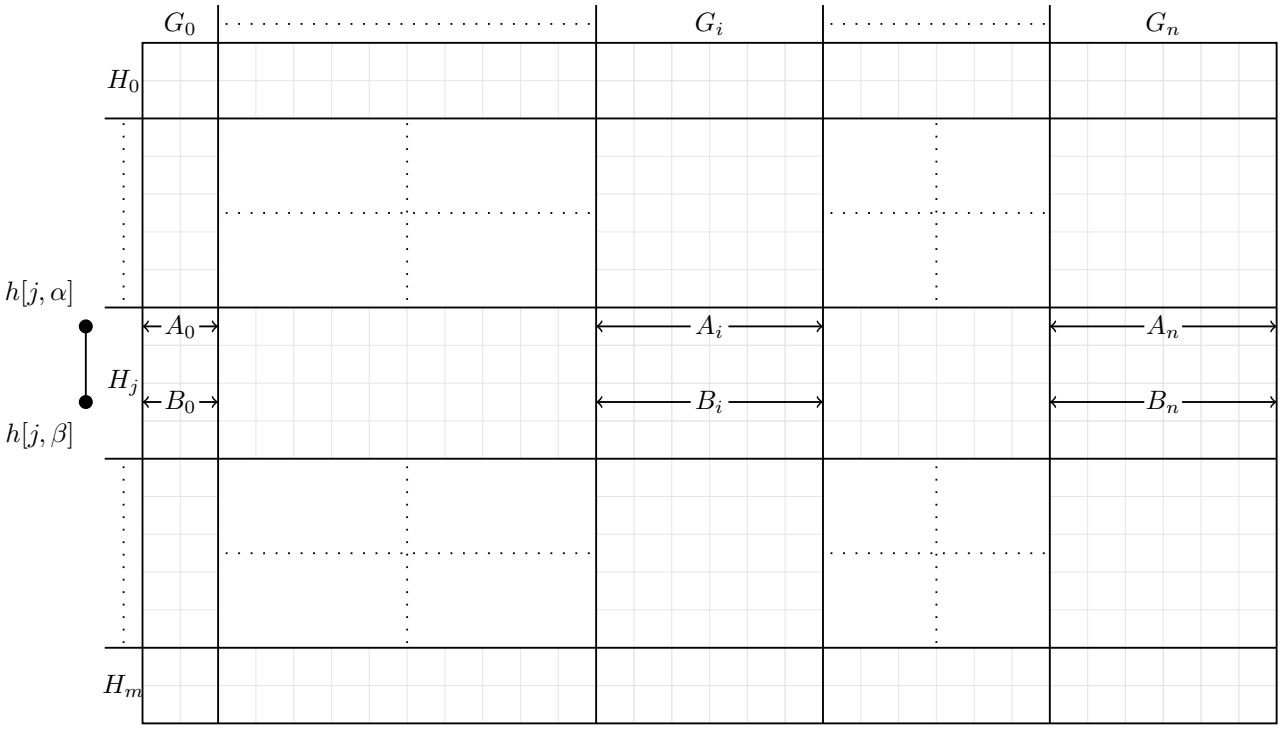


Figure 9.2: Showing the projectors A_i and B_i within Q annotated with an edge of the graph H.

$$B_a \perp B_b. \tag{9.21}$$

The first is due to equation (9.16). The projective permutation matrix axioms given by the left hand side equations of (9.3) and (9.4) gives us the other two. From right hand side equations of (9.3) and (9.4), we also have that:

$$\bigoplus_{i=0}^{n-1} A_i = \bigoplus_{i=0}^{n-1} B_i = \mathcal{H}. \tag{9.22}$$

Let $x \in \mathcal{H}$ be in the subspace A_i for some $i \in [n]$ then $x \not\perp B_k$ for $k \neq i$ by condition (9.19). Combining equations (9.21) and (9.22) we conclude that $x \in B_i$. Similarly $x \in B_i \Rightarrow x \in A_i$. Thus for all $i \in [n]$ we have $A_i = B_i$.

If $L_j \geq 3$ consider $\gamma \in [L_j]$ such that $h[j,\gamma] \sim h[j,\beta]$ (if this is not possible replace choose γ such that $h[j,\gamma] \sim h[j,\alpha]$) and define the projector C_i as:

$$C_i := Q_{g[i,0],h[j,\gamma]} \oplus Q_{g[i,1],h[j,\gamma]} \oplus \ldots \oplus Q_{g[i,K_i-1],h[j,\gamma]}. \tag{9.23}$$

We can now repeat exactly the same argument as we did for A_i and B_i to conclude that $C_i = B_i = A_i$ for all $i \in [n]$. Since H_j is a connected component if we repeat the above argument we find that for all $i \in [n]$ and $\theta \in [L_j]$:

$$A_i = Q_{g[i,0],h[j,\theta]} \oplus Q_{g[i,1],h[j,\theta]} \oplus \ldots \oplus Q_{g[i,K_i-1],h[j,\theta]}. \tag{9.24}$$

We can now switch the roles of G and H to derive the same condition for the column below a connected component of G. Explicitly, we take G_i for some $i \in [n]$. For some $h[i,\eta], h[i,\zeta] \in V_{H_i}$ such that $g[i,\eta] \sim g[i,\zeta]$ we define the projectors $P_j^{(\eta)}$ and $P_j^{(\zeta)}$ as follows:

$$P_j^{(\eta)} := Q_{g[i,\eta],h[j,0]} \oplus Q_{g[i,\eta],h[j,1]} \oplus ... \oplus Q_{g[i,\eta],h[j,L_j-1]}, \tag{9.25}$$

$$P_j^{(\zeta)} := Q_{g[i,\zeta],h[j,0]} \oplus Q_{g[i,\zeta],h[j,1]} \oplus ... \oplus Q_{g[i,\zeta],h[j,L_j-1]}. \tag{9.26}$$

We can conclude that for all a, $b \in [m]$ with $a \neq b$ and for all $\psi \in [L_a]$ and $\phi \in [L_b]$ we have that $h[a,\psi] \not\sim h[b,\phi]$ and thus by equation (9.5):

$$Q_{g[i,\eta],h[a,\psi]} Q_{g[i,\zeta],h[b,\phi]} = 0. \tag{9.27}$$

We now repeat exactly the same line of reasoning as above with A_i and B_i replaced by P_j and K_j and rows replaced by columns. From equation (9.27) and the PPM axioms (9.3), (9.4) and condition (9.5) we conclude that for all a, $b \in [m]$ such that $a \neq b$:

$$P_a^{(\eta)} \perp P_b^{(\zeta)}, \tag{9.28}$$

$$P_a^{(\eta)} \perp P_b^{(\eta)}, \tag{9.29}$$

$$P_a^{(\zeta)} \perp P_b^{(\zeta)}, \tag{9.30}$$

$$\bigoplus_{i=0}^{m-1} P_i^{(\eta)} = \bigoplus_{i=0}^{m-1} P_i^{(\zeta)} = \mathcal{H}. \tag{9.31}$$

From this we can conclude that for all $j \in [m]$ we have $P_j^{(\eta)} = P_j^{(\zeta)}$. Further, for all $\chi \in [K_i]$ we have the following equality:

$$P_j^{(\eta)} = Q_{g[i,\chi],h[j,0]} \oplus Q_{g[i,\chi],h[j,1]} \oplus ... \oplus Q_{g[i,\chi],h[j,L_j-1]}. \tag{9.32}$$

For clarity we refer to figure 9.3.

Now consider the rectangle of Q corresponding to H_j and G_i. Let Q_{pq} be any of the subspaces projected onto by the projectors in the right hand side summation of equation (9.17) which defines A_i. Since P_j contains every subspace Q_{gh} such that $g \in V_{G_i}$ and $h \in V_{H_j}$ we have that $Q_{pq} \subseteq P_j$. Similarly all the projectors of equation (9.25) project onto subspaces of A_i. We thus conclude that $A_i = P_j$.

We now deal with connected components with just a single vertex. Suppose we have a component G_k of graph G with one vertex which we label $g[k,*]$. For some connected component H_j as above with $L_j \geq 2$ we have that $A_k = Q_{g[k,*],h[j,\alpha]} = Q_{g[k,*],h[j,\beta]} = ...$ for all $\alpha, \beta, ... \in [L_k]$. Since these projectors

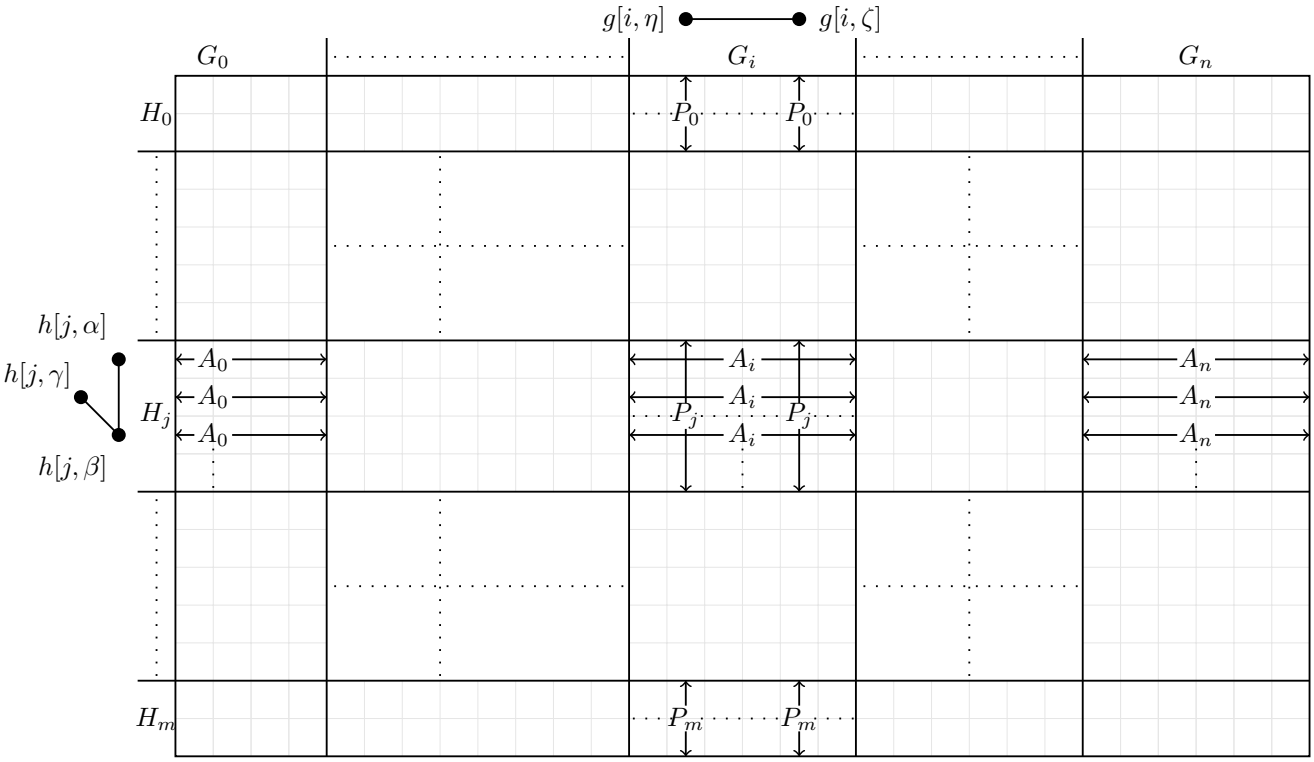


Figure 9.3: Showing the projectors A_i and P_j.

are on the same column they are orthogonal by condition (9.3). Thus for all $h \in V_H$ such that h is not an isolated vertex we have $Q_{g[k,*],h} = 0$. It then follows that there must be an equal number of isolated vertices in each graph as the projectors indexed by them form a PPM.

Since we chose the connected components G_i and H_j arbitrarily this holds for all $i \in [n]$ and $j \in [m]$. We denote the projector/subspace corresponding to G_i and H_j (and equal to A_i and P_j) as T_{ij}. So Q is an $m \times n$ grid of projectors T_{ij} such that the following conditions hold. For all $i, i_1, i_2 \in [n]$ and $j, j_1, j_2 \in [m]$ such that $i_1 \neq i_2$ and $j_1 \neq j_2$:

$$T_{ij_1} T_{ij_2} = 0, \tag{9.33}$$

$$T_{i_1 j} T_{i_2 j} = 0, \tag{9.34}$$

$$\sum_{k \in [m]} T_{ik} = \mathbb{I}_{\mathcal{H}}, \tag{9.35}$$

$$\sum_{k \in [n]} T_{kj} = \mathbb{I}_{\mathcal{H}}. \tag{9.36}$$

The first two conditions hold due to equations (9.29) and (9.20), the third is due to equation (9.31) and the fourth by equation (9.22). These are precisely the conditions for a PPM. Let T be the PPM with projectors T_{ij}. Since T is a PPM, by Corollary 9.5.4 T must be square so $m = n$.

We now return to the $K_i \times L_j$ rectangular array of projectors $Q_{g[i,\psi],h[j,\phi]}$ on the subspace T_{ij} for $i, j \in [n]$, $\psi \in [K_i]$ and $\phi \in [L_j]$. For convenience and since we have fixed T_{ij} let us make the following

notational switch. Denote $g[i,\psi]$ as ψ and $h[j,\phi]$ as ϕ for all $\psi \in [K_i]$ and $\phi \in [L_j]$. The following conditions hold. For all $\psi, \psi_1, \psi_2 \in [K_i]$ and $\phi, \phi_1, \phi_2 \in [L_j]$ such that $\psi_1 \neq \psi_2$ and $\phi_1 \neq \phi_2$:

$$Q_{\psi\phi_1} Q_{\psi\phi_2} = 0,$$

$$Q_{\psi_1\phi} Q_{\psi_2\phi} = 0,$$

$$\sum_{k\in[m]} Q_{\psi k} = T_{ij},$$

$$\sum_{k\in[n]} Q_{k\phi} = T_{ij}.$$

The first two hold due to equations (9.4) and (9.3) as Q is a PPM. Since $T_{ij} = A_i = P_j$, the third and fourth conditions above follow by equations (9.24) and (9.32).

If T_{ij} is a non-zero subspace of H then the conditions above imply that the projectors $Q_{\psi\phi}$ form a PPM and therefore by Corollary 9.5.4 $K_i = L_j$. It follows that for all pairs of connected components G_i and H_j we have $K_i \neq L_j \Rightarrow T_{ij} = 0$.

Consider the subset of $[n]$ given by $X := \{i | K_i = w\}$ for some $w \in \mathbb{N}$ such that X is non-empty. Let $Y := \{i | L_i = w\}$. Y cannot be the empty set since given a connected component G_i, we have that $\bigoplus_{k=0}^{n-1} T_{ik} = \mathcal{H}$ by equation (9.36). So there must exist some $j \in [n]$ such that $T_{ij} \neq 0$ and thus $K_i = L_j = w$.

Let $|Y| = y$ and $|X| = x$. Consider the rectangle $s \times t$ which forms a sub-rectangle of the PPM T given by the projectors T_{ij} such that $i \in X$ and $j \in Y$. For $i \in X$ and $k \in \{[n] \backslash Y\}$ we have $K_i \neq L_k$ and so $T_{ik} = 0$. Thus for all $i \in X$:

$$\bigoplus_{k\in Y} T_{ik} = \bigoplus_{k=0}^{n-1} T_{ik} = \mathcal{H}. \tag{9.37}$$

Similarly for all $j \in Y$:

$$\bigoplus_{k\in X} T_{kj} = \bigoplus_{k=0}^{n-1} T_{kj} = \mathcal{H}. \tag{9.38}$$

We inherit the LHS equations of (9.3) and (9.4) from T. Equations (9.37) and (9.38) give us the RHS equations of(9.3) and (9.4). So this is a w-by-w PPM, we will call it T^w.

It follows that $x = y$ by Corollary 9.5.4. Clearly this holds for all values of w and so we have now proven that $M(G) = M(H)$.

For all pairs G_i and H_j such that $T_{ij} \neq 0$ we have $G_i \cong_q H_j$ since T_{ij} is a PPM and the additional quantum isomorphism condition equation (9.5) is satisfied due to Q being a quantum isomorphism.

We now show that a permutation $p \in S_n$ exists for which $G_i \cong_q H_{p(i)}$ for all $i \in [n]$ when $|V_G| \leq 11$. For values of w such that $x = y = 1$ suppose $X = \{i\}$ and $Y = \{j\}$, then we simply choose $p(i) = j$ and we must have that $T^w = T_{ij} = \mathcal{H}$ by equations (9.37) and (9.38) and thus $G_i \cong_q H_j = H_{p(i)}$.

For $w \leq 2$ we can choose any permutation $|X| \to |Y| = |X|$ as a sub-permutation of p and we have

$G_x \cong_q H_{p(x)}$ as all pairs of 1-vertex graphs and pairs of 2-vertex graphs are classically isomorphic and therefore quantum isomorphic.

For $w \geq 3$ and $|X| \leq 3$ we have that T^w is a 3×3 PPM. By [MRV18a, Proposition 6.14] all PPMs of size 3×3 or smaller are the direct sum of permutations. So we can always choose one of these permutations as a sub-permutation of p, and then for each pair $i \in X$ and $p(i) \in Y$ we will have that $T_{i,p(i)}$ is non-zero and thus a PPM which witnesses a quantum isomorphism $G_i \cong_q H_{p(i)}$. For $w \geq 3$ and $|X| = |Y| \geq 4$ it is possible that no such permutation exists as not all components are necessarily classically isomorphic and there are PPMs that are not the direct sum of permutations. The first value of $|V_G|$ for which this could happen is $3 \times 4 = 12$. Thus for $|V_G| \leq 11$ such a permutation exists. □

Bibliography

[Abd14] Kanat Abdukhalikov. Symplectic spreads, planar functions, and mutually unbiased bases. *Journal of Algebraic Combinatorics*, 41(4):1055–1077, 2014.

[ABdSZ17] Samson Abramsky, Rui Soares Barbosa, Nadish de Silva, and Octavio Zapata. The quantum monad on relational structures. *Proceedings of Mathematical Foundations of Computer Science*, 2017.

[AHKS06] David Avis, Jun Hasegawa, Yosuke Kikuchi, and Yuuya Sasaki. A quantum protocol to win the graph colouring game on all Hadamard graphs. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 89(5):1378–1381, 2006.

[AMR+19] Albert Atserias, Laura Mančinska, David E. Roberson, Robert Šámal, Simone Severini, and Antonios Varvitsiotis. Quantum and non-signalling graph isomorphisms. *Journal of Combinatorial Theory, Series B*, 136:289–328, 2019.

[Ban05] Teodor Banica. Quantum automorphism groups of homogeneous graphs. *Journal of Functional Analysis*, 224(2):243–280, 2005.

[Ban19a] Teodor Banica. Higher orbitals of quizzy quantum group actions. *Advances in Applied Mathematics*, 109:1–37, 2019.

[Ban19b] Teodor Banica. Higher transitive quantum groups: theory and models. *Colloquium Mathematicum*, 156(1):1–14, 2019.

[Bar14] Bruce Bartlett. Quasistrict symmetric monoidal 2-categories via wire diagrams. 2014.

[BB07] Teodor Banica and Julien Bichon. Quantum automorphism groups of vertex-transitive graphs of order ≤ 11. *Journal of Algebraic Combinatorics*, 26(1):83–105, 2007.

[BB09] Teodor Banica and Julien Bichon. Quantum groups acting on 4 points. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2009(626):75–114, 2009.

[BBC+93] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993.

[BBC07a] Teodor Banica, Julien Bichon, and Gatan Chenevier. Graphs having no quantum symmetry. *Annales de l'institut Fourier*, 57(3):955–971, 2007.

[BBC07b] Teodor Banica, Julien Bichon, and Benoît Collins. Quantum permutation groups: A survey. In *Noncommutative Harmonic Analysis with Applications to Probability*. Institute of Mathematics Polish Academy of Sciences, 2007.

[BBE+07] Ingemar Bengtsson, Wojciech Bruzda, Åsa Ericsson, Jan-Åke Larsson, Wojciech Tadej, and Karol Życzkowski. MUBs and Hadamards of order six. *Journal of Mathematical Physics*, 48(5):052106, 2007.

[BBRV02] Somshubhro Bandyopadhyay, P Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002.

[BCF18] Michael Brannan, Alexandru Chirvasitu, and Amaury Freslon. Topological generation and matrix models for quantum reflection groups. 2018.

[BČL+16] Karol Bartkiewicz, Antonín Černoch, Karel Lemr, Adam Miranowicz, and Franco Nori. Temporal steering and security of quantum key distribution with mutually unbiased bases against individual attacks. *Physical Review A*, 93(6), 2016.

[Bic03] Julien Bichon. Quantum automorphism groups of finite graphs. *Proceedings of the American Mathematical Society*, 131(3):665–673, 2003.

[BMS12] John W Barrett, Catherine Meusburger, and Gregor Schaumann. Gray categories with duals and their diagrams. 2012.

[BN08] Kyle Beauchamp and Remus Nicoara. Orthogonal maximal abelian *-subalgebras of the 6×6 matrices. *Linear Algebra and its Applications*, 428(8):1833–1853, 2008.

[BN17] Tristan Benoist and Ion Nechita. On bipartite unitary matrices generating subalgebra-preserving quantum operations. *Linear Algebra and its Applications*, 521:70–103, 2017.

[BSTW05] P Oscar Boykin, Meera Sitharam, Pham Huu Tiep, and Pawel Wocjan. Mutually unbiased bases and orthogonal decompositions of lie algebras. 2005.

[BW04] Thomas Beth and Paweł Wocjan. New construction of mutually unbiased bases in square dimensions. 2004.

[CBKG02] Nicolas J Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(12):127902, 2002.

[CC15] Xiwang Cao and Wun-Seng Chou. More constructions of approximately mutually unbiased bases. *Bulletin of the Australian Mathematical Society*, 93(2):211–222, 2015.

[CD11] Bob Coecke and Ross Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011.

[CDKW12] Bob Coecke, Ross Duncan, Aleks Kissinger, and Quanlong Wang. Strong complementarity and non-locality in categorical quantum mechanics. In *2012 27th Annual IEEE Symposium on Logic in Computer Science*. IEEE, 2012.

[CMN+07] Peter J Cameron, Ashley Montanaro, Michael W Newman, Simone Severini, and Andreas Winter. On the quantum chromatic number of a graph. *The Electronic Journal of Combinatorics*, 14(1):R81, 2007.

[CPV09] Bob Coecke, Duško Pavlović, and Jamie Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 2009.

[Cra91] Robert Craigen. Equivalence classes of inverse orthogonal and unit Hadamard matrices. *Bulletin of the Australian Mathematical Society*, 44(01):109–115, 1991.

[DCK+13] Vincenzo D'Ambrosio, Filippo Cardano, Ebrahim Karimi, Eleonora Nagali, Enrico Santamato, Lorenzo Marrucci, and Fabio Sciarrino. Test of mutually unbiased bases for six-dimensional photonic quantum systems. *Scientific reports*, 3, 2013.

[DD16] Ross Duncan and Kevin Dunne. Interacting frobenius algebras are hopf. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science - LICS 16*. ACM Press, 2016.

[DSW13] Runyao Duan, Simone Severini, and Andreas Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number. *IEEE Transactions on Information Theory*, 59(2):1164–1174, 2013.

[FY34] Ronald A. Fisher and Frank Yates. The 6×6 latin squares. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 30.04, pages 492–507. Cambridge Univ Press, 1934.

[GCA+12] Mile Gu, Helen M. Chrzanowski, Syed M. Assad, Thomas Symul, Kavan Modi, Timothy C. Ralph, Vlatko Vedral, and Ping Koy Lam. Observing the operational significance of discord consumption. *Nature Physics*, 8(9):671–675, 2012.

[GM82] Chris Godsil and Brendan McKay. Constructing cospectral graphs. *Aequationes Mathematicae*, 25(1):257–268, 1982.

[GR09] Chris Godsil and Aidan Roy. Equiangular lines, mutually unbiased bases, and spin models. *European Journal of Combinatorics*, 30(1):246–262, 2009.

[GRDMŻ18] Dardo Goyeneche, Zahra Raissi, Sara Di Martino, and Karol Życzkowski. Entanglement and quantum combinatorial designs. *Physical Review A*, 97(6):062326, 2018.

[GS14] Sibasish Ghosh and Ajit Iqbal Singh. Invariants for maximally entangled vectors and unitary bases. 2014.

[GZ15] Stefano Gogioso and William Zeng. Fourier transforms from strongly complementary observables. 2015.

[Hal45] Marshall Hall. An existence theorem for latin squares. *Bulletin of the American Mathematical Society*, 51(6):387–388, 1945.

[HM63] Paul R Halmos and Jack McLaughlin. Partial isometries. *Pacific Journal of Mathematics*, 13(2):585–596, 1963.

[Ivo81] ID Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241, 1981.

[JS91] André Joyal and Ross Street. An introduction to Tannaka duality and quantum groups. In *Lecture Notes in Mathematics*, pages 413–492. Springer Berlin Heidelberg, 1991.

[Kni96] Emanuel Knill. Group representations, error bases and quantum codes. 1996.

[KR] Andreas Klappenecker and Martin Rtteler. Constructions of mutually unbiased bases. In *Lecture Notes in Computer Science*, pages 137–144. Springer Berlin Heidelberg.

[KR03] Andreas Klappenecker and Martin Rötteler. Unitary error bases: Constructions, equivalence, and applications. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 139–149. Springer, 2003.

[KW12] Greg Kuperberg and Nik Weaver. *A von Neumann algebra approach to quantum metrics/quantum relations*, volume 215. American Mathematical Society, 2012.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[LW18] Mao-Sheng Li and Yan-Ling Wang. Masking quantum information in multipartite scenario. *Physical Review A*, 98(6), 2018.

[Mac12] Duncan B Macdonald. Description of a silver amulet. *Zeitschrift für Assyriologie und Vorderasiatische Archäologie*, 26(1-3):267–269, 1912.

[Man42] Henry B Mann. The construction of orthogonal latin squares. *The Annals of Mathematical Statistics*, 13(4):418–423, 1942.

[MDG+13] Mhlambululi Mafu, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus, and Andrew Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3):032305, 2013.

[Mla91] Włodzimierz Mlak. *Hilbert spaces and operator theory*, volume 51. Springer, 1991.

[MR16] Laura Mančinska and David E Roberson. Quantum homomorphisms. *Journal of Combinatorial Theory, Series B*, 118:228–267, 2016.

[MRV18a] Benjamin Musto, David Reutter, and Dominic Verdon. A compositional approach to quantum functions. *Journal of Mathematical Physics*, 59(8):081706, 2018.

[MRV18b] Benjamin Musto, David Reutter, and Dominic Verdon. The morita theory of quantum graph isomorphisms. *Communications in Mathematical Physics*, 365(2):797–845, 2018.

[Mus14] Benjamin Musto. Exploring quantum teleportation through unitary error bases. Master's thesis, Department of Computer Science, University of Oxford, 2014.

[Mus17] Benjamin Musto. Characterizing maximal families of mutually unbiased bases. 2017.

[MV15] Benjamin Musto and Jamie Vicary. Quantum Latin squares and unitary error bases. *Quantum Information and Computation*, pages 1318–1332, 2015.

[OP16] Carlos M Ortiz and Vern I Paulsen. Quantum graph homomorphisms via operator systems. *Linear Algebra and Its Applications*, (497):23–43, 2016.

[PDB09] Tomasz Paterek, Borivoje Dakić, and Časlav Brukner. Mutually unbiased bases, orthogonal latin squares, and hidden-variable models. *Physical Review A*, 79(1), 2009.

[PSS+16] Vern I Paulsen, Simone Severini, Daniel Stahlke, Ivan G Todorov, and Andreas Winter. Estimating quantum chromatic numbers. *Journal of Functional Analysis*, 270(6):2188–2222, 2016.

[PT15] Vern I Paulsen and Ivan G Todorov. Quantum chromatic numbers via operator systems. *The Quarterly Journal of Mathematics*, 66(2):677–692, 2015.

[PYHP15] Fernando Pastawski, Beni Yoshida, Daniel Harlow, and John Preskill. Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence. *Journal of High Energy Physics*, 2015(6), 2015.

[Rob16] David E Roberson. Conic formulations of graph homomorphisms. *Journal of Algebraic Combinatorics*, 43(4):877–913, 2016.

[RV16] David Reutter and Jamie Vicary. Biunitary constructions in quantum information. 2016.

[Sel08] Peter Selinger. Idempotents in dagger categories. *Electronic Notes in Theoretical Computer Science*, 210(Supplement C):107 – 122, 2008. Proceedings of the 4th International Workshop on Quantum Programming Languages (QPL 2006).

[SHB+12] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C Hiesmayr. Entanglement detection via mutually unbiased bases. *Physical Review A*, 86(2):022311, 2012.

[Sho96] Peter Shor. Fault-tolerant quantum computation. pages 56–65. IEEE Computer Society Press, 1996.

[Smi06] Jonathan D. H. Smith. *An Introduction to Quasigroups and Their Representations*. Chapman and Hall/CRC, 2006.

[Soł19] P. M. Sołtan. Quantum semigroups from synchronous games. *Journal of Mathematical Physics*, 60(4):042203, 2019.

[SS12] Giannicola Scarpa and Simone Severini. Kochen–Specker sets and the rank-1 quantum chromatic number. *IEEE Transactions on Information Theory*, 58(4):2524–2529, 2012.

[Sta16] Dan Stahlke. Quantum zero-error source-channel coding and non-commutative graph theory. *IEEE Transactions on Information Theory*, 62(1):554–577, 2016.

[Ste96] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.

[Sti55] W. Forrest Stinespring. Positive functions on c ∗ -algebras. *Proceedings of the American Mathematical Society*, 6(2):211, 1955.

[Str72] Ross Street. The formal theory of monads. *Journal of Pure and Applied Algebra*, 2(2):149–168, 1972.

[TŻ06] Wojciech Tadej and Karol Życzkowski. A concise guide to complex Hadamard matrices. *Open Systems & Information Dynamics*, 13(02):133–177, 2006. quant-ph/0512154.

[Vic10] Jamie Vicary. Categorical formulation of finite-dimensional quantum algebras. *Communications in Mathematical Physics*, 304(3):765–796, 2010.

[VV17] Dominic Verdon and Jamie Vicary. Tight reference frame–independent quantum teleportation. *Electronic Proceedings in Theoretical Computer Science*, 236:202–214, 2017.

[VV18] Dominic Verdon and Jamie Vicary. Tight quantum teleportation without a shared reference frame. *Physical Review A*, 98(1), 2018.

[VW00] Karl Gerd H. Vollbrecht and Reinhard F. Werner. Why two qubits are special. *Journal of Mathematical Physics*, 41(10):6772–6782, 2000.

[Wan98] Shuzhou Wang. Quantum symmetry groups of finite spaces. *Communications in Mathematical Physics*, 195(1):195–211, 1998.

[Wea10] Nik Weaver. Quantum relations. 2010.

[Wea15] Nik Weaver. Quantum graphs as quantum relations. 2015.

[Wer01] Reinhard F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, 2001.

[WF89] William K Wootters and Brian D Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[WW10] Stephanie Wehner and Andreas Winter. Entropic uncertainty relations a survey. *New Journal of Physics*, 12(2):025009, 2010.

[ZV14] William Zeng and Jamie Vicary. Abstract structure of unitary oracles for quantum algorithms. 2014.